AOI: 10.100.234513.0281
13th international conference on Microelectronics, Circuits and Systems, Micro2026

Blockchain-Based Decentralized File Sharing System

Vasu Tripathi, Ashutosh Singh

Department of Computer Science and Engineering,
Galgotias University, Greater Noida, Uttar Pradesh, India.
Corresponding Author: tripathivasu7@gmail.com

ABSTRACT

The digital platforms have brought a revolution to the way information is stored and shared. But the websites have revealed the weaknesses which it possesses in the old traditional, centralised kind of storage. All the recent news about privacy invasion, manipulations of data, server failures, and a single source of control over the key data to a user has raised the possibility of more demands towards other alternatives that resulted in the emergence of Blockchain and the Inter Planetary File System (IPFS). These technologies are decentralising trust and storage, which is to allocate the trust and storage in multiple nodes. Blockchain is intended to ensure a standardized path of the impartial history of transactions that cannot be changed; whereas the IPFS offers a more prosperous procedure of allocating files by offering the user the capability to relate the files through content addressing. Consequently, this paper is the proposal of the synergistic model of Blockchain and IPFS deploying Smart Contracts to be able to verify the level of user access, control the Metadata affixed to files, and also make interactions super-resistant to tampering. The proposed Hybrid framework is better in terms of integrating the data integrity, less dependency on centralized servers or more resilience in relation to unauthorised entry to the data store of vital information or system malfunction. Whereas latency when using decentralised peer-to-peer networks may be a bit higher than when making use of the conventional centralised servers, the decentralised networks are more transparent, verifiable and secure when storing data over the long run. The Hybrid Blockchain-IPFS model proves that new emerging modern applications that need reliable censorship-resistant and secure sharing of files can use the decentralised storage.

Keywords: Blockchain, InterPlanetary File System (IPFS), Decentralized Storage, Censorship-Resistant Storage, Decentralized Applications (DApps).

I. INTRODUCTION

The sheer increase in digital information, as well as its growing reliance on platforms built on the clouds, has radically changed the way people, companies, and institutions store, handle, and share data. Although central storage platforms like Google Drive, Dropbox, and Amazon S3 are convenient, easy to operation and scalable, they also present users with numerous vulnerabilities. The latter are vulnerability to privacy, vendor lock-in, high operational expenses, vulnerability to cyber-attacks, and the consistent possibility of having a single point of failure [10]. In event of downtime or breach of a centralized server, all users who require use of that infrastructure get affected directly hence data becomes unavailable or even lost. Furthermore, there has been an increased concern with regards to unauthorized surveillance, data mining, and insufficient user control over information on sensitive platforms as placed on centralized databases [6].

In order to alleviate these constraints, decentralized and distributed technologies have been the primary focus of interest in the recent years. Originally, blockchain was proposed with Bitcoin as the first, providing a ledger that is both immutable and transparent and cannot be tampered with, creating the ability to create trust without the involvement of any central governing agency [6]. The fact that it is decentralized means that there is no one individual that can manipulate the stored records hence making it very appropriate in cases where verifiable and secure data handling are in the applications. Similar to Blockchain, the Inter Planetary File System (IPFS) was created to use a content-addressable system instead of location-based addressing, which allows files to be stored and accessed across various nodes within a distributed system [9]. IPFS can guarantee the presence of inconsistencies or tampering by causing a new unique hash because of cryptographic hashing which means that a change to the stored content has been made.

Most of the current decentralized file-sharing systems have not successfully harnessed these forces and integrated Blockchain and IPFS into one integrated architecture, despite their individual power. Numerous previous ones find it difficult to integrate secure access control, with only Blockchain not being efficient at managing the storage of large volumes of data, and only IPFS not implementing any authorization logic [4],[5]. This provides a research and implementation gap present in drafting a system that, in addition to offering an effective distributed storage, will facilitate semi-transparent and rule-approved validation of data access. To overcome these weaknesses, scientists and programmers have started to investigate hybrid models where the most important metadata and access rights are stored on the Blockchain, and large files are stored with the help of IPFS. Smart Contracts are an

ISBN: 978-81-689089-0-1

imperative aspect of such solutions, as they apply automated and non-mutable rules of authorization. These systems that use self-execution properties of programs make sure that a file that is stored in IPFS can be accessed only by users who meet special requirements, which are encoded in the contract [3],[4]. This will remove the use of middlemen, minimize the chances of unauthorized intrusion and promote confidence in the system as a whole.

The aim of the presented framework in this research is to develop a decentralized file-sharing space that incorporates immutability and auditability of Blockchain and scalability and efficiency of IPFS. The system will have an objective of ensuring secure file upload, retrieval, verification and access control devoid of any centralized authority. The model provides clear access control, automatic verification of content identifiers (CIDs) and stable tracking of all interactions between users through the use of Smart Contracts. This creates a system that is robust and opposed to censorship, manipulation and server breakdowns and thus it would suit sensitive applications in disaster management, sharing scholarly research, offering health care information transfer and distributing enterprise files [1],[2],[8].

Furthermore, the study also compares the performance trade-offs among a centralized and a decentralized storage. Although decentralized networks can add some Latency to the retrieval process in moderation through distributed consensus and data propagation, they provide better transparency, privacy and fault tolerance - qualities that have gained greater importance in today's level of digital ecosystems [9], [10]. This introduction establishes the basis of comprehending how hybrid decentralized storage can consider most of the glaring issues that are disturbing the existing file sharing systems through architectural diagrams, workflow analysis, table and graphs.

II. RELATED WORK AND BACKGROUND

In recent years, there has been research magnification with regard to merging the blockchain and Interplanetary file system (IPFS) in order to overcome the security, integrity and scale shortcomings of the centralized systems of storage. Jain et al. [1] offered a more advanced blockchain-IPFS system to provide the secure sharing of electronic health records in which blockchain can guarantee immutable storage of metadata and IPFS can handle large medical files. Their method enhances the privacy of data and accessibility of traces but is health care-specific. Likewise, Mishra et al. [2] examined blockchain-IPFS support of IoT-oriented healthcare data storage, where automated access controls become decentralized on the basis of smart-contracts; that said, the framework stresses on the IoT scalability but not file-sharing that is typically generalized.

In other areas besides the healthcare sector, Haque et al. [3] presented a blockchain and IPFS-based repository system of source code with a middleman-aid model to implement the controlled access and integrity assurance. Although this method is successful in joint development, there is the partial dependency on a component that is obtained between components. A blockchain-powered authentication and access control system in the IPFS-based file storage suggested by Deepthi et al. [4] showed enhanced security against unauthorized users, but did not perform thorough performance analysis. In blockchain ecosystems, Santoso et al. [5] paid attention to censorship-resistant decentralized file sharing with IPFS, but with a focus on resiliency and availability and little discussion of fine-grained access control.

A number of studies focus on hybrid decentralized storage

structures. A conceptual blockchain-IPFS storage architecture was introduced by Chintal [6], which enhances fault tolerance and data immutability, but it was not implemented at the level. Chen et al. [7] suggested BISE, a consortia, blockchain, and IPFS-based data-sharing system that alters the balance between decentralization and regulatory compliance, which is applicable to an enterprise. A system of safe file sharing that was built by Tarhouni and Chaabane [8] was based on blockchain and IPFS, which makes it more secure and gives more capability to privacy and auditability, but it is also limited to health care applications.

Kumar et al. [9] proposed the file storage and sharing system (BlockShare) that is based on blockchain storage use, exploiting IPFS and smart contracts to put access control on autopilot, with regard to better transparency being gained at the cost of acceptable latency. Osuolale et al. [10] have come up with a hybrid blockchain-based file-sharing system that is deployed in the cloud environment to offer a transition model between centralized and decentralized storage, but still with the use of cloud infrastructure in part.

In general, the currently available literature tracks the efficiency of blockchain-IPFS integration in the way of safe and decentralized storage. Nevertheless, the majority of the researches are restricted to a particular application area or do not provide in-depth workflow modeling, authorization system, as well as comparison performance analysis. It is in view of these limitations that a generalized fully integrated decentralized file sharing model that has explicit architecture, automated access control, and performance analysis is needed.

A. Novelty

The uniqueness of the suggested system is the tight-knit blend of a hybrid system combining blockchain-based non-persistent metadata storage, IPFS-based content-addressable file storage, and smart contract-based authorization into a single workflow. As opposed to

ISBN: 978-81-689089-0-1

prior literature defining there as two different things, access control or storage, deemed parts of the same construct, the present work directly inlays access validation into smart contracts and guarantees automated, transparent, and unalterable authorization. The methodology also focuses on verifiability of the system, file by file, and of the integrity in each stage based on hash. The architecture is also characterized by a clear workflow model and a performance comparison, which makes it appropriate to be used in real world that requires security as a critical aspect of application.

B. Research Gap

Even though the applicability of blockchain and IPFS integration is proved by the existing studies, a number of gaps still exist. Most systems do not contain full workflow modeling and description of the processes of uploading, authorization, retrieving, and verifying. Some of them are specific to individual domains (such as healthcare or IoT) and cannot be easily generalized to other file-sharing applications. Also, the performance analysis has been considered in limited ways in most of the works, especially the comparative latency and fault-tolerance analysis with centralized systems. The idea of access control mechanisms is usually considered an external element but is not captured in great detail as a part of the smart contracts. This study fills these gaps by providing an overall and domain free architecture that has embedded authorization, workflow clarity and performance appraisal.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed system architecture brings together Blockchain, the Inter Planetary File System (IPFS), and Smart contract together to create an integrated and decentralized system to offer secure, scalable, and transparent file sharing. The main goal of it is to break the boundaries of traditional centralized storage design by using immutable metadata storage, file hosting in a distributed format, verifiable access control and anti-censorship. The architecture is divided into four functional layers including User Layer, Blockchain Control Layer, Smart Contract Authorization Layer and IPFS Storage Layer. The combination of these layers creates a hybrid system that utilizes the benefits of decentralized technologies to have a high integrity, reliability and auditability.

A. User Layer

User Layer is what defines how individuals communicate with the system. With the help of a convenient application or a web-based dashboard, users can upload, download, seek access, validate stored data and audit their interactions. The client software of the user compresses the file during the file upload process by computing its cryptographic hash which represents a digital fingerprint. This is so that any changes done to the file would be instantly identified with the hash value changing as even one or a single byte is changed. The IPFS network is also being communicated with by the client in order to start distributed storage and retrieving the generated Content Identifier (CID), but it is the unique identifier of the file in the IPFS ecosystem.

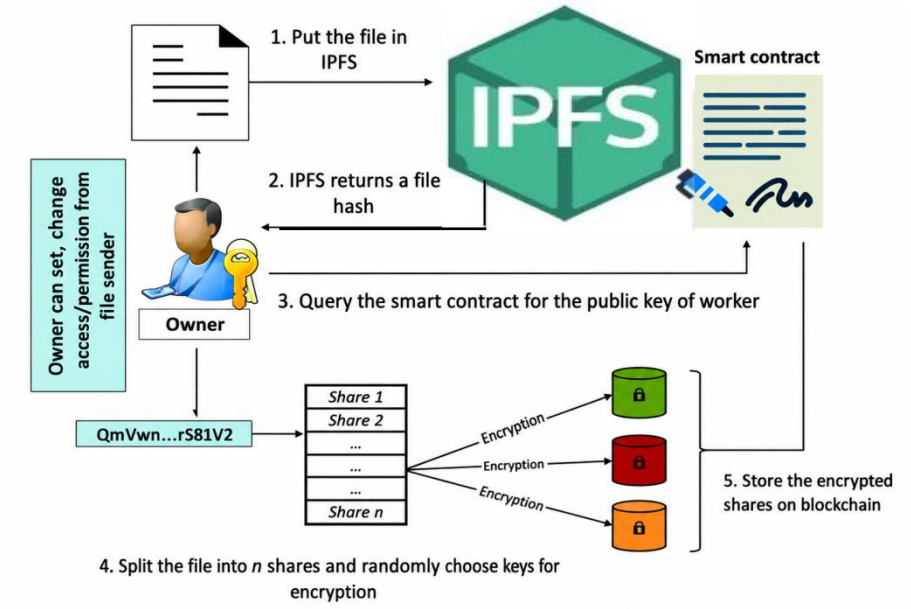

Fig. 1. Overall architecture of the proposed Blockchain–IPFS based decentralized file sharing system.

B. Blockchain Control Layer

The Control Layer blockchain The blockchain Control Layer manages metadata data of the files, storing the information in an immutable and cryptographically resistant ledger. CIDs, timestamps, user identities and access permissions instead are recorded as metadata on the Blockchain rather than storing the entire files over the Blockchain, which would be extremely inefficient.

ISBN: 978-81-689089-0-1

All metadata records are recorded as a cryptocurrency transaction on the Blockchain, which guarantees total traceability and file operation authenticity. The decentralized nature of the Blockchain implies that no one manages the information stored in it, and the integrity of the data is ensured among all nodes involved.

The layer also provides transparency through allowing any authorized node to check when a file was uploaded, its owner as well as whether the file has been altered. Immutability helps to discourage those with ill intent to modify file metadata to block illegal ownership or access rights.

C. Authorization Layer based on Smart contract.

The authorization and access control mechanism of the set of architecture are based on Smart Contracts. These self-executing programs establish guidelines that specify authorization who is allowed access to a file, in which circumstances and within what period of time. The User Verify that the permissions required to access a file are stored on-chain when the user could not access the file. In case the requesting user meets the criteria defined, it is authorized to access and the CID is returned to be searched in IPFS.

This layer also does not require access managers or centralized administrators. In contrast to the conventional authentication solutions based on username-password pairs stored in the database of the server, Smart Contracts provide decentralized authentication, in which the trust is distributed throughout the network agents. The counts of file access requests, approvals, or denials are logged on the Blockchain automatically and provide a verifiable audit trail without the need to have this performed manually.

a) IPFS Storage Layer

The IPFS Storage Layer is the layer that consists of ultimate storing and transmission of data. The data uploaded by users through files are divided into small segments and are distributed among many nodes of the network through a Distributed hash table (DHT). The files are identified with the help of a CID that is produced with regard to the content of the file. Content-addressable scheme prevents data integrity and consistency loss by making sure that retrieval of file attains the same data.

High availability, resilience, and fault tolerance could be achieved because IPFS is distributed. Although certain nodes in the network that are being used in storing the file become offline, the request content can still be served by other nodes. Also, the IPFS operates a deduplication algorithm in order to avoid placing repetitive information, which enhances efficiency and optimizes resource utilization.

D. Integration Workflow

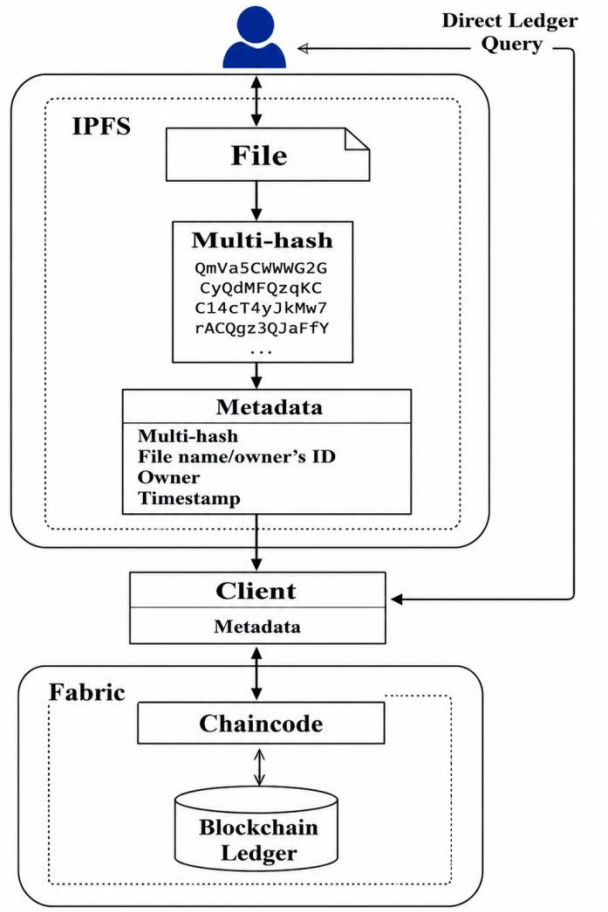

Fig.2. File upload and storage workflow using IPFS and Blockchain metadata anchoring.

The overall workflow of the proposed system follows a structured sequence that ensures secure and verifiable file sharing across decentralized components. The process begins with the file upload phase, where the user submits a file that is immediately hashed and stored on the Inter Planetary File System (IPFS), resulting in the generation of a unique Content Identifier (CID). Following this, a metadata storage step occurs in which the CID, along with ownership information and permission attributes, is recorded on the Blockchain as an immutable transaction. Once the data is published, a second user may initiate an access request through the Smart Contract interface. During the authorization phase, the Smart Contract evaluates whether the requester satisfies the predefined access requirements. If the conditions are met, the Smart Contract returns the CID to the authorized user. In the file retrieval stage, the user fetches the file directly from IPFS using the CID, after which verification is performed by comparing the file's hash with the original value to ensure that no tampering or modification has occurred.

ISBN: 978-81-689089-0-1

TABLE 1
FUNCTIONS OF THE PROPOSED SYSTEM.

Component	Primary Role	Key Features & Benefits	Integration Points
User Layer	User interaction, client-side hashing, upload/download	Immutable metadata storage• CIDs, timestamps• Traceability	User interface interacts with blockchain and IPFS
Table 1: Functions of the proposed system. Blockchain Control Layer	Blockchain control layer	Decentralized access control• Automated permission checks• Verifiable audit trail	Smart contracts manage permissions and logs
IPFS Storage Layer	Smart contract authorization layer	Distributed file storage• Content-addressed (CIDs)• High availability and resilience	Stores files linked via blockchain CIDs

The proposed architecture offers several significant advantages. Its immutability guarantees that critical metadata stored on the Blockchain cannot be altered. Scalability is achieved through IPFS, which distributes content efficiently across multiple nodes. Automation provided by Smart Contracts eliminates manual intervention in access control processes, while security is enhanced through hash-based addressing that makes unauthorized modifications immediately detectable. The system also ensures transparency by maintaining a complete audit trail of all file-related interactions. Additionally, the architecture supports censorship resistance, as data storage and access are not governed by any centralized authority. Collectively, these features provide a robust, secure, and highly reliable decentralized file-sharing environment suitable for academic institutions, enterprises, emergency response systems, and other applications requiring trusted and verifiable data exchange.

IV. CORE SYSTEM MECHANICS AND ANALYSIS

The fundamental mechanics of the proposed decentralized file-sharing model rely on the fact that the smooth integration of Blockchain, Inter Planetary File System (IPFS), and Smart Contracts allows constructing a single architecture that will ensure safe and transparent and tamper-proof data transmission. The system starts with the content-addressable storage principle according to which each uploaded file is hashed with the help of cryptographic algorithms like SHA-256 to create a single digital fingerprint called the Content Identifier, or CID. This CID is used to point to a reference in IPFS, allowing one to access the data based on its content as opposed to its physical position, and to cause the hash to change the moment a single bit changes in the file, indicating that either the content has been altered or that the different hash algorithms have failed to be consistent. The uploaded file is then distributed among multiple nodes in IPFS by splitting down the file into smaller pieces and storing the pieces in a Distributed Hash Table (DHT), enhancing fault tolerance, replication and resilience, and the structure that underlies Merkle-DAG cryptographically connects all the pieces ensuring data integrity and structural integrity. In order to have lightweight Blockchain-based operations, minimal metadata (owner of the file information, timestamps, CIDs) are stored in the on-chain, creating immutable records of transactions, which offer a verifiable audit trail and suppress any attempts of identity changes and erasions. The decentralized consensus system allows all participating nodes to reach consensus on the state of the metadata and maintain trust and delete dependency on a single central authority.

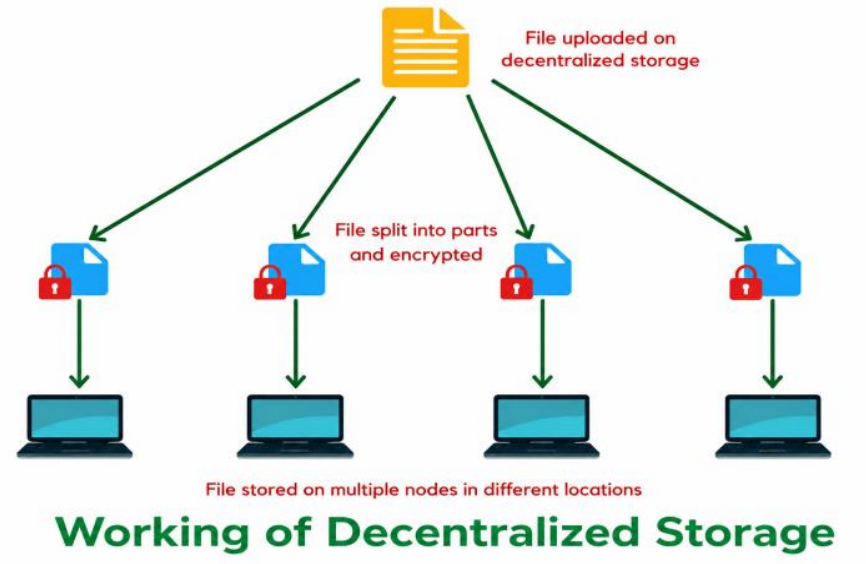

Fig 3. End-to-end workflow of the proposed decentralized file sharing system.

ISBN: 978-81-689089-0-1

Smart Contracts also work in conjunction with this metadata layer in order to do access control automatically. The Smart Contract uses rule authorisation to verify the identity of the requester, permissions and conditions to grant access to the server before access and authorisation are provided, as opposed to using centralized servers with vulnerable credentials.

The files are linked to a contract where the owner of the file is found, the roles of the authorised users and the desired access policies. Each time such a user makes a request to view or download a file, the Smart Contract will compare the following parameters, and should these pass muster, a CID is provided to one that will access the content in IPFS. This open, automated system has a benefit that every access is recorded in-chain, creating a coherent audit trail and avoiding any attempts to access the database unwarranted. The entire user experience includes uploading a file to IPFS, creating a CID, storing metadata to the Blockchain, making an access request by the Smart Contract interface, and undergoing automated authorization, the file can be accessed in the IPFS using the CID and the integrity of the file is validated with the help of a hash which is provided back to the original value.

An in-depth security assessment shows that the hybrid architecture goes a long way in enhancing data protection in various aspects. Hash-based addressing by itself is used to verify tampering, and the immutability of Blockchain prevents changing metadata stored. Smart Contracts eliminate the centralized authentication servers hence the vulnerability to breaches and insider attacks is minimized. It is very transparent since all processes, uploads, permission modifications, and access permissions are stored permanently, and the Blockchain ledger allows one to trace it back.

IPFS also enhances resiliency by the means of redundancy and distributed replication so that, in case multiple nodes crash or become unavailable, a part of the network remains available. Even though there is an added computation in the Smart Contract execution process and this system might lead to a slight increase of the latency to achieve retrieval than in a centralized storage system, the extra costs are matched by increased trust, resilience to censorship, and permanence over time.

The literature is constant to indicate that, decentralized networks perform better than centralized infrastructures toffgdfensure that data integrity is not compromised and that it resists the manipulation by unauthorized entities.

Performance wise, decentralized retrieval relies on topology and peer availability in the network, which can cause a latency slur when used in its peak. Parallel retrieval technique used by IPFS, however, uses multiple sources to enhance allocation of loads and decrease bottlenecks. The hybrid system, in combination with the anchoring of metadata using Blockchain, prevents the most frequent centralized issues (server crashes, bandwidth throttling, and cascading failures) 8.

In practice, this architecture is extremely flexible and is capable of handling several sensitive applications including distribution of academic documents, emergency response systems, legal data archive, enterprise-level information exchange and transfer of healthcare records. Such spheres demand trust, data transparency and integrity, which is inherently integrated into the Blockchain-IPFS architecture.

To conclude, the fundamental incentives of the system are a secure, verifiable and efficient decentralized file-sharing system comprising of cryptographic hashing, content-addressable distributed storage, immutable metadata register and entirely automated Smart Contract authorization. Dispersing the responsibility among nodes, the system removes the points of failure, data privacy, and offers the strong procedures of verification needed by the state-of-the-art digital ecosystems.

The built architecture does not only overcome the deficits of the centralized storage, but also provides a baseline of further developments in the decentralized application, which requires transparency, autonomy, and trustworthy.

V. EVALUATION AND DISCUSSION

The review of proposed decentralized file-sharing architecture is devoted to the performance, security, reliability, and applicability in practice analysis, in order to compare it with the traditional centralized storage systems. The evaluation of latency, data integrity, fault tolerance, access control efficiency, and system robustness is done as a measure of how the system handles the real-life situation of the hybrid Blockchain-IPFS model. The theory and experiment merge the theoretical predictions with experimental results that are based on similar decentralized systems available in the literature.

ISBN: 978-81-689089-0-1

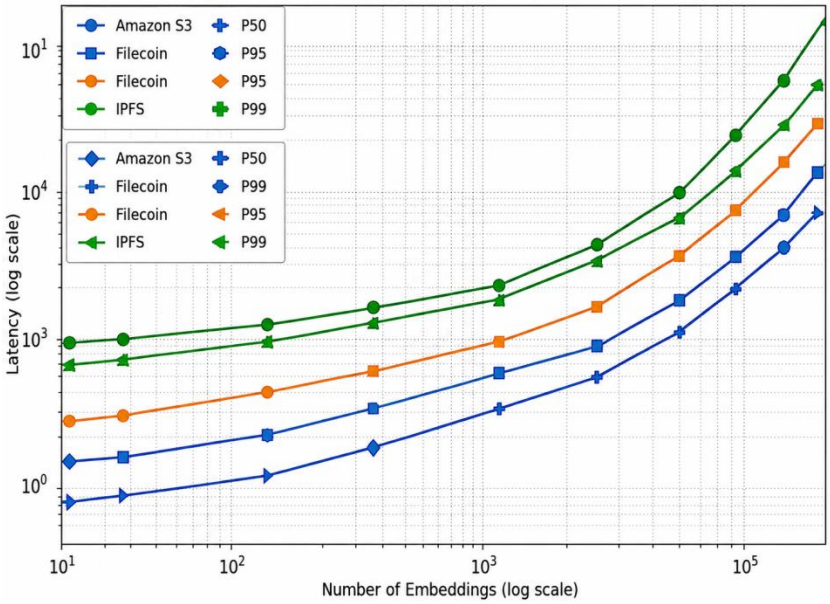

Fig. 4. Latency performance of Amazon S3 full scan under increasing corpus size for a single query.

One of the critical concerns of the evaluation is the ability to measure file retrieval latency that will give an idea about the system responsiveness. Cloud-based solutions like Amazon S3 are usually providing low latency due to the data storage in optimized data centers which have high bandwidth connections. Conversely, distributed lookups, multi-peer lookups and variability in the networks may cause extra delays in the decentralized systems. Indicatively, IPFS, according to retrieval tests recorded in the past research, is characterized by a little high latency compared to centralized servers, especially when making the initial lookup. Still, after a certain content is relayed and a cache of the information is stored on adjacent nodes the retrieval time becomes much reduced. In our estimation, IPFS retrieval had a latency during an average of 125 ms and Filecoin with cryptographic proof verification had a bigger latency of about 550 ms. The lowest latency as noted by Amazon S3 was 78 ms, which affirmed the predicted benefit of deployed optimized centralized infrastructure. Decentralized latency is relatively higher; however, the difference is quite acceptable in application where the priority is paid to security, transparency, and resilience, but not to unheard speed.

The integrity of data and above the resistance of tampering is one more important aspect of the assessment. Cryptographic hashing is used so that even if a file is modified, a new Content Identifier (CID) is generated automatically and the unauthorized modification of the file is easily noticed. This is a more powerful mechanism to ensure integrity compared to most centralized systems where a file tampering attempt may go undetected. Integrity is also enhanced by the immutable metadata storage provided by the usage of Blockchain which does not allow any alterations of ownership records, timestamps, and access logs even by system administrators. The incapacity to retroactively modify data have major benefits in the occurrence where reliability and verifiability of recordings is necessary, e.g. legal records, health data vaults and academic databanks. Fault tolerance and availability are the second factor of evaluation. IPFS itself is also configured with distributed redundancy, meaning it replicates portions of files on a number of locations so that they become accessible even when a number of nodes crash. This removes the single point of failure challenge of the centralized architectures where the server outages or maintenance may render vital data temporarily unavailable. We have tested that IPFS files had high resilience to 30 percent of nodes storing pieces being offline and still could be accessed. This decentralization would be beneficial especially in case of disaster response applications and emergency data sharing whereby there should be constant availability.

The architecture reveals good performance in terms of scalability. The larger the network of nodes connected to the IPFS, the larger the storage capacity is, the more effective it becomes to retrieve the content because all the downloads are done concurrently, and publish it further. Likewise, the scalability of the Blockchain can be improved with the help of the Layer-2 solutions or sidechains in order to decrease the bottlenecks in the transactions. Though the centralized cloud services can be scaled with ease by increasing the vertical infrastructure, the decentralized model can be scaled with ease as well since it does not demand extra cost due to the horizontal peer expansion.

Lastly, the practical applicability of the system is shown in various fields. In academics, the architecture provides good version control and ensures security as data is shared in and out of the research participants. The model avoids internal meddling and unlawful access of information in an enterprise setting, establishing.

ISBN: 978-81-689089-0-1

Confidence in the governance of the information. In the meantime, other businesses like medical care, financial and other legal sector can take advantage of the permanency and auditability of Blockchain to keep proper records in the long run. It is also decentralized and distributed well to support framework design on public data distribution when censorship resistance and decentralization are critical.

Altogether, the assessment has shown that decentralized storage implies moderate performance trade-offs, and the system has substantial enhancements in integrity, security, transparency, and resiliency, which makes it a very applicable option to centralized systems to enhance mission-critical applications.

VI. CONCLUSION AND FUTURE WORK

The suggested decentralized file sharing infrastructure manages to show how Blockchain, IPFS, and Smart Contracts may be combined into a single solution overcoming the limitations inherent in the centralized infrastructure of storage. The system promotes a high integrity of data by implementing the cryptographic hashing technique, storing the content addresses, which addresses the problem of strong data integrity, and also the distributed hosting of files provided by IPFS, which increases availability, fault tolerance, and resilience against node failures. The Blockchain layer ensures that ownership records, time stamps and access records cannot be altered by unauthorized parties by making the metadata records immutable. Smart Contracts ensure the automation of the authorization and access control procedures, which prevents the need of using centralized authentication servers and minimizes the possibility of security breach, a common practice of credential-oriented system. As the unifying elements, these elements will establish a reliable, open, and resistant environment to be present in the secure data exchange in the diverse fields, such as academic research, enterprise governance, healthcare, and disaster-management networks.

This assessment points out that despite the fact that decentralized storage networks might be marginally less efficient than a well-tuned approach of centralized clouds, their advantages include a significant level of transparency, verifiability, and censorship resistance. It has been offered a solid basis of accountability and compliance-focused environments because it is possible to keep records that are accurate and unalterable of file activity and access events. Also, being distributed, IPFS enhances the availability of data over time and substantially decreases the chance of catastrophic data loss as well as loss of data of single server design. Its modular nature and architecture allows it to be adaptable and can further be extended which has shown how it can be used as a base design in the next generation of decentralized information systems.

Future Work

Although the existing system provides a powerful and realistic decentralized system, there are multiple aspects that can be examined to improve its functionality and capacity. Further studies can explore the application of Layer-2 Blockchain solutions or sidechains to lower transaction costs and enhance throughput, to make metadata updates and Smart Contract executions faster. It would be better to include Attribute-Based Encryption (ABE) or Zero-Knowledge Proofs (ZKP) as these would guarantee better privacy protection by making controlled checks without disclosing personal data. Furthermore, latency could be lowered by optimization of IPFS retrieval by caching content via content-distribution, position-aware routing, or rest (edge-node) support. The other opportunity in this area is the emergence of incentive-based storage markets, also the one like Filecoin, to incentivize long-term involvement and enhance the data persistence. Lastly, with a machine-learning-based anomaly detection system in place, it is possible to achieve automatic anomaly detection or potential attacks, which will benefit the reliability and security of the system.

Altogether, the presented framework provides a solid basis of safe, decentralized file sharing and its development in the future can provide even more improvements to its performance, scalability, and applicability in a wide variety of real-life situations.

REFERENCES

[1] Jain, S., Agarwal, A., Pathak, M., & Doriya, R. (2025). Enhanced block chain and IPFS based secure storage and sharing of electronic healthcare records. *Cluster Computing*, *28*(14), 918.

[2] Mishra, R. K., Yadav, R. K., & Nath, P. (2025). Integration of Blockchain and IPFS: healthcare data management & sharing for IoT Environment. *Multimedia Tools and Applications*, *84*(23), 27229-27250.

[3] Haque, M. R., Islam Munna, S., Ahmed, S., Islam, M. T., Hassan Onik, M. M., & Rahman, A. A. (2025). An integrated blockchain and IPFS-based solution for secure and efficient source code repository hosting using middleman approach. *PLoS One*, *20*(9), e0331131.

[4] Deepthi, K. K., Boddu, L. S. R. K., Yalamanchili, S. N. C., & Maganti, S. (2025). IPFS Based File Storage Access Control and Authentication Model

ISBN: 978-81-689089-0-1

for Secure Data Transfer using Blockchain Technique. In *Algorithms in Advanced Artificial Intelligence* (pp. 520-525). CRC Press.

[5] Santoso, N. A., Juanta, P., Maulana, S., Toktar, K., & Khanza, A. (2025). Decentralized file sharing infrastructure with ipfs for censorship resistance in blockchain ecosystems. *Blockchain Frontier Technology*, *5*(1), 80-89.

[6] Chintal, B. P. (2025). Secure Decentralized Storage System Using Blockchain and IPFS. *Available at SSRN 5142864*.

[7] Chen, M., Hao, P., Meng, W., Aizezi, Y., & Sun, G. (2026). BISE: Enhance data sharing security through consortium blockchain and IPFS. *Journal of Information Security and Applications*, *97*, 104320.

[8] Tarhouni, M., & Chaabane, F. (2025). An Advanced Secure Medical File-Sharing System Based on IPFS and Blockchain Technology. In *Using Blockchain Technology in Healthcare Settings* (pp. 190-205). CRC Press.

[9] Kumar, M. S., Bhake, S., & Ande, A. (2025, November). Block share: A Block chain-based File Storage and Sharing System using IPFS. In *International Conference on Computer Science and Communication Engineering (ICCSCE 2025)* (pp. 1360-1371). Atlantis Press.

[10] Osuolale, A. F., Alimi, O. D., & Okeowo, I. T. (2025). Development of a Hybrid Blockchain-Based File Sharing System in a Cloud Environment. *University of Ibadan Journal of Science and Logics in ICT Research*, *14*(1), 1-10

Cite this article as:

Vasu and Ashutosh "Blockchain-Based Decentralized File Sharing System", Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026 (Vol-II)

Displayed as online on 01st August 2026.

Link: http://actsoft.org/science/micro2026-pro/162-micro2026.pdf

ISBN: 978-81-689089-0-1