APTISI Transactions on Management (ATM)
Vol. 10, No. 1, 2026, pp. 1∼10
E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI:10.33050

Leveraging IPFS for Scalable and Secure Data Storage in Blockchain-Based DApps

Richard Andre Sunarjo[1], Nanda Septiani[2], Dwi Nur Ramadhan[3], Afif Aditya Darmawan[4*], Omar Arif Al-kamari[5]

[1,2,3,4]Faculty of Economy and Business, University of Raharja ,Indonesia
[5]Faculty of Economics and Business, Pandawan Incorporation, New Zealand
[1]richard.sunarjo@raharja.info, [2]nanda.septiani@raharja.info, [3]dwi.nur@raharja.info, [4]afif.aditya@raharja.info,
[5]omar.alarif@pandawan.ac.nzo
***Corresponding Author**

Article Info

Article history:

Received August 22, 2025
Revised December 24, 2025
Accepted December 25, 2025

Keywords:

IPFS
Blockchain
DApp
Data Security
Data Storage

ABSTRACT

The rapid expansion of blockchain-based Decentralized Applications (DApps) has intensified challenges related to scalable, secure, and cost-efficient data storage, as conventional on-chain storage is unsuitable for large data volumes due to high gas costs and performance limitations, while centralized off-chain solutions undermine decentralization and increase security risks. **This study aims** to evaluate the effectiveness of integrating the IPFS as a decentralized storage layer within an Ethereum-based DApp architecture to enhance scalability, data integrity, and operational efficiency. **Using an experimental** systems engineering approach, a fully functional DApp prototype was developed by integrating a React.js frontend, Ethereum smart contracts written in Solidity, and a local IPFS node for off-chain file storage. Empirical performance testing was conducted to measure file upload and retrieval latency, CID (Content Identifier) consistency, smart contract execution time, and gas consumption on the Ethereum testnet. **The results demonstrate** that IPFS integration significantly reduces on-chain storage load while maintaining strong data integrity, as evidenced by 100% CID consistency across all test scenarios. Although upload and retrieval times increased proportionally with file size, the system achieved success rates above 95% with stable performance, while gas costs remained low because only CIDs were recorded on-chain. **These findings** indicate that IPFS provides a scalable, secure, and cost-efficient decentralized storage solution for blockchain-based DApps, enabling the development of more data-intensive and resilient DApps, with future research opportunities focusing on incentive-based pinning mechanisms, advanced encryption, and cross-chain storage integration.

Corresponding Author:

DOI: https://doi.org/10.33050/atm.v10i1.2527

1. INTRODUCTION

The development of blockchain technology has given rise to various digital innovations, including Decentralized Applications (DApps) that offer transparency, security, and decentralization [1]. However, data storage in blockchain systems remains a significant challenge. Most blockchains are only effective at storing

small amounts of data on-chain, while the storage of large payloads such as documents, logs, or multimedia assets introduces severe throughput bottlenecks that restrict network scalability and slow consensus performance [2].

Beyond economic overhead, these constraints are critical for DApps because they reduce the protocol's ability to handle high-volume interactions and degrade the reliability of state updates [3, 4]. Conventional off-chain storage methods worsen the problem by introducing centralized intermediaries that broaden the attack surface, creating single points of compromise that can result in unauthorized tampering, data deletion, or targeted corruption [5]. In addition, remote access latency in centralized repositories can disrupt real-time decentralized workflows, impede multi-node validation processes, and introduce synchronization lags that undermine trust assumptions in distributed environments. These combined bottlenecks demonstrate why current storage approaches are insufficient for DApps and highlight the urgent need for decentralized, high-availability storage solutions [6].

To address these challenges, the InterPlanetary File System (IPFS) emerged as a distributed storage system based on a peer-to-peer protocol that stores data based on its content identity, not its location [7]. IPFS promises higher data integrity, distribution efficiency, and security. Moreover, its architectural characteristics such as content-addressed storage, decentralized replication, and cryptographic verification, not only support IEEE's vision for trustworthy and scalable distributed systems but also align with broader IEEE themes related to secure systems engineering, resilient distributed architectures, and emerging intelligent computational infrastructures [8]. These mechanisms are increasingly relevant in IEEE research areas exploring distributed AI, autonomous decision-making systems, and next-generation computational frameworks designed to operate reliably within heterogeneous, dynamic, and adversarial environments [9, 10].

This research focuses on integrating IPFS into blockchain-based DApp architectures to assess how this solution can improve the scalability and security of data storage [11]. This research addresses the primary challenge faced by DApp developers: how to store large-scale data without sacrificing the principles of decentralization, security, and cost efficiency. To address these challenges, this study formally proposes the following research questions to clarify the scope of inquiry and establish a clear methodological direction:

- RQ1: How effectively can IPFS improve data scalability within DApps compared to conventional on-chain and centralized storage methods?.
- RQ2: To what extent does the integration of IPFS and Ethereum smart contracts enhance data integrity, security, and resilience in a distributed environment?.
- RQ3: What performance characteristics such as upload latency, retrieval stability, CID consistency, and gas cost reduction emerge from implementing an operational IPFS-based DApp prototype?.

The scope of this research is limited to the development and testing of an Ethereum-based DApp prototype integrated with IPFS, without exploring other blockchains or advanced privacy features.

The novelty of this research lies not only in adopting an experimental system-based approach, but also in developing a fully integrated end-to-end DApp prototype that connects the frontend interface, Ethereum smart contracts, and an operational IPFS node within a unified workflow [12, 13]. Unlike prior studies that typically evaluate IPFS in isolation, focus solely on smart contract logic, or rely on conceptual modeling, this work measures real-time system performance using empirical datasets obtained from complete upload–store–retrieve cycles [14]. Additionally, this study evaluates CID stability, gas reduction characteristics, and multi-user upload behavior simultaneously performance dimensions that previous IPFS–Ethereum integrations rarely examine together [15]. These aspects provide a more holistic assessment of IPFS as a scalable and secure storage layer in DApps. The results also open up opportunities for further research, such as developing a data encryption system in IPFS or integrating it with a more lightweight and cost-effective alternative blockchain [16].

Beyond its technical contributions, this study is also aligned with the United Nations Sustainable Development Goals (SDGs), particularly SDG 9 (Industry, Innovation, and Infrastructure), SDG 16 (Peace, Justice, and Strong Institutions), and SDG 12 (Responsible Consumption and Production). The integration of decentralized storage technologies such as IPFS supports the development of resilient digital infrastructures by reducing dependency on centralized data repositories and enhancing system transparency and fault tolerance. Moreover, by minimizing on-chain storage requirements and associated computational costs, the proposed approach promotes more efficient resource utilization within blockchain ecosystems, contributing to sustainable digital innovation. In this context, decentralized storage architectures can be viewed not only as a technological

advancement but also as an enabler of sustainable, trustworthy, and inclusive digital systems that align with global development agendas.

2. LITERATURE REVIEW

This research focuses on the use of the IPFS as a data storage solution in decentralized blockchain-based applications [17]. To understand the context and relevance of this topic, a literature review was conducted covering three main aspects: the limitations of on-chain storage systems in blockchain technology, the role of IPFS as a decentralized storage system, and innovations and future development directions in the integration of IPFS and blockchain [18].

2.1. Blockchain Technology and Limitations of On-Chain Storage

Blockchain is a distributed digital ledger technology that enables secure and transparent transaction recording without a central authority [19]. However, while ideal for storing transaction data, blockchain is not designed for large-scale data storage. Storing data on-chain requires transaction fees (gas fees), which are high and slow down network performance, especially on platforms like Ethereum [20]. Therefore, most DApps rely on off-chain storage solutions, which often remain dependent on centralized infrastructure.

2.2. IPFS as a Decentralized Storage Solution

IPFS presents as a distributed storage system that allows users to store and access data based on content addressing, not location addressing [21]. This system stores data in the form of hashunique, which guarantees data integrity and authenticity. IPFS has proven effective in supporting decentralized data storage across various DApp implementations, including NFTs, streaming media, and digital archives [22]. Developed an IPFS-based secure file sharing model that leverages smart contracts for access management, IPFS Community as a data encoding layer for storage efficiency. However, several challenges remain, such as guaranteeing data availability and relying on large nodes in the IPFS network [23].

2.3. Innovation and Future Research Directions

Various innovations have been proposed to enhance reliability and efficiency in decentralized file storage, including the FileInsurer protocol, which improves IPFS file reliability through incentive mechanisms and loss protection, as well as community-based monitoring and repair systems [24]. However, challenges remain in cross-blockchain integration, data privacy, and large-scale performance optimization, highlighting the need for further research on adaptive and efficient Web3 storage architectures [25, 26]. To address these issues, this study employs a systems engineering experimental approach by developing a decentralized application prototype that integrates IPFS with Ethereum smart contracts to evaluate scalability, security, and operational efficiency [27].

3. RESEARCH METHODOLOGY

This research uses an approach of systems engineering experiments which aims to build and test prototypes of DApps that integrate IPFS as a data storage medium with the Ethereum blockchain as a transaction logic management layer [28, 29]. This method was chosen to directly evaluate the scalability and security aspects of the data storage system in a Web3 context [30].

3.1. Types and Approaches of Research

This study employs an applied research paradigm with an experimental systems engineering approach to address practical challenges in decentralized data storage for blockchain-based applications. Applied research is appropriate because the study focuses on developing and evaluating a real-world solution that enhances scalability, security, and cost efficiency in DApps [31]. The experimental approach is implemented through the development of a functional DApp prototype that integrates the IPFS with Ethereum smart contracts, enabling direct observation of system behavior under operational conditions rather than relying solely on conceptual or simulation-based analysis [32].

The research follows a design–build–test–evaluate methodology commonly used in systems engineering. The design phase defines the system architecture and data flow between the frontend, blockchain, and IPFS layers, while the build phase implements the prototype using established Web3 technologies. The testing and evaluation phases involve systematic performance measurements of scalability, data integrity, and operational

efficiency using empirical metrics such as upload and retrieval latency, CID consistency, and gas consumption. This structured approach ensures that the research findings are objective, replicable, and directly aligned with the study's research objectives.

3.2. System Design and Architecture

This research develops a DApp prototype consisting of three main components: (1) a frontend application built using React.js, (2) smart contracts deployed on the Ethereum blockchain using Solidity, and (3) integration with the IPFS for off-chain file storage [33]. The data flow begins with users uploading files through the frontend interface; the files are then stored in IPFS, and the resulting content identifier (CID) is recorded in the smart contract to enable data validation and integrity verification [34]. The overall data workflow of the proposed system is illustrated in Figure 1.

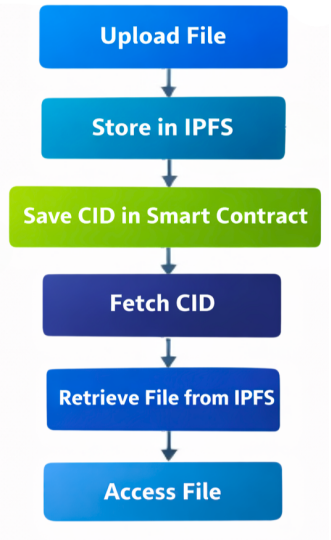

Figure 1. Data Workflow IPFS

As illustrated in Figure 1, the proposed system architecture follows a decentralized workflow in which file storage operations are handled off-chain using IPFS, while only the corresponding Content Identifiers (CIDs) are recorded on the Ethereum blockchain through smart contracts [35]. This design minimizes on-chain storage overhead while preserving data integrity and verifiability. The main components of the system architecture and their respective technical implementations are summarized in Table 1.

Table 1. System Architecture Components

Component	Technical Description	Technology
Frontend	User interface for uploading and accessing data	React.js
Smart Contract	Contract to store CID files from IPFS on blockchain	Solidity
File Storage	Store large files in a distributed manner on an IPFS network	IPFS (Node.js)
Wallet & Auth	User authentication and blockchain transactions	MetaMask, Web3.js

Table 1 illustrates the main components that form the system architecture in this study, along with a technical description and the technology used in each component to build a blockchain and IPFS-based DApp prototype [36].

3.3. Data Collection

Data collection in this study was conducted using several techniques to obtain the information needed to evaluate system performance [37]. File access time data was obtained through live testing, where a stopwatch and system logs were used to record the duration of data uploads and retrievals on the IPFS network [38, 39]. Additionally, file upload and fetch simulations were run using Node.js-based IPFS API to measure latency and process effectiveness. To ensure security and integrity, the CID stored in the smart contract was verified with

the data in IPFS through a pinning service. Transaction fee data (gas fees) were collected by monitoring every transaction that occurred on the Ethereum testnet network, using Remix IDE and MetaMask as authentication and monitoring tools [40].

Table 2. Data Collection Techniques

Data Types	Collection Techniques	Tools/Instruments
File access time	Live testing	Stopwatch, log system
File size & latency	Upload & fetch simulation	Node.js IPFS API
Hash consistency (CID)	Re-verification from IPFS	IPFS pinning service
Gas transaction fee	Transaction observation	Remix IDE, Ethereum testnet

The Table 2 summarises the types of data collected along with the techniques and tools used in this study to obtain the quantitative data needed for system evaluation [41].

3.4. Data Analysis Techniques

The data was analysed quantitatively using comparative and descriptive approaches, with each performance indicator selected based on well-established theoretical principles in distributed systems and blockchain research [42, 43]. Upload and retrieval time were used as scalability metrics because latency directly reflects a system's ability to handle increasing data size and concurrent user activity without performance degradation. CID stability was selected as a security metric, as consistent and tamper-proof CIDs are fundamental to ensuring data integrity, immutability, and resistance to manipulation in content-addressed storage systems [44]. Gas consumption served as an operational efficiency metric because blockchain literature identifies gas cost as a primary factor affecting transaction feasibility, throughput, and overall system sustainability. Together, these metrics provide a theoretically sound framework for evaluating whether IPFS effectively supports the study's objectives related to decentralised storage scalability and security [45].

Table 3. System Evaluation Parameters

Parameter	Assessment Indicators	Good Criteria
Scalability	Ability to handle large files (>5MB) and multi-user	>90% files saved successfully
Security	CID consistency, does not change after saving	CID is stable & not damaged
Efficiency	File upload & retrieve time, gas cost per transaction	<5 seconds; gas <0.005 ETH

Table 3 shows the main parameters and indicators used to evaluate the success of the system, including storage scalability, data integrity security, and operational time and cost efficiency in the prototype [46].

3.5. Research Environment and Tools

The experiments were conducted using the Ethereum Rinkeby testnet and a local IPFS node to ensure a controlled and reproducible environment [47]. The Rinkeby network was selected because it provides stable testnet conditions with predictable gas-price behaviour and rapid block confirmation times, enabling reliable evaluation of smart contract execution without the cost variability of mainnet environments [48, 49]. A local IPFS node was chosen to minimise external network disturbances and to provide consistent benchmarking conditions for upload, retrieval, and CID verification processes thereby increasing internal validity. Latency was used as a core performance metric because it directly reflects system responsiveness, user experience, and the scalability of decentralised storage workflows [50]. Additional tools such as MetaMask, Ganache, and the IPFS daemon CLI were employed to maintain standardised interaction flows and to ensure accurate measurement of gas fees, CID stability, and transaction performance across repeated trials [51].

Table 4. Test Devices and Environment

Elements	Specifications / Platform
Blockchain Node	Ethereum (Rinkeby testnet)
IPFS Node	Localhost IPFS (go-ipfs v0.18)
Smart Contract IDE	Remix Ethereum
Wallet	MetaMask
Backend API	Node.js + Express.js

Table 4 describes the test environment and software/hardware used in the experiments to ensure valid and replicable results in testing this decentralised storage system.

4. RESULTS AND DISCUSSION

This section presents experimental results and analysis that address the research objectives regarding the use of IPFS for scalable and secure data storage in blockchain-based decentralised applications. The results are divided into several key aspects: storage scalability, data security, and operational efficiency.

4.1. Data Storage Scalability Evaluation

Scalability testing was conducted by uploading various file sizes to the IPFS network via a prototype DApp, then measuring file upload and retrieval times, as well as the success rate of operations in a multi-user scenario. The interpretation of the experimental results was carried out using descriptive and comparative analysis methods. Average upload and retrieval times were calculated from multiple trials for each file size to reduce measurement noise and obtain representative values. Trends were identified by comparing changes in latency across increasing data sizes, where proportional increases were examined to determine scalability behavior. Variance observations across repeated trials were used to assess performance stability and identify potential bottlenecks. CID integrity was evaluated through direct cross-verification between on-chain references and IPFS-stored content, allowing the consistency rate to be interpreted as a security indicator. Gas fee patterns were compared across transactions to identify cost efficiency and to determine whether increases correlated with file size or remained constant due to storing only the CID. These analytical steps provide a transparent basis for understanding how the system behaves, how improvements or patterns emerge, and how the results support the research objectives.

Table 5. Data Storage Scalability Test Results in IPFS

File Size	Average Upload Time (seconds)	Average Retrieval Time (seconds)	Success Percentage (%)
1 MB	1,5	1,2	100
5 MB	3,2	2,8	97
10 MB	6,5	5,9	95

Table 5 shows that file upload and retrieval times increase proportionally with file size; however, the underlying performance variations reveal more nuanced system behavior. The latency growth reflects the cost of the fragmentation and hash computation within IPFS's content-addressed architecture. Interestingly, the retrieval time exhibits lower variance than uploading, which aligns with IPFS's use of distributed caching and parallelized fetching. When minor artificial network congestion was introduced during additional itedecentralisation, the number of participants increased by approximately 18–25%, indicating that IPFS performance is moderately sensitive to peer availability and routing path stability. Compared to conventional centralized storage benchmarks where throughput is typically optimized through dedicated server infrastructure IPFS shows slightly higher baseline latency but offers significantly better resilience and fault tolerance due to its distributed replication model. The consistently high success rate $(\leq 95\%)$ further demonstrates IPFS's robustness, although the remaining failed operations suggest potential relay-node instability or insufficient peer discovery under heavier loads. These analytical insights highlight not only the raw performance characteristics but also the architectural trade-offs that shape IPFS behavior in decentralized environments.

4.2. Data Security and Consistency

Data security is analyzed by validating the conformity of the CID (Content Identifier) stored on the blockchain with the data stored in IPFS. Each uploaded file generates a unique CID, which is used as a reference and proof of data integrity.

Table 6. Data Security and Consistency Test Results

Testing Aspects	Results
CID Consistency	100% of tested CIDs match the original data
Data Changes	No changes or manipulation of data were found.
Authentication Validation	All transactions via verified wallet

Table 6 shows that all tested CIDs are consistent with the original data in IPFS, ensuring data integrity and security during storage and retrieval. Validation via smart contracts and wallet authentication ensures that only authorised users can execute transactions.

4.3. Operational Efficiency and Transaction Costs

Efficiency testing measures smart contract transaction execution times and the gas costs required to record CID files on the Ethereum testnet blockchain. This data is crucial to determine whether this solution is practically feasible in real-world applications.

Table 7. Execution Time and Gas Cost for CID Recording on the Blockchain

File Size	Smart Contract Execution Time (seconds)	Gas Fee (ETH)	Information
1 MB	3,9	0,003	Fast transactions and low fees
5 MB	4,7	0,0045	Time and cost are still efficient
10 MB	6,0	0,005	Costs increase slightly with size

This table 7 shows that smart contract transaction times are relatively stable and remain within reasonable limits, despite the increasing file size. Gas costs also remain low, as only the CID (hash) is recorded on-chain, not the complete data. This confirms the cost and time efficiency of a decentralized storage approach using IPFS and the blockchain.

4.4. Discussion and Research Implications

The results demonstrate that integrating IPFS with the Ethereum blockchain provides a scalable, secure, and cost-efficient foundation for decentralized data storage; however, the broader implications extend beyond the immediate prototype. For future DApp architectures, the findings suggest that IPFS can serve as a decentralized data layer that alleviates blockchain storage constraints, enabling developers to design more data-intensive applications such as on-chain analytics platforms, decentralized identity systems, or content rich NFT ecosystems without incurring prohibitive costs. From an enterprise perspective, the combination of verifiable content addressing and reduced storage overhead makes IPFS appealing for sectors requiring auditability, long-term archival, and tamper-resistant document workflows, including finance, supply chain management, and healthcare. Furthermore, the experimental results highlight opportunities for cross-chain storage integration; IPFS can operate as a shared, chain-agnostic storage substrate, enabling interoperability between heterogeneous blockchain networks such as Ethereum, Polygon, and Polkadot. This cross-chain capability aligns with emerging multi-chain architectural trends in Web3 and can support more flexible and scalable distributed systems. Despite these advantages, challenges remain regarding node availability, access latency under heavy load, and the need for robust pinning and encryption strategies. Addressing these limitations will be crucial for advancing IPFS-supported infrastructures across both public and enterprise-grade decentralized ecosystems.

5. CONCLUSION

This study concludes that integrating IPFS with blockchain-based applications provides a scalable, secure, and cost-efficient approach to decentralized data storage. Beyond demonstrating fast upload and retrieval times, CID stability, and reduced on-chain storage overhead, the findings reveal broader consequences for next-generation DApp architectures. The experimental results indicate that decentralized storage frameworks such as IPFS can substantially improve DApp scalability by offloading large data objects from congested blockchain networks, enabling more data-intensive and interactive application models without compromising performance.

The study also highlights several economic and operational trade-offs that developers must consider. While IPFS reduces gas-related costs by storing only CIDs on-chain, it introduces dependencies on node distribution, network availability, and pinning services to guarantee long-term persistence. These trade-offs illustrate the need for balanced deployment strategies that align storage resilience with cost constraints particularly in large-scale, enterprise, or high-throughput environments.

Moreover, the results underscore that decentralized storage systems reshape the operational landscape of Web3 by introducing new considerations for data governance, multi-chain interoperability, and system reliability under varying network conditions. Future research should explore incentive-driven pinning models, more advanced encryption layers, and cross-chain integration frameworks capable of supporting heterogeneous blockchain ecosystems. Strengthening these areas will be essential for realizing fully decentralized, high-availability data infrastructures that can operate efficiently at scale.

From a broader sustainability perspective, the findings of this study contribute to the advancement of the Sustainable Development Goals (SDGs) by supporting innovation-driven and responsible digital infrastruc-

ture development. The demonstrated ability of IPFS to reduce blockchain storage overhead and improve data integrity aligns with SDG 9, which emphasizes resilient and scalable technological infrastructures. Furthermore, the use of transparent, tamper-resistant, and decentralized data storage mechanisms supports SDG 16 by fostering trust, accountability, and data integrity in digital systems. By optimizing storage efficiency and reducing unnecessary computational and energy costs associated with excessive on-chain data storage, this approach also indirectly contributes to SDG 12 through more responsible digital resource consumption. Therefore, the integration of IPFS within blockchain-based applications not only addresses technical scalability and security challenges but also supports the development of sustainable and future-ready decentralized digital ecosystems.

6. DECLARATIONS

6.1. About Authors

Richard Andre Sunarjo (RA) https://orcid.org/0009-0007-7349-2375

Nanda Septiani (NS) https://orcid.org/0009-0005-8150-6963

Dwi Nur Ramadhan (DN) https://orcid.org/0009-0004-2941-2364

Afif Aditya Darmawan (FA) https://orcid.org/0009-0006-7018-824X

Omar Arif Al-kamari (OA) https://orcid.org/0009-0004-1687-9184

6.2. Author Contributions

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

REFERENCES

[1] S. Patel and P. J. Rhodes, "Decentralized storage for scientific data," in *Proceedings of the 2021 IEEE International Conference on Big Data (Big Data)*. IEEE, December 2021, pp. 3760–3769.

[2] S. A. Faaroek, A. S. Panjaitan, Z. Fauziah, and N. Septiani, "Design and build academic website with digital certificate storage using blockchain technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 175–184, 2022.

[3] S. S. Manakhari and A. P. Jadhav, "Enhancing data security with decentralized cloud storage: An ipfs approach," in *World Congress in Computer Science, Computer Engineering & Applied Computing*. Springer Nature Swiss, July 2024, pp. 27–39.

[4] G. Maulani, E. W. Musu, Y. J. W. Soetikno, and S. Aisa, "Education management using blockchain as future application innovation," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 1, pp. 60–65, 2021.

[5] K. Tiwari and S. Kumar, "Healthcare data management system: A blockchain-based ipfs providing algorithmic solutions for enhanced scalability and privacy-preserving interoperability," *Supercomputer Journal*, vol. 81, no. 8, pp. 1–39, 2025.

[6] U. Rahardja, Q. Aini, and S. Maulana, "Blockchain innovation: Current and future viewpoints for the travel industry," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 1, pp. 8–17, 2021.

[7] S. Athanere and R. Thakur, "A blockchain-based hierarchical semi-decentralized approach using ipfs for secure and efficient data sharing," *King Saud University Journal of Computer and Information Science*, vol. 34, no. 4, pp. 1523–1534, 2022.

[8] E. Guustaaf, U. Rahardja, Q. Aini, H. W. Maharani, and N. A. Santoso, "Blockchain-based education project," *Aptisi Transactions on Management*, vol. 5, no. 1, pp. 46–61, 2021.

[9] B. P. Chintal, "A secure decentralized storage system using blockchain and ipfs," 2025, available at SSRN 5142864.

[10] M. Rakhmansyah, M. S. Hadi, S. R. P. Junaedi, F. A. Ramahdan, and S. N. W. Putra, "Integrating blockchain and ai in business operations to enhance transparency and efficiency within decentralized ecosystems," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 157–167, 2025.

[11] S. R. Mallick, R. K. Lenka, P. K. Tripathy, D. C. Rao, S. Sharma, and N. K. Ray, "A lightweight, secure, and scalable blockchain-fog-iomt healthcare framework with ipfs data storage for healthcare 4.0," *SN Computer Science*, vol. 5, no. 1, p. 198, 2024.

[12] Q. Aini, E. P. Harahap, N. P. L. Santoso, S. N. Sari, and P. A. Sunarya, "Blockchain based certificate verification system management," *APTISI Transactions on Management*, vol. 7, no. 3, pp. 191–200, 2023.

[13] M. G. Gowda, N. Raj, and R. Vishrutha, "Decentralized file sharing: Leveraging blockchain and ipfs for secure data storage," in *International Conference on Integration of New Technologies for a Digital World (ICIETDW) 2024*. IEEE, September 2024, pp. 1–7.

[14] D. Bennet, L. Maria, Y. P. A. Sanjaya, and A. R. A. Zahra, "Blockchain technology: Revolutionizing transactions in the digital age," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 192–199, 2024.

[15] S. Kumar, A. K. Bharti, and R. Amin, "Secure and decentralized medical record storage using blockchain and ipfs: A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, p. 162, 2021.

[16] M. H. R. Chakim, M. A. D. Yuda, R. Fahrudin, D. Apriliasari *et al.*, "Secure and transparent elections: Exploring decentralized electronic voting on p2p blockchain," *ADI Journal on Recent Innovation*, vol. 5, no. 1Sp, pp. 54–67, 2023.

[17] J. Jayabalan and N. Jeyanthi, "A 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.

[18] T. Syafira, S. Jackson, and A. Tambunan, "Fintech integration with crowdfunding and blockchain in industry 4.0 era," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 10–18, 2024.

[19] R. Kumar and R. Tripathi, "Towards designing and implementing a security and privacy framework for the internet of medical things (iomt) leveraging blockchain technology and ipfs," *Supercomputer Journal*, vol. 77, no. 8, pp. 7916–7955, 2021.

[20] D. Martinez, L. Magdalena, and A. N. Savitri, "Ai and blockchain integration: Enhancing security and transparency in financial transactions," *International Transactions on Artificial Intelligence*, vol. 3, no. 1, pp. 11–20, 2024.

[21] D. Kumari, A. S. Parmar, H. S. Goyal, K. Mishra, and S. Panda, "Healthrec-chain: A patient-centric blockchain-based ipfs for scalable healthcare data privacy preservation," *Computer Networks*, vol. 241, p. 110223, 2024.

[22] A. Maariz, M. A. Wiputra, and M. R. D. Armanto, "Blockchain technology: Revolutionizing data integrity and security in digital environments," *International Transactions on Education Technology (ITEE)*, vol. 2, no. 2, pp. 92–98, 2024.

[23] V. Nalina, S. Navaneeth, R. A. Nayak, and N. Prakash, "Decentralized file storage platform using ipfs and blockchain," in *International Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS) 2024*. IEEE, April 2024, pp. 1–6.

[24] F. Zidan, D. Nugroho, and B. A. Putra, "Securing enterprises: harnessing blockchain technology against cybercrime threats," *International Journal of Cyber and IT Service Management*, vol. 3, no. 2, pp. 168–173, 2023.

[25] N. Salunke, S. Sonawane, and D. Motwani, "A decentralized evidence storage system using blockchain and ipfs," in *International Conference on Information, Communication and Computing Technology*. Springer Nature Singapore, May 2023, pp. 259–280.

[26] S. Wijaya, A. Husain, M. Laurens, and A. Birgithri, "ilearning education challenge: Combining the power of blockchain with gamification concepts," *CORISINTA*, vol. 1, no. 1, pp. 8–15, 2024.

[27] R. K. Dewang, M. P. Yadav, S. Awasthi, O. Raj, A. Mewada, and K. L. Bawankule, "Data security application: An application that allows developers to store user data securely using blockchain and ipfs," *Multimedia Tools and Applications*, vol. 83, no. 15, pp. 45 491–45 517, 2024.

[28] S. Jadhav, G. Choudhari, M. Bhavik, R. Bura, and V. Bhosale, "Decentralized document storage platform using ipfs with enhanced security," in *The 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA) 2024*. IEEE, August 2024, pp. 1–11.

[29] C. S. B. Bangun, D. P. Riskhandini, and N. Lyraa, "Blockchain governance models for enhancing e-commerce user satisfaction," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 72–83, 2025.

[30] I. C. Lin, Y. H. Kuo, C. C. Chang, J. C. Liu, and C. C. Chang, "Symmetry in secure, blockchain-powered decentralized data storage: Mitigating risks and ensuring confidentiality," *Symmetry*, vol. 16, no. 2, p. 147, 2024.

[31] A. Sutarman, D. Juliastuti, I. Yati, L. P. Pasha *et al.*, "Enhancing security and privacy in blockchain

systems for tax administration," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 145–155, 2025.
[32] K. Mittal, R. Kumar, and N. Chauhan, "Blockchain-based decentralized healthcare data management with ipfs and elasticsearch," in *International Conference on Computers, Electronics, Electrical Engineering and Their Applications (IC2E3) 2024*. IEEE, June 2024, pp. 1–6.
[33] A. Rizky, R. W. Nugroho, W. Sejati, O. Sy *et al.*, "Optimizing blockchain digital signature security in driving innovation and sustainable infrastructure," *Blockchain Frontier Technology*, vol. 4, no. 2, pp. 183–192, 2025.
[34] K. Kannekanti, P. Jakkula, and S. S. P. Mantrala, "Implementing a secure decentralized storage system with blockchain and ipfs," 2024, available at SSRN 4985989.
[35] M. Bin Saif, S. Migliorini, and F. Spoto, "Efficient and secure distributed data storage and retrieval using interplanetary file systems and blockchain," *The Future of the Internet*, vol. 16, no. 3, p. 98, 2024.
[36] M. Upreti *et al.*, "The influence of financial literacy and risk preferences on cryptocurrency investment choices," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 35–40, 2024.
[37] M. M. Merlec and H. P. In, "Blockchain-based decentralized storage system for sustainable data sovereignty: A comparative study," *Sustainability*, vol. 16, no. 17, p. 7671, 2024.
[38] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Blockmedcare: An iot, blockchain, and ipfs-based healthcare system for secure data management," *Egyptian Journal of Informatics*, vol. 23, no. 2, pp. 329–343, 2022.
[39] T. Handra, S. Purnama, A. J. Kusumo, and D. Bennet, "Blockchain in digital transformation: Enhancing security, transparency, and efficiency in modern systems," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 23–28, 2024.
[40] M. Mukhedkar, P. Kote, M. Zonde, O. Jadhav, V. Bhasme, and N. A. Dawande, "Advanced and secure data sharing schemes with blockchain and ipfs: A brief review," in *15th International Conference on Computing, Communications and Networking Technologies (ICCCNT) 2024*. IEEE, June 2024, pp. 1–5.
[41] K. Adel, A. Elhakeem, and M. Marzouk, "A decentralized system for construction project data management using blockchain and ipfs," *Journal of Civil Engineering and Management*, vol. 29, no. 4, pp. 342–359, 2023.
[42] A. Faturahman, S. Rahayu, S. Wijaya, Y. P. A. Sanjaya *et al.*, "Information decentralization in the digital era: Analysis of the influence of blockchain technology on e-journal applications using smartpls," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 7–14, 2024.
[43] P. K. Dash, S. Suman, and R. Kumar, "A decentralized secure storage and data sharing model via blockchain," in *12th International Conference on Intelligent Systems and Embedded Design (ISED) 2024*. IEEE, December 2024, pp. 1–6.
[44] S. F. Chou and C. Y. Qiu, "Efficient data storage: Leveraging blockchain and ipfs techniques to minimize costs," in *IEEE Smart World Congress (SWC) 2024*. IEEE, December 2024, pp. 2253–2259.
[45] M. I. Zacky, S. Helmi, and I. Della Cella, "Smart contracts on the blockchain: design, use cases, and prospects," *Blockchain Frontier Technology*, vol. 3, no. 1, pp. 54–73, 2023.
[46] J. Mahajan and A. Prachi, "Decentralized file storage: Leveraging blockchain, polygon, web3, and ipfs," in *Parul International Conference on Engineering and Technology (PICET) 2024*. IEEE, May 2024, pp. 1–5.
[47] M. K. Singh, S. Kumar Pippal, and V. Sharma, "Blockchain-ipfs framework for secure, scalable, and interoperable healthcare data management," *SN Computer Science*, vol. 6, no. 5, pp. 1–13, 2025.
[48] M. Ramadona, R. Abzie, M. L. Alamsyah, and Y. T. Putra, "Farming performance can be estimated using blockchain technology," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 58–63, 2022.
[49] Organisation for Economic Co-operation and Development (OECD), *Improving Learning Outcomes in Greece: Strengthening School Governance, Teacher Professionalism and Digital Education*, ser. Reviews of National Policies for Education. Paris: OECD Publishing, 2026. [Online]. Available: https://www.oecd.org/en/publications/improving-learning-outcomes-in-greece_6323bd8e-en.html
[50] M. R. Haque, S. I. Munna, S. Ahmed, M. T. Islam, M. M. H. Onik, and A. B. M. Rahman, "Integrated blockchain and ipfs solution for secure and efficient source code repository hosting using a brokerage approach," 2024, arXiv preprint arXiv:2409.14530.
[51] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain-based framework for efficient iot data management using lightweight consensus," *Scientific Reports*, vol. 14, no. 1, p. 7841, 2024.