Blockchain Frontier Technology (B-Front)
Vol. 5, No. 2, 2026, pp. 124∼135
E-ISSN: 2808-0009 P-ISSN: 2808-0831, DOI:10.34306

Utilizing IPFS for Decentralized Data Storage a Security and Censorship Resistance Solution

Herman[1], Willya Achmad[2], Nur Aulia Lindzani[3*], Suca Rusdian[4], Thomas Green[5]
[1]Department of English Education, University of HKBP Nommensen Pematangsiantar, Indonesia
[2]Department of Social and Political Sciences, University of Pasundan, Indonesia
[3]Faculty of Economic and Business, University of Raharja, Indonesia
[4]Department of Management, STIE Yasa Anggana Garut, Indonesia
[5]Faculty of Economic and Business, Eesp Incorporation, British Indian Ocean Territory
[1]herman@uhnp.ac.id, [2]willyaachmad@unpas.ac.id, [3]nur.aulia@raharja.info, [4]sucarusdian@stieyasaanggana.ac.id [5]thom.green@eesp.io
***Corresponding Author**

Article Info

Article history:

Submission, 07-08-2025
Revised, 21-10-2025
Accepted, 07-11-2025

Keywords:

IPFS
Decentralized Storage
Blockchain
Data Security
Smart Contract

ABSTRACT

This study explores the InterPlanetary File System (IPFS) as a decentralized storage solution aimed at reducing dependence on centralized cloud systems. The **research analyzes** how the integration of IPFS with blockchain and smart contracts can enhance data security, maintain data availability, and minimize censorship risks in digital environments. This topic is relevant because centralized storage still places control in a single point, creating vulnerabilities to cyberattacks, unauthorized access, and failures caused by system dependency. Although several studies have discussed IPFS in different contexts, there is a clear **gap** in the absence of a structured comparative explanation showing how IPFS, blockchain, and smart contracts operate together in decentralized data governance. Using a qualitative literature review from reputable academic sources, this **study synthesizes** existing findings into a clearer conceptual mapping. The **novelty** lies in the development of a comparative matrix that unifies previous technical insights, providing a more accessible understanding of how decentralized technologies support secure and censorship-resistant data ecosystems. The **results** indicate that IPFS preserves data authenticity through cryptographic hashing, improves data availability through distributed replication, and reduces censorship risks because access does not depend on a central authority. However, several challenges remain, including latency, uneven node distribution, and the difficulty of fully removing stored data. Overall, the study concludes that IPFS shows strong potential for future digital infrastructure, yet its adoption requires strategic planning, supportive policies, and gradual implementation to ensure sustainability and operational effectiveness across diverse technological environments

DOI: https://10.34306/bfront.v5i2.896

1. INTRODUCTION

In today's rapidly evolving digital world, data has become one of the most valuable resources across various sectors, including business, government, and daily life [1]. As the volume of internet based activities and technological advancements increase, the need for storage systems that can efficiently handle, manage, and secure large amounts of data has grown substantially [2].

Centralized cloud storage solutions, which rely on servers in a single location, remain among the most widely used options. Services such as Google Drive, Dropbox, and Amazon S3 offer flexibility, integration, and convenient access. However, these systems are not without their drawbacks, such as vulnerabilities to cybersecurity threats, privacy concerns, limited access in case of server failures, and the overbearing control of centralized service providers [3].

To address these challenges, decentralized data storage systems are emerging as a solution [4]. By distributing data across a network of interconnected nodes, these systems reduce reliance on any single point, thus improving security and accessibility [5]. In this model, users act not only as consumers but also as contributors to the storage ecosystem [6].

The IPFS is a widely recognized decentralized storage technology. It operates as an open source, peer to peer protocol that enables the storage and sharing of files using content based addresses rather than their physical location [7]. Every file or its segment is given a distinct cryptographic hash, which enables immediate verification of its authenticity across the network [8].

One of the most popular decentralized data storage systems is the IPFS. An open source peer to peer protocol called IPFS makes it possible to store and distribute files using content addresses rather than physical locations [9]. Each file or file chunk is uniquely identified by a cryptographic hash, which enables realtime data authenticity verification on the network and supports safe and dependable information systems in line with SDGs 16 [7].

This study seeks to evaluate and synthesize the existing research on the IPFS in decentralized cloud storage. By reviewing a range of studies and practical cases, this research aims to explore how IPFS can address key limitations seen in centralized cloud storage, particularly with respect to data security, access availability, and resistance to censorship. Given the growing interest in decentralized technologies, this analysis will be crucial in understanding how IPFS can meet the demands of modern data storage needs [10]. The core focus of this research revolves around three main areas: enhancing data security, ensuring reliable service availability, and combating censorship. With regard to data security, IPFS leverages cryptographic hashing and content based addressing, which guarantees the integrity and authenticity of stored data. In terms of availability, the system's design, which involves replicating data across various nodes, reduces the risks of service outages and enhances overall data accessibility. Additionally, IPFS decentralized structure naturally offers resistance to censorship, as no single authority can control the data stored across the network, protecting the freedom of information.

The goal of this study is to examine and evaluate the corpus of research on IPFS usage in decentralized cloud storage. This study is primarily concerned with data security, service accessibility, and censorship resistance. By comprehending the prospects, challenges, and future directions of IPFS development, this research is anticipated to contribute to SDGs 9 and SDGs 16 by promoting innovation, inclusion, and robust digital institutions. This will help create a more equitable, secure, and transparent data storage system [11].

2. LITERATURE REVIEW

The advancement of decentralized cloud storage through the IPFS emphasizes three essential dimensions. Data Security, Service Availability, and Resistance to Censorship [12]. Over the past few years, various studies have examined both the potential and limitations of IPFS as a foundational technology for decentralized data management and storage ecosystems.

To address the inherent weaknesses of centralized cloud infrastructures—such as privacy concerns, single point failures, and third party control IPFS introduces a peer to peer, content addressed architecture. Unlike traditional storage systems that depend on physical server locations, IPFS distributes and retrieves data based on its cryptographic hash, ensuring data redundancy, authenticity, and independence from centralized authorities [13].

From a security perspective, IPFS utilizes a hash based addressing mechanism that guarantees file immutability and integrity. Each modification to stored data results in a unique hash, allowing the network to verify authenticity automatically [14]. When integrated with blockchain technology, IPFS enhances transparency and immutability by maintaining tamperresistant records. However, studies also highlight ongoing challenges such as limited scalability, inconsistent node distribution, and latency issues that must be resolved for broader deployment [15].

User authentication represents another critical component in decentralized frameworks. In blockchain integrated IPFS environments, digital wallets serve as secure identity verifiers, while two factor authentication (2FA) provides additional security assurance. Despite these innovations, large scale implementation still faces challenges regarding accessibility, interoperability, and usability across diverse user bases [16].

The use of smart contracts provides automation and transparency in managing access control. These self executing agreements define policies for data interaction, such as who can upload, read, or modify files, without relying on centralized intermediaries [17]. This concept aligns with the User Based Access Control (UBAC) model, which empowers users with complete authority and ownership over their digital assets addressing one of the major limitations of conventional cloud storage [18].

Regarding data availability, IPFS ensures persistent access through distributed data replication across multiple nodes. This approach reduces dependency on any single point of failure. Nevertheless, when IPFS nodes are hosted on major commercial clouds, concerns arise over recentralization risks, thereby emphasizing the need for a more equitable and geographically diverse node distribution to preserve the true essence of decentralization [19].

Building on previous studies, the integration of IPFS, blockchain, and smart contracts forms a robust foundation for secure, distributed, and censorship resistant storage infrastructures. Additionally, the emergence of Filecoin as a token based incentive mechanism further promotes long term sustainability by encouraging active participation within decentralized storage ecosystems [20].

Table 1. Synthesis of IPFS Utilization in Decentralized Storage

Research Focus	**Methodology**	**Key Findings**
Blockchain Technology and Data Security	Analysis of blockchain platforms, consensus mechanisms (PoW, PoS), and applied cryptographic models.	Blockchain ensures data immutability, enhances storage integrity, and enables secure access management via smart contracts.
Decentralized Storage Solutions	Comparative evaluation of IPFS and Filecoin frameworks.	IPFS ensures redundancy and global accessibility, while Filecoin incentivizes users to contribute storage capacity, enhancing ecosystem sustainability.
User Authentication in Blockchain Systems	Examination of digital wallet management and 2FA implementations.	Blockchain wallets offer encrypted identity validation, and two factor authentication further strengthens user verification.
Access Control in Decentralized Cloud Systems	Implementation studies utilizing smart contracts for granular data access management.	Smart contracts support transparent and automatic access policies based on user defined preferences.
User Controlled Data Ownership Models	Conceptual analysis of ownership structures and their implications for data privacy and trust.	Decentralized, user centered models increase transparency, enhance privacy, and improve trust in data management systems.

As outlined in Table 1, previous research highlights that the synergy between IPFS, blockchain, and smart contracts contributes significantly to building transparent, secure, and censorship resistant data infrastructures [21]. Blockchain introduces a distributed trust mechanism, while IPFS provides the architectural foundation for efficient peer to peer storage. Meanwhile, smart contracts and authentication systems ensure equitable access control and reinforce privacy preservation [22].

However, despite these advancements, the reviewed literature consistently identifies challenges related to network scalability, infrastructure readiness, and user adoption [23]. Addressing these aspects through ongoing technical refinement and policy development will be vital to achieving sustainable implementation of decentralized storage technologies [24].

3. RESEARCH METHOD

The research methodology used in this study was a qualitative literature review. This approach was selected in order to obtain a thorough grasp of the fundamentals, uses, difficulties, and opportunities associated with IPFS technology in the context of decentralized data storage. It enables the researcher to methodically review earlier research findings, especially those examining how IPFS might be integrated with blockchain and smart contracts. Various scientific articles published in international journals and conference proceedings were among the data sources gathered from reputable academic databases like Google Scholar, IEEE Xplore, SpringerLink, and arXiv [25].

Data security, service availability, and censorship resistance are the three primary topics into which the material was divided using thematic analysis. Every reference was examined according to its study goal (referred to as Method X) and methodological approach (referred to as Method Y). This categorization offered an organized perspective on the evolution and implementation of IPFS in diverse settings. A SOTA Matrix table was then created using the results to help with comparison and to recommend future lines of inquiry [26].

The use of a qualitative literature review does, however, have certain methodological limitations for technical conference settings like IEEE or Scopus indexed venues, which usually highlight innovative technical contributions from simulations, experiments, or prototype implementations. Therefore, in order to enhance its technical contribution, future research should strive to incorporate empirical validation or system level experiments, even though this study provides conceptual and analytical insights [27].

Table 2. SOTA Matrix of IPFS Based Decentralized Storage Studies

Title / Reference	**Method (X) Result (Y)**	**Novelty**	**Future Direction**
Blockchain Based Decentralize Architecture for Cloud Storage	X: System architecture and cloud storage evaluation. Y: Integration of blockchain and IPFS for secured access management.	Enhanced blockchain IPFS security model.	Implementation in realtime enterprise environments.
Decentralized Secure Storage of Medical Records	X: Comparative approach between traditional and decentralized models. Y: Demonstration of IPFS in medical data protection.	Decentralized framework for healthcare data.	Development of healthcare focused decentralized applications.
Toward Decentralized Cloud Storage with IPFS	X: Literature based analysis. Y: Assessment of IPFS scalability and constraints.	Comprehensive study of IPFS limitations.	Address technical adoption and infrastructure readiness.
Lightweight Hash Based De Duplication System	X: Data simulation and performance evaluation. Y: Self detecting chunk mechanism for storage optimization.	Novel duplication algorithm for large scale data.	Integration in real world cloud environments.
Integrated Blockchain IPFS for Code Hosting	X: Prototype development of repository management. Y: "Middleman" model utilizing IPFS and smart contracts.	Secure decentralized DevOps repository framework.	Expand applicability to CI/CD and DevOps systems.
Secure Data Transfer via IPFS and Smart Contracts	X: Case study in construction sector. Y: Implementation of smart contracts for transparent data sharing.	Integration of blockchain IPFS in data integrity assurance.	Extend adoption to broader industrial infrastructure.
Decentralized Document Storage Using IPFS	X: Prototype testing for decentralized file management. Y: Implementation of public ready IPFS based document storage.	Improved data security and user transparency.	Enhance usability and scalability for large scale adoption.

Using the SOTA Matrix table, numerous research have looked at the combination of IPFS and blockchain for decentralized data storage. For example, according to Table 2, the concept applies to sensitive healthcare

data while emphasizing architectural design for larger cloud systems. These tests demonstrate how merging blockchain technology with IPFS may improve security and user control. Meanwhile, an evaluation of IPFS highlights technical issues like scalability and uneven node deployment and calls for further research to overcome these infrastructure gaps so that adoption can increase [28].

Some research indicate lightweight hash based de duplication techniques as a technical optimization to increase storage efficiency in large scale digital environments. Other study offers a decentralized source code repository approach that offers a safe substitute for version control in software development by combining IPFS and smart contracts in a ”Middleman” architecture [29]. These studies provide fresh perspectives on the potential applications of decentralized technologies to improve data efficiency, control, and redundancy management.

Because IPFS is still a relatively new technology and a synthesis of previous work is necessary to provide a baseline before experimental validation, a literature study was chosen. However, because the analysis is based on pre existing data, this approach restricts the originality of empirical findings [30].

In order to overcome this constraint, future studies will incorporate the modeling and prototype implementation of IPFS combined with blockchain for performance evaluation, with a specific emphasis on latency, throughput situations [31].

4. RESULT AND DISCUSSION

The analysis encompasses a diverse body of literature that investigates the implementation of IPFS technology in decentralized cloud storage systems. This exploration focuses on understanding how IPFS contributes to reshaping data storage infrastructures by offering an alternative to centralized models that often suffer from single points of failure and privacy vulnerabilities. Through a synthesis of prior studies, the research highlights the conceptual foundations and technological advancements that make IPFS a viable solution for distributed data management.

The discussion is structured around three central analytical themes: data security, service availability, and censorship resistance. Each theme serves as a crucial benchmark for evaluating the stability, reliability, and transparency of decentralized cloud systems. The emphasis on these dimensions allows for a comprehensive assessment of IPFS performance in addressing challenges that persist in centralized systems, such as unauthorized access, downtime, and control by dominant service providers. The analysis not only identifies the advantages of IPFS but also critically examines the technical trade offs that accompany its adoption. While IPFS offers enhanced data integrity and availability through peer to peer replication and cryptographic verification, it also presents challenges in scalability, latency, and infrastructure management. By comparing these strengths and weaknesses across various implementations, the study underscores that IPFS represents both a technological innovation and a strategic shift toward more open, resilient, and censorship resistant data ecosystems.

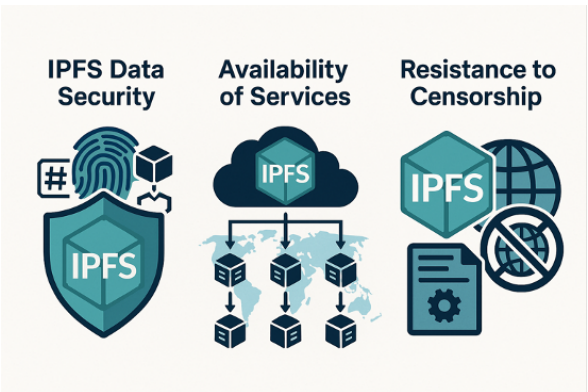

Figure 1. Key Advantages of IPFS in Security, Availability, and Censorship Resistance

Figure 1 illustrates the three main benefits of IPFS, strong resistance to censorship due to its decentralized architecture, continuous data availability through replication across several nodes, and secure data security via cryptographic hashes. As a result, IPFS is a stable and open decentralized data storage option [32].

4.1. IPFS Data Security

The findings of this research highlight that IPFS serves not only as a technological advancement but also as a strategic solution to modern data management challenges. Its decentralized architecture minimizes reliance on centralized systems and promotes user independence, while its content based addressing mechanism ensures the authenticity and reliability of stored data. Moreover, IPFS proves particularly significant in environments where information accessibility and freedom are threatened, thanks to its strong resistance to censorship.

The reviewed literature consistently highlights this synergy as a foundation for tamper proof and transparent data governance frameworks. However, some studies emphasize that this integration also introduces computational overhead and storage redundancy challenges that require optimization for large scale deployments. Hence, while IPFS represents a major advancement in data authenticity and traceability, its long term scalability and processing efficiency remain open research questions requiring further empirical validation [33].

4.2. Availability of Services

Data is stored across several nodes using IPFS's automatic replication technology, which guarantees that data is still available even in the event that some nodes go down. Multiple node IPFS systems have been shown in tests to be able to avoid the complete failures that frequently happen in centralized cloud systems [34].

Furthermore, even in areas lacking extensive cloud infrastructure, data availability is increased by the worldwide spread of IPFS nodes [35]. As more IPFS nodes are dispersed over nations and areas, there is a greater chance to create a reliable and user friendly storage system [36].

Nevertheless, there are performance trade off associated with this availability benefit [37]. IPFS's distributed architecture can present serious issues with latency and data retrieval speed, according to the research, especially those cited by Doan et al. IPFS must carry out content discovery over a network of peers, in contrast to centralized systems where data location is known [38]. Variable latency may arise from this procedure, particularly for data that is not frequently replicated across numerous nodes or is not popular [39]. A significant obstacle to IPFS adoption in applications that require immediate or fast data access, like real time video streaming or high frequency data transactions, is this practical performance constraint [40].

4.3. Resistance to Censorship

The decentralized nature of IPFS allows it to operate without reliance on a single centralized server or domain, making it inherently resistant to censorship, data deletion, or access restrictions [41]. By distributing files across a vast peer to peer network, IPFS ensures that information remains retrievable even when individual nodes are offline or blocked. Several real world implementations have demonstrated its ability to bypass government imposed internet restrictions by creating alternative data access routes, thus maintaining the free flow of information across the digital ecosystem [42].

Despite these advantages, existing literature highlights the challenges of recentralization. When the majority of IPFS nodes are hosted on dominant commercial cloud providers, such as AWS or Google Cloud, the principle of decentralization can be undermined. This reliance risks reintroducing vulnerabilities to censorship, as these providers may still comply with external regulations or content removal requests. Researchers warn that such infrastructure concentration could transform a theoretically open network into one that exhibits the same vulnerabilities as centralized storage systems.

To solve this problem, a recent study proposed an incentive based framework that encourages broader participation in the IPFS ecosystem. One notable example is Filecoin, which rewards individuals and small organizations for providing storage capacity, encouraging a more diverse and resilient distribution of nodes. This mechanism aims to democratize data storage and minimize dependence on major service providers. However, the practical effectiveness of such incentives in achieving longterm decentralization and combating censorship remains an important area for further research, particularly in understanding the economic sustainability and dynamics of user engagement in distributed storage networks [43].

4.4. Interpretation and Discussion

Collectively studies illustrate that IPFS is not merely a technological innovation but a strategic transformation in how modern data management is conceptualized. As a decentralized framework, IPFS minimizes reliance on central authorities and enhances user autonomy. Through content based addressing, it ensures

data integrity and traceability across distributed systems, making it a significant advancement over traditional centralized models [44].

The findings of this research reaffirm that IPFS functions both as a technical breakthrough and as a strategic response to the growing challenges of digital data governance. By eliminating dependence on centralized servers, IPFS empowers users to maintain control over their information while ensuring transparency in data transactions. Its decentralized nature aligns well with the evolving demand for secure and open data ecosystems that promote collaboration without compromising integrity.

In contexts where information freedom is at risk, IPFS demonstrates exceptional relevance due to its inherent resistance to censorship. By distributing data across multiple nodes globally, it allows users to access and share content even under restrictive environments. This characteristic positions IPFS as a key enabler of digital resilience, supporting the free flow of information while mitigating risks associated with centralized control or political influence.

Beyond these strengths, a deeper comparative review of the literature uncovers both complementary and divergent perspectives among existing studies. Some researchers advocate for large scale architectural integration to achieve enterprise grade efficiency, while others focus on lightweight, modular implementations tailored for specific applications. These varying priorities underscore the need for future research to explore hybrid models that balance scalability, performance, and adaptability in decentralized data management systems.

Table 3. Simplified Comparison of Selected IPFS Based Studies

Study	Main Focus	Strengths	Weaknesses
[45]	Blockchain integrated cloud architecture	Secure design for enterprise systems	Lacks implementation and scalability testing
[46]	IPFS and smart contract "Middleman" model	Flexible and transparent for development use	Limited for large scale deployment
[47]	Review of IPFS challenges and opportunities	Identifies key technical issues	Offers little empirical validation

A range of concentration throughout the literature is revealed by the comparative analysis in Table 3. Emphasize architectural integration as a way to accomplish both security and functionality [48]. Studies like the one by Doan et al, on the other hand, are more grounded and demonstrate how network performance causes adoption barriers in the real world. They raise the crucial point that unless a global solution to data retrieval latency is found, IPFS's potential benefits will be difficult to realize in speed sensitive commercial applications. Future research ought to concentrate on this important discrepancy between excellent architectural design and useful functionality.

These opposing strategies show that user accessibility, implementation complexity, and system scalability are all traded off. Future studies should focus on combining these advantages using hybrid frameworks that combine effective and modular designs appropriate for a range of use cases with strong enterprise level security [49].

A thorough examination of the body of extant material also reveals a basic conflict between the practical reality of infrastructure dependency and the theoretical promise of IPFS's resistance to censorship. Despite the intrinsic decentralization of the IPFS architecture, the deployment of its nodes has a significant impact on how effective it is in practice. If node centralization is not proactively addressed, its censorship resistance may become more of a theoretical idea than a real world assurance [50]. Therefore, to ensure sustainable decentralization, future research should seek to simulate the economic consequences of incentive systems and community driven deployment tactics in addition to focusing on prototype validation [51].

It's also crucial to remember that this study's Results and Discussion section mostly summarizes previous research rather than offering brand new empirical data [52]. This method lacks direct experimental validation, yet offering insightful conceptual information [53]. Future research could properly evaluate the performance and scalability of IPFS based systems using comparing simulations, prototype assessments, or

empirical testing to bolster the technical and critical depth.

5. MANAGERIAL IMPLICATION

The decision to implement the IPFS should be viewed as a strategic organizational initiative rather than a simple technical deployment. The transition to decentralized storage influences how an organization allocates budgets, structures its teams, and enforces data governance. Therefore, managers need to assess organizational readiness and understand the changes that accompany this technology.

5.1. A shift in investment and the need for specialized skills

IT managers need to understand that typical IT teams cannot handle the implementation of IPFS combined with blockchain. Employers will have to spend money on people with specific expertise, such blockchain coders, smart contract auditors (for security), and DevOps engineers with knowledge of decentralized systems. Expenses are shifted from capital expenditures (CapEx) on servers that are unavailable to continuous operational expenditures (OpEx) for node maintenance, network incentive fees (like Filecoin), or the use of third party pinning services under this model.

5.2. Performance and availability are traded of

While IPFS enhances data availability by eliminating dependence on a single central server, performance may vary depending on node distribution. Retrieving files through a peer to peer network can take longer, especially when nodes are located across multiple geographical regions. Additionally, maintaining high availability requires storing multiple copies of data, which increases redundancy related costs. Operational leaders must weigh the organization's tolerance for slower retrieval times against the benefits of higher system resilience and failover capability.

5.3. A paradigm shift in compliance and data governance

The adoption of the IPFS complex implications for regulatory compliance and organizational data governance. Unlike centralized storage, where data remains within a controlled infrastructure, IPFS disperses content across multiple independent nodes, forming a persistent and redundant network. Once information is distributed, removing or altering it becomes technically impractical. This creates inherent tension with data protection frameworks most notably the General Data Protection Regulation (GDPR) that guarantee individuals the legal right to request erasure of personal data. Therefore, organizations must reconsider their data handling principles, especially when dealing with confidential, sensitive, or legally protected information.

To mitigate exposure to regulatory violations, governance mechanisms must be embedded at the earliest stages of IPFS adoption. This requires close coordination between legal, cybersecurity, and compliance units to develop preventive safeguards. Practical measures may include encrypting data prior to distribution, implementing selective pinning practices to control the persistence of stored files, and employing hybrid architectures that place sensitive information on managed repositories while leveraging IPFS for public or non regulated content. Through these strategies, organizations maintain control over the lifecycle of stored data while still benefiting from decentralization.

Integrating IPFS within institutional workflows is not merely a technical enhancement it demands a reorientation of organizational structures and decision making processes. Shifting from a centralized authority model to decentralized data governance involves reallocating budgets, redefining internal performance indicators, and revising accountability frameworks. This paradigm shift requires organizations to accept a shared responsibility model, where control is distributed rather than concentrated. If approached strategically, IPFS enables institutions to achieve long term resilience, transparency, and sustainability in digital information management.

6. CONCLUSION

This study concludes that the IPFS presents a strong alternative to centralized cloud storage, particularly in addressing critical issues such as data security, service availability, and censorship resistance. By applying a qualitative literature review, the findings demonstrate that IPFS enables content based addressing supported by cryptographic hashes, ensuring data integrity and authenticity across distributed storage nodes.

When combined with blockchain and smart contracts, IPFS strengthens decentralized data governance by enabling immutable records and automated access control.

Furthermore, the adoption of IPFS significantly improves service availability because data replication across multiple nodes eliminates the risks of single point failures commonly found in traditional cloud systems. The decentralized architecture ensures that content remains accessible even when some nodes are offline or subject to external interference. In censorship sensitive environments, IPFS shows superiority by maintaining information accessibility regardless of network restrictions, which supports the principle of information freedom and aligns with global demands for transparent data ecosystems

Nevertheless, several challenges must be addressed before large scale adoption becomes feasible. The literature indicates obstacles related to network latency, uneven node distribution, and compliance issues with data deletion regulations. Future studies should therefore focus on prototype implementation and performance testing to assess real world effectiveness, especially in large scale or enterprise environments. With continuous refinement and broader adoption efforts, IPFS has the potential to serve as the backbone of future decentralized and censorship resistant digital ecosystems.

7. DECLARATIONS

7.1. About Authors

Herman (HH) https://orcid.org/0000-0001-6818-5142

Wilya Achmad (WA) https://orcid.org/0009-0003-0900-1181

Nur Aulia Lindzani (NA) https://orcid.org/0009-0006-0182-7773

Suca Rusdian (SR) https://orcid.org/0009-0008-4805-1524

Thomas Green (TG) https://orcid.org/0009-0001-7048-2231

7.2. Author Contributions

Conceptualization: WA, NA, and SR; Methodology: TG; Software: HH; Validation: WA and NA; Formal Analysis: TG and HH; Investigation: WA; Resources: NA; Data Curation: TG; Writing Original Draft Preparation: WA and SR; Writing Review and Editing: TG; Visualization: WA; All authors, HH, WA, NA, SR and TG, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] R. Vadisetty, "Efficient large-scale data based on cloud framework using critical influences on financial landscape," in *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)*. IEEE, 2024, pp. 1–6.

[2] M. Alqaraleh, "Enhancing internet-based resource discovery: The efficacy of distributed quadtree overlay," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. IEEE, 2024, pp. 1619–1628.

[3] F. Yang, Z. Ding, Y. Yu, and Y. Sun, "Interaction mechanism between blockchain and ipfs," *Blockchain*, vol. 1, no. 2, pp. 24–25, 2023.

[4] D. Surya, D. Setiawan, Y. A. Aryani, T. Arifin *et al.*, "Cyberattacks on the accounting profession: a literatur review," *Media Riset Akuntansi, Auditing & Informasi*, vol. 24, no. 2, pp. 255–272, 2024.

[5] P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, and N. N. Xiong, "Ppsf: A privacy-preserving and secure framework using blockchain-based machine-learning for iot-driven smart cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326–2341, 2021.

[6] B. Singh, "Cherish data privacy and human rights in the digital age: Harmonizing innovation and individual autonomy," in *Balancing human rights, social responsibility, and digital ethics*. IGI Global, 2024, pp. 199–226.

[7] G. Ha, C. Jia, X. Ge, Y. Chen, and X. Shan, "Similarity-aware defense scheme for online brute-force attacks in encrypted deduplication," *IEEE Transactions on Dependable and Secure Computing*, 2025.

[8] K. F. P. Oganda, N. Lyraa, and G. Jacqueline, "Harnessing economic opportunities: Business and blockchain technology introduction for communities," *Blockchain Frontier Technology*, vol. 3, no. 2, pp. 144–149, 2024.

[9] M. R. Haque, S. I. Munna, S. Ahmed, M. T. Islam, M. M. H. Onik, and A. Rahman, "An integrated blockchain and ipfs solution for secure and efficient source code repository hosting using middleman approach," *arXiv preprint arXiv:2409.14530*, 2024.

[10] S. Ahmed, "Enhancing data security and transparency: The role of blockchain in decentralized systems," *International Journal of Advanced Engineering, Management and Science*, vol. 11, no. 1, p. 593258, 2025.

[11] S. Millah, A. Waskito, E. A. Natalia, S. H. Lase, and M. Rodriguez, "Decentralized solutions for intellectual property security using the interplanetary file system," *Blockchain Frontier Technology*, vol. 5, no. 1, pp. 49–59, 2025.

[12] H. Zang, H. Kim, and J. Kim, "Blockchain-based decentralized storage design for data confidence over cloud-native edge infrastructure," *IEEE Access*, vol. 12, pp. 50 083–50 099, 2024.

[13] J.-T. Lou, S. A. Bhat, and N.-F. Huang, "Blockchain-based privacy-preserving data-sharing framework using proxy re-encryption scheme and interplanetary file system," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2415–2437, 2023.

[14] M. S. Irfan, A. Asghar, A. Khan, and E. D. A. R. Chishti, "The file integrity checker using blockchain: A review: A review," *Journal of Emerging Technology and Digital Transformation*, vol. 4, no. 1, pp. 114–126, 2025.

[15] R. K. Mishra, R. K. Yadav, and P. Nath, "Integration of blockchain and ipfs: healthcare data management & sharing for iot environment," *Multimedia Tools and Applications*, vol. 84, no. 23, pp. 27 229–27 250, 2025.

[16] M. Mahmud, M. S. H. Sohan, S. Reno, M. B. Sikder, and F. S. Hossain, "Advancements in scalability of blockchain infrastructure through ipfs and dual blockchain methodology," *The Journal of Supercomputing*, vol. 80, no. 6, pp. 8383–8405, 2024.

[17] L. Franke, H. Liang, S. Farzanehpour, A. Brantly, J. C. Davis, and C. Brown, "An exploratory mixed-methods study on general data protection regulation (gdpr) compliance in open-source software," in *Proceedings of the 18th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, 2024, pp. 325–336.

[18] C. Salger, "Decentralized dispute resolution: using blockchain technology and smart contracts in arbitration," *Pepp. Disp. Resol. LJ*, vol. 24, p. 65, 2024.

[19] U. Rahardja and Q. Aini, "Analyzing player performance metrics for rank prediction in valorant using random forest: A data-driven approach to skill profiling in the metaverse," *International Journal Research on Metaverse*, vol. 2, no. 2, pp. 102–120, 2025.

[20] C. Gilbert and M. A. Gilbert, "The integration of blockchain technology into database management systems for enhanced security and transparency," *International Research Journal of Advanced Engineering and Science*, vol. 9, no. 4, pp. 316–334, 2024.

[21] Y. Wei, D. Trautwein, Y. Psaras, I. Castro, W. Scott, A. Raman, and G. Tyson, "The eternal tussle: exploring the role of centralization in {IPFS}," in *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*, 2024, pp. 441–454.

[22] J. S. Mole and R. Shaji, "Ethereum blockchain for electronic health records: securing and streamlining patient management," *Frontiers in Medicine*, vol. 11, p. 1434474, 2024.

[23] U. Rahardja, V. Meilinda, R. A. Sunarjo, A. Williams, and S. A. Anjani, "Mapping the information and communication technology research landscape through bibliometric analysis," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2024, pp. 1–8.

[24] M. Boughdiri, T. Abdellatif, and C. G. Guegan, "A systematic literature review on blockchain storage scalability," *IEEE Access*, 2025.
[25] A. Kumar, M. Litterick, and S. Candido, "Efficient verification of a radar soc using formal and simulation-based methods," *arXiv preprint arXiv:2404.15371*, 2024.
[26] S. H. Alsamhi, A. Hawbani, S. Kumar, M. Timilsina, M. Al-Qatf, R. Haque, F. M. Nashwan, L. Zhao, and E. Curry, "Empowering dataspace 4.0: Unveiling promise of decentralized data-sharing," *IEEE Access*, vol. 12, pp. 112 637–112 658, 2024.
[27] S. Mittal and M. Ghosh, "A three-phase framework for secure storage and sharing of healthcare data based on blockchain, ipfs, proxy re-encryption and group communication," *The Journal of Supercomputing*, vol. 80, no. 6, pp. 7955–7992, 2024.
[28] J. Medina and R. Rojas-Cessa, "Ami-chain: A scalable power-metering blockchain with ipfs storage for smart cities," *Internet of Things*, vol. 25, p. 101097, 2024.
[29] H. D. Le, V. T. Truong, and L. B. Le, "Blockchain-empowered metaverse: decentralized crowdsourcing and marketplace for trading machine learning data and models," *IEEE Access*, vol. 12, pp. 68 556–68 572, 2024.
[30] S. Basudan, "Ipfs-blockchain-based delegation model for internet of medical robotics things telesurgery system," *Connection Science*, vol. 36, no. 1, p. 2367549, 2024.
[31] J. Kaur, R. Rani, and N. Kalra, "Attribute-based access control scheme for secure storage and sharing of ehrs using blockchain and ipfs," *Cluster Computing*, vol. 27, no. 1, pp. 1047–1061, 2024.
[32] R. Shi, R. Cheng, B. Han, Y. Cheng, and S. Chen, "A closer look into ipfs: Accessibility, content, and performance," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 8, no. 2, pp. 1–31, 2024.
[33] S. Jadhav, G. Choudhari, M. Bhavik, R. Bura, and V. Bhosale, "A decentralized document storage platform using ipfs with enhanced security," in *2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE, 2024, pp. 1–11.
[34] S. K. Dwivedi, R. Amin, and S. Vollala, "Smart contract and ipfs-based trustworthy secure data storage and device authentication scheme in fog computing environment," *Peer-to-Peer Networking and Applications*, vol. 16, no. 1, pp. 1–21, 2023.
[35] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and ipfs: A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, p. e162, 2021.
[36] N. Mahmoud, H. Abdelkader, and A. Aly, "Brip: Towards a privacy-preserving, trustworthy, and transparent ride-sharing system with semantic matching powered by blockchain and ipfs," *Journal of Network and Computer Applications*, vol. 226, p. 103870, 2024.
[37] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy," *Journal of Parallel and distributed computing*, vol. 164, pp. 152–167, 2022.
[38] D. Trautwein, Y. Wei, Y. Psaras, M. Schubotz, I. Castro, B. Gipp, and G. Tyson, "Ipfs in the fast lane: Accelerating record storage with optimistic provide," in *IEEE INFOCOM 2024-IEEE Conference on Computer Communications*. IEEE, 2024, pp. 1920–1929.
[39] K. Adel, Elhakeem, and M. Marzouk, "Decentralized system for construction projects data management using blockchain and ipfs," *Journal of Civil Engineering and Management*, vol. 29, no. 4, pp. 342–359, 2023.
[40] C. Karapapas, G. C. Polyzos, and C. Patsakis, "What's inside a node? malicious ipfs nodes under the magnifying glass," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2023, pp. 149–162.
[41] A. Sclocchi, A. Favero, and M. Wyart, "A phase transition in diffusion models reveals the hierarchical nature of data," *Proceedings of the National Academy of Sciences*, vol. 122, no. 1, p. e2408799121, 2025.
[42] R. M. Purohit, J. P. Verma, R. Jain, and A. Kumar, "Fedblocks: federated learning and blockchainbased privacy-preserved pioneering framework for iot healthcare using ipfs in web 3.0 era," *Cluster Computing*, vol. 28, no. 2, p. 139, 2025.
[43] Z. Hasan, W. Wiryadi, A. Fadhulrrahman, M. Dimas, and R. D. Al Jabbar, "Regulation of blockchain technology and cryptocurrencies as future challenges in cyber law," *Jurnal Ilmu Hukum dan Tata Negara*, vol. 2, no. 2, 2024. [Online]. Available: https://garuda.kemdiktisaintek.go.id/documents/detail/4350060
[44] M. Jubur, P. Shrestha, and N. Saxena, "An in-depth analysis of password managers and two-factor authen-

tication tools," *ACM Computing Surveys*, vol. 57, no. 5, pp. 1–32, 2025.
[45] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based decentralized architecture for cloud storage system," *Journal of Information Security and Applications*, vol. 62, p. 102970, 2021.
[46] M. R. Haque, S. Islam Munna, S. Ahmed, M. T. Islam, M. M. Hassan Onik, and A. A. Rahman, "An integrated blockchain and ipfs-based solution for secure and efficient source code repository hosting using middleman approach," *PLoS One*, vol. 20, no. 9, p. e0331131, 2025.
[47] T. V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward decentralized cloud storage with ipfs: opportunities, challenges, and future considerations," *IEEE Internet Computing*, vol. 26, no. 6, pp. 7–15, 2022.
[48] V. M. Opanasenko, S. K. Fazilov, O. N. Mirzaev, and S. Sa'dullo ugli Kakharov, "An ensemble approach to face recognition in access control systems," *Journal of Mobile Multimedia*, vol. 20, no. 3, pp. 749–768, 2024.
[49] A. A. Ayare, V. A. Jadhav, M. K. Banatwala, S. V. Changlere, A. Mote, P. Joshi, A. Mr, V. Ms, and M. Banatwala, "A systematic review on blockchain-based framework for storing educational records using interplanetary file system," *Cureus Journals*, vol. 2, no. 1, 2025.
[50] F. Yang, Z. Ding, L. Jia, Y. Sun, and Q. Zhu, "Blockchain-based file replication for data availability of ipfs consumers," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1191–1204, 2024.
[51] D. Cuellar, M. Sallal, and C. Williams, "Bsm-6g: Blockchain-based dynamic spectrum management for 6g networks: addressing interoperability and scalability," *IEEE Access*, vol. 12, pp. 59 643–59 664, 2024.
[52] L. Li, K. Xiong, G. Wang, and J. Shi, "Ai-enhanced security for large-scale kubernetes clusters: Advanced defense and authentication for national cloud infrastructure," *Journal of Theory and Practice of Engineering Science*, vol. 4, no. 12, pp. 33–47, 2024.
[53] G. of Indonesia, "Utilizing ipfs for decentralized data storage as a security and censorship resistance solution," *Ministry of Communications and Informatics of the Republic of Indonesia Technical Report*, vol. 1, no. 1, pp. 1–10, 2025, draft document; accessed 2025-10-30. [Online]. Available: https://www.kominfo.go.id/