International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4781-4787
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0628

Tamperproof File Replication for Data Availability for IPFS User

S Gayathri[1], Dr V Mareeswari[2]
[1]PG Scholar, Department of Data Science, AMC Engineering College, Bengaluru, India.
[2]HOD, Department of Computer Science, AMC Engineering College, Bengaluru, India.
Email Id: *gayathrisushan@gmail.com[1], mareesh.prasanna@gmail.com[2]*

Abstract
The increasing dependence on digital information has created a need for storage systems that can provide reliable access, security, and long-term data preservation The Interplanetary File System (IPFS) has emerged as a decentralized storage solution that enables distributed data management without relying on centralized servers. Ensuring consistent file availability in decentralized networks remains a persistent challenge, particularly when participating nodes disconnect or voluntarily withdraw previously stored content. This study proposes a blockchain-assisted file replication framework aimed at enhancing data availability while protecting stored content from unauthorized modification. In the proposed system, files are distributed across the Interplanetary File System (IPFS) and identified through unique Content Identifiers (CIDs). File metadata and replica status are recorded on a blockchain via smart contracts, establishing a transparent and tamper-evident audit trail for all storage activities. Replicas are strategically distributed across multiple storage nodes to improve data persistence and fault tolerance. Smart contracts serve as the core automation layer, handling replica verification, health monitoring, and lifecycle management — significantly reducing reliance on centralized oversight. Cryptographic hash validation further strengthens data integrity by enabling detection of unauthorized alterations at the file level. Experimental evaluation confirms that the proposed framework improves file accessibility, optimizes replica distribution, and enhances overall system resilience under conditions of node failure and network disruption.
Keywords: *IPFS; Blockchain; Decentralized Storage; Smart Contracts; Arweave-Inspired Replication; Distributed Systems.*

1. Introduction
The Storage architecture, retrieval efficiency, and large-scale data management all face significant difficulties because of the exponential growth of digital data generated by contemporary software systems. Due to their cross-platform accessibility, scalability, and flexibility, centralized cloud storage solutions have gained widespread acceptance. However, their reliance on centralized infrastructures opens the door to critical vulnerabilities like service outages, unauthorized access to data, content censorship, and single points of failure. As an alternative that is more resiliant, secure, and transparent, decentralized storage paradigms have sparked growing interest. The Peer-to-peer, content-addressed storage protocol known as the Interplanetary File System (IPFS) uses identifiers created by cryptographic hashing rather than specific server locations. In contrast to conventional location-based addressing, this content-addressing model enables effective content distribution and improves network fault tolerance IPFS lacks native mechanisms to guarantee long-term data persistence despite these architectural advantages. The active participation of storage nodes, which continuously store and serve content throughout the network. Despite these architectural advantages, IPFS lacks native mechanisms for guaranteeing long-term data persistence. File availability is contingent upon active participation of storage nodes that continuously retain and serve content throughout the network. Consequently, when nodes disconnect or purge locally stored files, the associated content risks becoming inaccessible — a risk that intensifies when the number of available replicas is limited Several approaches have been proposed to address this limitation, including incentive-based storage mechanisms, pinning services, and replica management strategies. Although these techniques

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4781-4787
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0628

improve data persistence, they introduce challenges such as higher storage overhead, increased system complexity, dependence on centralized entities, and suboptimal replica placement. Furthermore, the absence of effective verification mechanisms allows malicious or dishonest nodes to falsely claim ownership of file replicas, which can compromise system dependability and reduce trust within the decentralized storage environment. The framework aims to improve file availability by maintaining multiple verified replicas across decentralized storage nodes as shown in Figure 1 Blockchain-Integrated Replication Framework for Secure Data Availability in IPFS Networks.

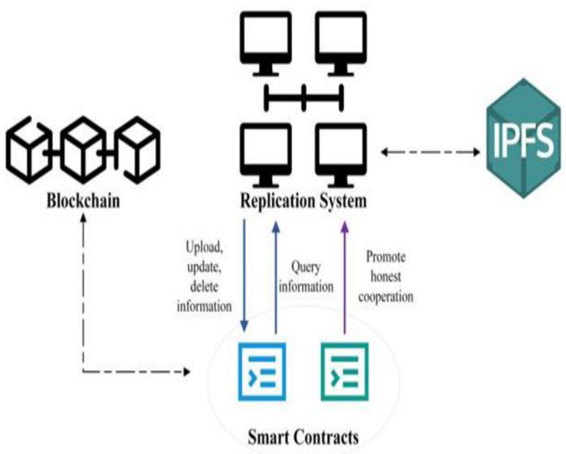

Figure 1 Blockchain-Integrated Replication Framework for Secure Data Availability in IPFS Networks

The overall working of the proposed framework is illustrated in Figure 1, which presents the integration of IPFS, blockchain technology, smart contracts, and replica management mechanisms. As shown in Figure 1, blockchain records are used to ensure transparency and tamper-resistant storage operations. Smart contracts are responsible for verifying replica ownership, monitoring storage commitments, and initiating replication activities automatically, eliminating the need for centralized control.

2. Literature Survey

[1] K. Nair, J. Thomas, and P. Varma (2025) Nair et al. [1] proposed a blockchain-based framework for file integrity verification in decentralized storage systems. Smart contracts are used to validate stored data and maintain immutable audit records. [2] A. Patel and R. Menon (2024) and [5] L. Santos and H. Wu (2024) Patel and Menon [2] developed a scalable IPFS-based decentralized storage framework using blockchain technology, while Santos and Wu [5] presented a survey of decentralized storage platforms such as IPFS and Filecoin. Both studies highlight the importance of data availability, fault tolerance, and efficient replica management. [3] B. Kumar, T. Yoon, and S. Lee (2024) Kumar et al. [3] proposed enhanced access-control mechanisms for blockchain-integrated storage environments. Their approach improves security and prevents unauthorized access to stored data through blockchain-based authentication and authorization methods. However, complex access-control policies may increase management overhead. [4] N. Prakash, M. Shetty, and A. Rahman (2024) and [7] S. Gupta, L. Zhao, and M. D'Souza (2023) Prakash et al. [4] introduced a hybrid encryption model for secure data distribution, whereas Gupta et al. [7] proposed a privacy-preserving blockchain framework for secure data sharing. Both works focus on protecting data confidentiality and integrity in decentralized systems. [6] R. Tan, S. Venkataraman, and M. Park (2024) Tan et al. [6] proposed an adaptive replication strategy for improving reliability in peer-to-peer storage networks. The framework dynamically adjusts replica allocation based on node availability and network conditions.

2.1. Research Gap

The reviewed studies mainly focus on security, access control, encryption, and decentralized storage management. Although some works address replication and availability, limited attention has been given to automated replica verification and intelligent replica allocation. Therefore, this research proposes a blockchain-assisted file replication framework that combines smart contract-based verification with an Arweave-inspired replication strategy to improve data availability, storage reliability, and fault tolerance in IPFS networks.

3. Objectives of the Proposed Work

3.1. Objective 1: Develop a Secure File Replication Framework

The primary objective of this research is to develop a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4781-4787
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0628

decentralized file replication framework that improves data availability in IPFS networks. The framework aims to maintain sufficient replicas of stored files, reduce the risk of data loss, and ensure reliable access to data even when storage nodes become unavailable.

3.1.1. Expected Outcome

The proposed framework is expected to improve file accessibility and storage reliability by maintaining an adequate number of replicas across the network. It also supports balanced utilization of storage resources and enhances overall system stability.

3.2. Objective 2: Implement Smart Contract-Based Verification

The second objective is to establish an automated verification mechanism using smart contracts. The framework verifies whether storage nodes actually maintain the assigned file replicas and records verification results on the blockchain to ensure transparency and trust.

3.2.1. Expected Outcome

The verification mechanism is expected to improve data integrity and prevent false storage claims by participating nodes. It enhances trust among network participants while reducing the need for centralized monitoring and control.

4. Problem Statement

The InterPlanetary File System (IPFS) has gained significant attention as a decentralized storage solution because of its peer-to-peer architecture and content-based addressing mechanism. Despite these advantages, IPFS does not inherently ensure persistent data availability over extended periods. The accessibility of stored content relies on participating nodes continuing to maintain and serve file replicas within the network. If nodes leave the network, encounter failures, or intentionally delete stored data, files with insufficient replication may become inaccessible[8]. Applications like digital archiving that rely on continuous data access face serious concerns due to this limitation. applications for the Internet of Things (IoT), cloud-based storage platforms, enterprise data repositories, and systems to increase file persistence, strategies frequently rely on incentive-based storage solutions or centralized pinning services. Even though these strategies aid in maintaining availability, they may result in increased costs, management complexity, trust dependencies, or constraints on scalability. Additionally, many decentralized storage systems lack efficient methods for determining whether storage nodes the replicas that were given to them, which made it easier for dishonest behavior and made the system's overall reliability less reliable. Therefore, there is a need for a secure and decentralized framework that can automatically manage file replication, verify storage commitments, identify unauthorized modifications, and guarantee the ongoing availability of data without relying on centralized infrastructure. Addressing these challenges can improve the reliability, transparency, and long-term sustainability of IPFS-based storage networks [9].

5. Methodology

The methodology consists of seven phases, including requirement analysis, architecture design, replication management, verification, monitoring, and performance evaluation. The complete workflow of the proposed approach is illustrated in the Methodology Workflow Diagram (Figure 2).

5.1. Followed

A systematic research methodology is adopted in this study to develop, implement, and assess a secure file replication framework for decentralized IPFS storage networks. The overall methodology is divided into seven distinct phases, each contributing to the successful design, deployment, and evaluation of the proposed framework.

Figure 2 **Methodology Workflow**

IRJAEH
International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4781-4787
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0628

As shown in Figure 2 The workflow demonstrates how files are uploaded to IPFS, replicated across nodes, verified through smart contracts, and continuously monitored to maintain availability.

5.2.Phase 1: Requirement Analysis

This phase focuses on studying the limitations of existing IPFS storage systems and identifying the requirements for secure file replication. Problems such as data unavailability, replica loss, and lack of verification mechanisms are analyzed. The scope and objectives of the proposed framework are also defined during this stage.

5.3.Phase 2: System Design

In this phase, the overall architecture of the framework is designed. Different modules such as file upload, replication management, blockchain integration, and monitoring components are identified. Process flow and system interactions are planned to ensure efficient operation.

5.4.Phase 3: Technology Selection

Suitable technologies required for implementation are selected in this phase. IPFS is chosen for decentralized storage, blockchain for immutable record keeping, and smart contracts for automation. Supporting tools and development frameworks are also finalized.

5.5.Phase 4: System Implementation

The proposed framework is developed by integrating IPFS, blockchain, and smart contracts. File upload, CID generation, replica management, verification, and monitoring functionalities are implemented. The individual modules are integrated to form a complete working system.

5.6.Phase 5: Testing and Verification

The implemented system is tested under different operating conditions. File upload, retrieval, replication, and verification processes are validated. The accuracy of replica monitoring and tamper detection mechanisms is also evaluated.

5.7.Phase 6: Deployment

After successful testing, the framework is deployed in a decentralized environment consisting of multiple IPFS nodes. Blockchain services and smart contracts are configured to support real-time storage and verification operations.

5.8.Phase 7: Monitoring and Maintenance

The deployed system is continuously monitored to track replica availability, node activity, and overall performance. Any failures or replica losses are detected and corrected automatically. Periodic maintenance and updates are performed to ensure long-term reliability and efficiency.

6. System Architecture

The architecture of the proposed framework is shown in Figure 3. It consists of multiple layers such as the User Upload Layer, Replication Manager Layer, Smart Contract Layer, Blockchain Ledger Layer, and Monitoring Layer. As illustrated in Figure 3, all replication and verification activities are coordinated through blockchain-enabled smart contracts to ensure secure and decentralized storage management.

6.1.User Interface Layer

This layer allows users to upload, retrieve, and manage files through a decentralized application. It serves as the communication point between users and the storage network.

6.2.File Processing Layer

Uploaded files are checked and prepared before storage. The system generates a unique Content Identifier (CID) for each file and collects metadata required for future verification and retrieval.

6.3.Replication Management Layer

This layer evaluates the availability of stored files and identifies content that requires additional replicas. It distributes replication tasks among suitable storage nodes to maintain balanced data availability.

6.4.Smart Contract Layer

Smart contracts automate important operations such as replica verification, storage validation, and replication management. These contracts reduce manual intervention and improve trust within the network.

6.5.Blockchain Layer

All metadata, verification records, and replication information are stored on the blockchain. This layer provides transparency, immutability, and secure record maintenance.

6.6.Storage Network Layer

The IPFS network stores file replicas across multiple decentralized nodes. This distributed storage approach improves fault tolerance and reduces dependence on any single storage location.

6.7.Monitoring Layer

The monitoring layer continuously observes node activity, replica status, and system performance. It detects failures or missing replicas and initiates corrective actions to maintain data availability. These layers work together to provide secure file storage, automated replication, blockchain-based verification, and continuous monitoring to ensure reliable data availability in IPFS networks.

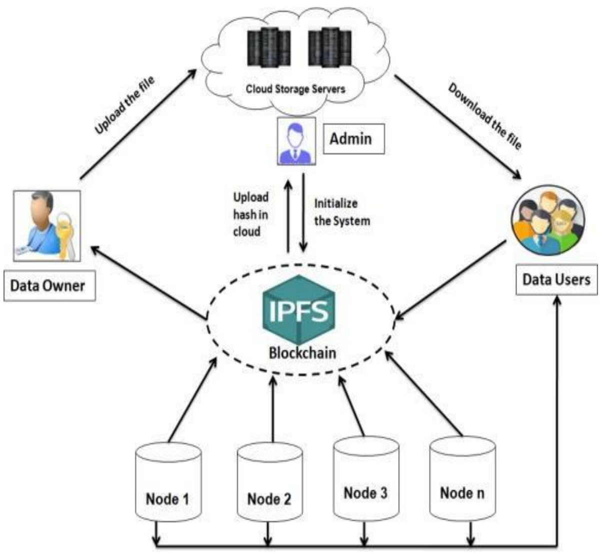

Figure 3 System Architecture of the Proposed Blockchain-Based File Replication Framework

Figure 3. System Architecture Flow Diagram of the Proposed Blockchain-Assisted File Replication Framework consists of seven layers, User Interface Layer, File Processing Layer, Replication Management Layer, Smart Contract Layer, Blockchain Layer, Storage Network Layer, and Monitoring Layer.

7. Implementation

The proposed implementation follows the architectural framework presented in Figure 3. Following the upload of a file, a unique Content Identifier (CID) is created and recorded on the blockchain to support data traceability and integrity verification. The Replication Manager continuously assesses the availability of storage nodes and allocates file replicas based on their respective availability ratings. At the same time, smart contracts oversee the validation of storage commitments, manage replication requirements, and maintain immutable records of all replication activities across the blockchain network, ensuring transparency and accountability throughout the process. A replication mechanism continuously monitors the availability of stored files. When the number of replicas falls below the required threshold, additional copies are automatically created and distributed across suitable storage nodes. Smart contracts manage replica verification and maintain records of storage activities without relying on a centralized authority. To ensure data integrity, the framework periodically compares file hashes with blockchain records. Any mismatch indicates possible tampering, and corrective actions are initiated to restore valid replicas. The system also monitors node status and replica availability, enabling automatic recovery during node failures and ensuring continuous access to stored data.

7.1.Implementation Steps

- Upload file to the IPFS network.
- Generate a unique Content Identifier (CID).
- Store metadata on the blockchain.
- Monitor file availability and replica count.
- Create additional replicas when required.
- Verify replicas using smart contracts.
- Detect tampering through hash validation.
- Perform automatic recovery and monitoring.

8. Results and Discussion

The effectiveness of the proposed framework can be observed from the architecture shown in Figure 2 and the workflow presented in Figure 3. The framework successfully maintained file availability under node failures and peer churn conditions through automated replica management and continuous monitoring. The performance comparison between the traditional IPFS approach and the proposed framework is presented in Table 1. As shown in Table 1, the proposed system provides higher data availability, automated replica verification, improved fault tolerance, enhanced transparency, and better long-term persistence compared to conventional IPFS storage systems. Furthermore, the blockchain-assisted verification process illustrated in Figure 2 enables reliable detection of invalid replicas and strengthens trust among participating nodes. The results summarized in Table 1 confirm that the proposed framework improves overall storage reliability and data accessibility.As shown in Table 1 Comparative analysis between traditional IPFS

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 07 July 2026
Page No: 4781-4787
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0628

storage and the proposed blockchain-assisted replication framework.

8.1.Comparative Analysis

Table 1 Comparative analysis between traditional IPFS storage and the proposed blockchain-assisted replication framework

Parameter	Traditional IPFS	Proposed Framework
Data Availability	Moderate	High
Replica Verification	Not Available	Smart Contract Based
Tamper Detection	Limited	Automatic
Fault Tolerance	Moderate	High
Transparency	Low	High
Replica Management	Manual	Automated
Trust Mechanism	Peer-Based	Blockchain-Based

Conclusion

The proposed blockchain-assisted file replication framework, illustrated in Figure 1 and Figure 2, provides an effective solution for improving data availability in decentralized storage environments. The comparative results shown in Table 1 demonstrate significant improvements in reliability, transparency, and fault tolerance over traditional IPFS-based storage systems. The integration of smart contracts, automated replication, and blockchain verification contribute to secure and dependable long-term data preservation.

Future Work

- Study of smart algorithms are used to find trustworthy storage nodes and make better decisions about how replicas are made. dispersed throughout the network.
- Create adaptable replication policies that can automatically adjust to changes in storage demand and network activity.
- Examine better methods for determining whether stored data has been altered and who holds each replica. AI Content Detection in DrillBit ID of the submission: 6201423 Report on AI Content Detection ID of the submission: 6201423
- Make the framework adaptable so that it can function on a variety of blockchain platforms and decentralized storage networks.
- Check the system's performance in real-world environments like cloud services, enterprise systems, and Internet of Things applications.

Research Contributions

- Designed a decentralized file replication model to improve data availability in IPFS storage networks.
- Introduced a priority-based replica allocation approach that focuses on files with lower availability.
- Implemented an automated verification process using blockchain and smart contracts to validate storage commitments.
- Developed a mechanism for detecting unauthorized data modifications through cryptographic hash comparison.
- This study proposes a blockchain-enabled file replication framework for decentralized storage systems. By incorporating replica monitoring, automatic recovery processes, and decentralized management of replication records, the framework strengthens storage reliability.

References

[1]. K. Nair, J. Thomas, and P. Varma, “Distributed file integrity verification using smart-contract automation,” IEEE Trans. Dependable Secure Comput., vol. 22, no. 1, pp. 312–324, Jan. 2025.
[2]. A. Patel and R. Menon, “A scalable blockchain-based framework for secure decentralized storage using IPFS,” IEEE Access, vol. 12, pp. 118423–118435, 2024.
[3]. B. Kumar, T. Yoon, and S. Lee, “Enhanced access-control mechanisms for blockchain-integrated storage systems,” IEEE Internet Things J., vol. 11, no. 4, pp. 7891–7903, Feb. 2024.
[4]. N. Prakash, M. Shetty, and A. Rahman, “A hybrid encryption model for secure data

distribution in decentralized networks," IEEE Trans. Inf. Forensics Security, vol. 19, pp. 2041–2054, 2024.

[5]. L. Santos and H. Wu, "A survey on decentralized storage technologies: IPFS, Filecoin, and next generation systems," IEEE Commun. Surveys Tuts., vol. 25, no. 3, pp. 1121–1150, 3rd Quart., 2024.

[6]. R. Tan, S. Venkataraman, and M. Park, "Improving reliability in peer-to-peer networks via adaptive replication strategies," IEEE Trans. Parallel Distrib. Syst., vol. 35, no. 2, pp. 455–468, Feb. 2024.

[7]. S. Gupta, L. Zhao, and M. D'Souza, "Privacy-preserving data sharing in healthcare using federated blockchain," in Proc. IEEE Int. Conf. Blockchain (Blockchain), 2023, pp. 441–449.

[8]. T. Lin, O. Pereira, and J. Ko, "Optimizing data replication in peer-to-peer storage networks using AI driven prediction," in Proc. IEEE/ACM Int. Symp., 2023, pp. 621–629.

[9]. N. Raddatz, J. Coyne, P. Menard, and R. E. Crossler, "Becoming a blockchain user: Understanding consumers' ,Eur. J. Inf. Syst., vol. 32, no. 2, pp. 287–314, 2023. [10] N. Lambert and B. Bollen, (Maidsafe, Ayrshire, UK). The SAFE Network: A New Decentralised Internet. (2014). Accessed: Dec. 19, 2023.