

Decentralized File Sharing Infrastructure with IPFS for Censorship Resistance in Blockchain Ecosystems

Nesti Anggraini Santoso^{1*} , Palma Juanta² , Sabda Maulana³ , Kerimbekov Toktar⁴ , Aulia

Khanza⁵ 

¹Department of Information System, University of Raharja, Indonesia

²Faculty of Science Education Doctoral Study Program, Padang State University, Indonesia

^{3,5}Department of Digital Business, University of Raharja, Indonesia

⁴Department of Language and Linguistics, Abai Kazakh National Pedagogical University, Kazakhstan

¹nesti@raharja.info, ²palmajunta@unprimdn.ac.id, ³sabda@raharja.info, ⁴tokhtarsenbekuli@gmail.com, ⁵aulia.khanza@raharja.info

*Corresponding Author

Article Info

Article history:

Received month dd, 2025-06-19

Revised month dd, 2025-07-25

Accepted month dd, 2025-07-31

Keywords:

Blockchain Technology

TikTok Influencer Marketing

Structural Equation Modeling (SEM)

Advertising Value



ABSTRACT

Traditional file sharing systems that rely on centralized servers face various challenges. problems such as vulnerability to censorship, blocking, and server failures. The background this research focuses on the need for file sharing technology that is more secure, censorship resistant, and does not depend on a single central authority. Challenge the main challenge in developing a new file sharing system is how to overcome the limitations of network scale, slow access speed, and lack of incentives for node providers. **Research purposes this** is to analyze the role of the InterPlanetary File System (IPFS) in building a censorship resistant file sharing infrastructure and evaluate its benefits and constraints compared to conventional file sharing systems. **Findings from the literature** study show that IPFS has advantages in data decentralization, increasing information availability, and strengthening resistance to censorship. **Research results also revealed** that although IPFS is able to overcome many weaknesses of traditional systems, further development is still needed in terms of network efficiency and user incentives. **The conclusion, IPFS has** great potential to become the main foundation in a future digital ecosystem that is more open, secure, and free of third party intervention. This paper contributes to the advancement of technical innovation by analyzing how IPFS, when combined with blockchain-based incentive systems like Filecoin, can create a highly resilient, decentralized, and censorship-resistant infrastructure for secure data distribution.

This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



DOI: <https://10.34306/bfront.v5i1.835>

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

1. INTRODUCTION

In today's digital era, data has become one of the most valuable assets in various aspects of life, including communication, business, and research. However, conventional file sharing systems that rely on centralized servers often face various challenges, such as limited access, service outages, and censorship threats from certain parties. In this condition, a solution is needed that can increase data resilience and availability without relying on a single entity. InterPlanetary File System (IPFS) emerged as a file sharing technology that offers a decentralized approach by relying on peer to peer (P2P) networks. Unlike HTTP-based protocols that

access files based on the location of a particular server, IPFS identifies data based on its content and stores it in a distributed network. In this way, data can be accessed from various nodes in the network, making it harder to censor or delete completely. One of the main challenges in conventional file sharing infrastructure is the risk of censorship by governments, technology companies, or other interested parties. This censorship can take the form of blocking websites, removing content, or restricting access to certain resources. IPFS resists censorship by eliminating single points of failure through a decentralized network.

IPFS offers a number of other advantages in terms of effectiveness and data security in addition to censorship resistance. Through data replication and caching across several nodes, this technology enables faster and more bandwidth-efficient file distribution. Users may be certain that the data they access has not been altered or modified by using a cryptographic hash scheme for file identification, which also enhances data integrity and authenticity. While IPFS has many advantages, it also faces several issues. These include limitations on network scale, the requirement for incentives for node providers, and privacy concerns regarding content traceability in an open network. For IPFS to become a mainstream solution for file sharing infrastructure across many industries, wider adoption is still needed. As a result, to address these issues, further research and development of new technologies, such as blockchain-based incentive systems, may be essential.

In recent years, IPFS has begun to be adopted by various platforms and communities as a solution for more secure data storage and distribution. Several blockchain projects and decentralized applications have utilized IPFS to ensure the availability of information without relying on traditional servers. The successful implementation of IPFS in various fields shows the great potential of this technology in supporting freedom of information and data resilience in the future.

In this paper, we will learn how IPFS creates a censorship resistant file sharing infrastructure, as well as how this technology works, its benefits, and its pitfalls. By understanding the role of IPFS, we hope to find better solutions to build a file sharing system that is more secure, effective, and free from centralized control. In alignment with the United Nations Sustainable Development Goals (SDGs), particularly Goal 9 (Industry, Innovation, and Infrastructure) and Goal 16 (Peace, Justice, and Strong Institutions), the implementation of decentralized file sharing technologies like IPFS contributes to building resilient infrastructure and promoting inclusive access to information. By enabling censorship-resistant and secure data distribution, IPFS supports transparency, technological equity, and the democratization of digital content. These characteristics are essential for ensuring that innovation in information systems advances not only in efficiency, but also in ethical and globally inclusive ways.

2. LITERATURE REVIEW

The InterPlanetary File System (IPFS) is a peer-to-peer (P2P) file sharing protocol. Its purpose is to improve decentralization, censorship resistance, and speed of data distribution. IPFS offers a distributed storage method that can be used as an alternative to centralized cloud systems [1, 2]. The rationale for selecting IPFS lies in its unique ability to leverage content-based addressing and peer to peer architecture, which sets it apart from location based and centralized file-sharing methods. The theoretical foundation is rooted in distributed systems theory and cryptographic trust models, making IPFS ideal for contexts requiring both data availability and integrity. Content addressing, or content addressing, is used by this system to improve data availability because it allows data to remain accessible even if the initial server is inaccessible. The rationale for selecting IPFS lies in its ability to overcome limitations of conventional systems through content-based addressing, eliminating dependency on a single point of failure. Theoretically, it is rooted in decentralized systems architecture and cryptographic trust models, which provide high resilience, transparency, and data integrity in untrusted environments. Compared to alternatives, IPFS uniquely supports censorship resistance and efficient distribution, making it ideal for decentralized file sharing. Examining the IPFS infrastructure and finding that even though the IPFS network is spread all over the world, there are still problems with the reliability and efficiency of data retrieval [3]. They emphasized that to make IPFS reliable as the backbone of the decentralized web, data routing and node replication are needed to be improved.

Discussing IPFS security issues, especially potential censorship attacks on unwanted content [4, 5]. They identify attack methods and suggest ways to protect content from blocking in the IPFS network, which is especially important in countries with restrictions on access to information. Comparing IPFS with other decentralized data networks and emphasizing its advantages in terms of content distribution and decentralization. However, they also highlight that large-scale deployment of IPFS still faces issues in terms of network

performance and ecosystem sustainability [6]. IPFS still lacks a built-in incentive system to motivate users to provide storage resources, despite its promising architecture [6]. IPFS relies on voluntary node involvement, in contrast to conventional centralized systems where service providers are compensated to maintain infrastructure [7, 8]. Complementary solutions like Filecoin, which provides a blockchain-based incentive layer for IPFS users, have been implemented by several initiatives in order to address this [9, 10]. The long-term sustainability of the decentralized ecosystem is increased by this integration, which allows users to receive tokens in return for providing storage space and preserving file availability [11].

Adoption of IPFS is further complicated by issues with content traceability and data privacy [12]. Any publicly accessible file can be viewed by anyone with the correct hash since IPFS addresses and retrieves content using a cryptographic hash. Although openness enhances transparency, it also presents privacy risks that require additional protective layers such as encryption and access control [13]. In order to enhance data security while preserving the advantages of decentralized storage, businesses and developers are investigating techniques including client-side encryption, access control layers, and private IPFS clusters [14, 15]. Future research should focus on exploring industry-specific applications of IPFS, such as in health care, journalism, or government archives, where censorship resistance and data integrity are critical [16]. Policymakers should consider developing regulatory frameworks that both encourage innovation in decentralized storage and enforce responsible data governance, especially regarding data traceability and encryption compliance. Furthermore, cooperation between developers, service providers, regulators, and end users is necessary for the successful large scale deployment of IPFS [17, 18]. To promote usability and trust, precise rules

for content moderation procedures, gateway compatibility, and metadata standards must be established. Coordinated efforts will be required when more platforms start integrating IPFS for decentralized publishing, archiving, and content distribution in order to maintain the technology's dependability, security, and usability for all users [19, 20].

3. RESEARCH METHOD

The purpose of this study is to gain a better understanding of the role of the InterPlanet File System (IPFS) in building a censorship-resistant file sharing infrastructure. The descriptive method of this study allows for a systematic explanation of the concepts, phenomena, and facts found in the academic literature on IPFS technology without resorting to statistical calculations or direct experiments [21, 22]. The data in this study were obtained by examining literature from various secondary sources, especially scientific journals that have been published since 2021. This study focuses on the potential of IPFS as a distributed storage system, assessing the IPFS infrastructure globally, emphasizing the security and censorship aspects of IPFS content, and comparing it with other decentralized data networks [23]. This research introduces a novel perspective by evaluating the potential synergy between IPFS and blockchain based token incentive mechanisms, such as Filecoin, which can address IPFS's scalability and sustainability limitations an angle that has not been thoroughly explored in prior literature. A descriptive analysis of the collected data was conducted by finding key issues such as system decentralization, censorship resilience, data distribution efficiency, and issues with scalability, performance, and network sustainability. The data was collected by systematically identifying relevant academic publications through Google Scholar and Scopus using keywords such as 'IPFS censorship resistance', 'decentralized file sharing', and 'blockchain incentives'. Each article was then coded and categorized based on core themes such as decentralization, resilience, privacy, and performance. This approach ensured consistency in analysis and strengthened the reliability of the conclusions. The researchers also relate the results of the study to the need for more secure and open file sharing technology from centralized control. This method allows researchers to create a comprehensive picture of how IPFS works, its benefits, and its pitfalls. This will allow the technology to be used more widely as a replacement for conventional file sharing systems.

Table 1. (SOTA) Matrix on Decentralized and Censorship-Resistant File Sharing Infrastructure Using IPFS in Blockchain Ecosystems

No.	Reference	Method	X (Focus)	Y (Comparison)	Novelty / Future Work
1	Total Eclipse of the	Experimental	IPFS	Attack vectors	Identification of

No.	Reference	Method	X (Focus)	Y (Comparison)	Novelty / Future Work
	Heart Disrupting the InterPlanetary File System	and Security Analysis	Infrastructure	and censorship resilience	IPFS vulnerabilities to censorship attacks →Development of mitigation strategies and adaptive security systems
2	<i>Mapping the Inter-Planetary File System</i>	Topology Mapping & Network Analysis	IPFS Data Routing	Global network performance	Modeling IPFS routing efficiency and network bottlenecks →Improvement of node replication and file access optimization
3	<i>Monitoring Data Requests in Decentralized Data Storage Systems</i>	Case Study & Data Monitoring	IPFS Data Request Monitoring	Privacy and censorship risks	Exploration of traceability within open IPFS networks →Integration of client-side encryption and content authorization systems
4	<i>Content Censorship in the InterPlanetary File System</i>	Qualitative Analysis	Content Censorship	Decentralized networks including IPFS	Identification of censorship patterns and mechanisms in IPFS →Development of anti-censorship protection layers
5	<i>(2022) IPFS and Friends: A Qualitative Comparison of Next Generation P2P Data Networks</i>	Qualitative Comparative Study	IPFS and other P2P protocols	Performance and decentralization	Comprehensive analysis of strengths and weaknesses among systems →Enhancement of interoperability and P2P system performance
6	<i>Implementing Content Erasure in IPFS</i>	Prototyping & Policy Design	Content Deletion in IPFS	Data control and erasure	Proposed mechanism for controlled content deletion in IPFS networks →Need for deletion auditing and metadata protection systems
7	<i>What's Inside a Node? Malicious IPFS Nodes Under the Magnifying Glass</i>	Node Forensics & Behavior Analysis	Malicious IPFS Nodes	Network trust and integrity	Investigation of insider threats within the IPFS network →Design of automated detection and isolation systems for malicious nodes

Table 1 presents a summary of recent studies related to IPFS, outlining their main focus and contributions. Numerous studies currently demonstrate the potential and limitations of IPFS as a sensor range infrastructure with decentralized files. highlight the need for increased routing efficiency and data replication, while emphasize the importance of IPFS security with regard to sensor range. Investigate the mechanism of content censorship in IPFS, while discuss the private risk associated with traceability. compare IPFS to other P2P protocols and highlight the importance of interoperability. Investigate malicious nodes and describe an automatic detection system, while propose a more advanced content detection mechanism. These findings indicate that although IPFS shows promise, significant advancements in security, privacy, and network operations are necessary to enable broader adoption.

4. RESULT AND DISCUSSION

Research has shown that the InterPlanetary File System (IPFS) is a system that provides a more decentralized, safe, and censorship-resistant method of file sharing [24, 25]. Data is not reliant on a central server thanks to IPFS's use of content addresses and peer-to-peer (P2P) networking. This increases data availability and resistance to disruption and censorship attempts by allowing access to data even in the event that the original server is inaccessible [26, 27]. This infographic illustrates how the InterPlanetary File System (IPFS) functions as a decentralized file sharing system that is impervious to censorship. The conclusions presented are based on the comparative matrix of recent studies (Table 1), which summarizes the technical strengths and gaps of IPFS systems. This structured synthesis supports the argument that integration with blockchain incentives is essential to overcoming IPFS's technical barriers [28, 29].

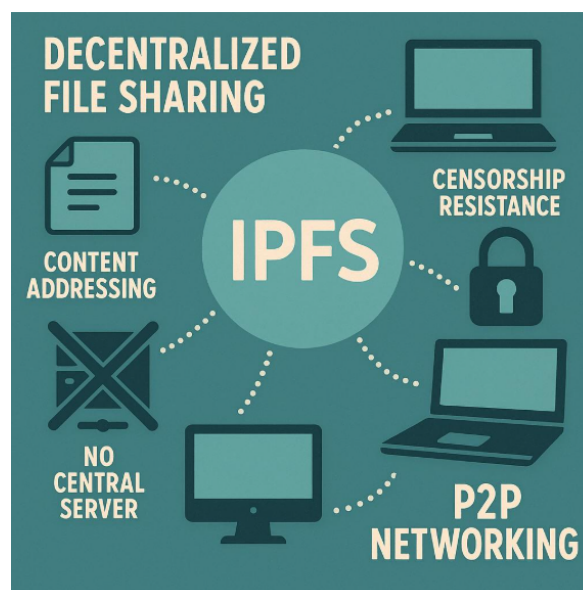


Figure 1. Infographic illustration that explains how the InterPlanetary File System

IPFS must be figure 1 gradually and strategically in order to be properly integrated into organizational data infrastructure. It is recommended that organizations start with trial projects for non-sensitive data in order to assess IPFS's applicability, durability, and performance in their operational environment. In addition to offering a platform for identifying potential roadblocks in technological deployment, content accessibility, and regulatory compliance, these pilot projects act as a risk mitigation measure. Managers can make more educated decisions about the full scale deployment of essential data storage needs with the help of these insights.

The literature was triangulated to ensure data integrity and eliminate bias. It demonstrates how IPFS employs content addressing, which makes data accessible even in the event that the original server is unavailable by accessing files based on their content (hash) rather than their server location [30, 31]. The main findings are derived from Table 1, which synthesizes the scope, methodology, and novelty of current IPFS-related studies. This matrix allows the identification of knowledge gaps and ongoing technical debates, especially in areas like

copyright threats and malicious node behavior. The analysis highlights that although IPFS has foundational strengths, its scalability and privacy limitations require systemic enhancement, which supports the conclusions proposed in this paper [32, 33]. Instead of depending on a central server, IPFS makes use of a peer-to-peer (P2P) network in which any user can serve as both a data source and a recipient [34, 35, 36].

The table shows some of the differences between IPFS and conventional file sharing systems [37, 38]. IPFS has a major advantage in its decentralized architecture because it is more resistant to censorship and does not rely on a central server [39, 40, 41]. Unlike conventional systems that rely on a central server, data remains accessible as long as there is a node to store it [42]. While conventional systems are usually faster and more stable, IPFS access speeds tend to vary depending on network conditions.

IPFS has a security advantage because it uses cryptographic hashes to keep data secure [43, 44, 45]. Unlike conventional systems that are usually based on paid services, IPFS still does not have a built-in incentive system. As a result, IPFS still needs improvements to become a major alternative in digital file sharing, even though it offers the advantages of decentralization and freedom [46, 47, 48]. Therefore, IPFS has a great potential to serve as a replacement for the conventional file sharing model, especially if the need for a more secure, open, and centrally controlled system is considered [49, 50]. However, to encourage wider adoption in the future, technical issues and ecosystem sustainability must be addressed.

5. MANAGERIAL IMPLICATIONS

In order to guarantee sustainable and censorship resistant file sharing systems, these management consequences highlight the importance of implementing decentralized technologies such as IPFS through strategic planning, infrastructure readiness, stakeholder cooperation, and privacy-aware behaviors.

5.1. Investment in Infrastructure and Human Capacity

Adoption of IPFS necessitates a significant investment in human capacity building and technical infrastructure. To preserve performance and availability, organizations must guarantee access to decentralized gateways, secure nodes, and quick peer-to-peer communication. Digital administrators and IT teams should also receive training on the technical aspects of IPFS, such as data replication, distributed node interaction, and content addressing. By giving internal teams these skills, operational dependability will increase and reliance on centralized cloud providers will decrease.

5.2. Collaboration with Ecosystem Stakeholders

Collaboration between developers, service providers, data users, and regulatory agencies is essential for the successful deployment of IPFS. Interoperability between IPFS and current digital systems will be promoted by standardizing metadata practices and establishing clear communication methods. Cooperation also promotes shared accountability for preserving network integrity and lowering the dangers of censorship or content loss. A coordinated strategy will contribute to the development of a decentralized, more sustainable ecology.

5.3. Privacy and Data Governance Considerations

IPFS makes data more accessible and censorship-resistant, but it also brings with it additional privacy and content traceability issues. In decentralized systems, organizations need to create policies for managing sensitive data. This could entail employing access control layers, encrypting files prior to distribution, or combining IPFS with blockchain technologies that prioritize privacy. Maintaining data integrity without jeopardizing confidentiality requires striking a balance between security and transparency.

6. CONCLUSION

Existing research indicates that the InterPlanetary File System (IPFS) is a decentralized file sharing platform that offers notable benefits in terms of data availability, safe information distribution, and resistance to censorship. IPFS makes possible a peer-to-peer network design that improves resilience and lowers single points of failure, in contrast to conventional file sharing systems that rely on centralized servers. This decentralized method makes files more accessible and less susceptible to server failures or censorship.


IPFS still has a number of significant issues that restrict its use and performance, despite its encouraging potential. Unstable access speeds, which can vary based on network circumstances and node availability,


are a significant problem. Additionally, to guarantee quicker and more dependable file retrieval, the effectiveness of data replication across nodes needs to be improved. The absence of an integrated incentive system to motivate nodes to retain and exchange data in a sustainable manner over time a crucial component for preserving the network's lifetime and health is another significant drawback.


To address these challenges, future research should focus on developing adaptive protocols to stabilize access speeds and optimize data replication strategies within the IPFS network. Investigating robust incentive systems, possibly leveraging blockchain-based token economies, could motivate greater participation and reliable data hosting by nodes. Furthermore, enhancing privacy protections and censorship resistance through advanced encryption and decentralized governance models will be vital for realizing IPFS's full potential as a secure and censorship free file sharing solution.

7. DECLARATIONS


7.1. About Authors

Nesti Anggraini Santoso (NA)  <https://orcid.org/0000-0001-9727-9092>

Palma Juanta (PJ)  <https://orcid.org/0009-0004-1990-7419>

Sabda Maulana (SM)  <https://orcid.org/0000-0002-0871-6463>

Kerimbekov Toktar (KT)  <https://orcid.org/0000-0002-4414-2102>

Aulia Khanza (AK)  <https://orcid.org/0009-0007-3736-4317>

7.2. Author Contributions

Conceptualization: NA, PJ, and SM; Methodology: KT; Software: AK; Validation: NA and PJ; Formal Analysis: SM and KT; Investigation: AK; Resources: PJ; Data Curation: NA; Writing Original Draft Preparation: NA and KT; Writing Review and Editing: AK; Visualization: PJ; All authors, NA, PJ, SM, KT, and AK, 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] S. M. Arafat, "A study of blockchain applications in the water sector," 2025, unpublished.
- [2] G. Jacqueline, Y. Putri Ayu Senjaya, M. Firli, and A. Bayu Yadila, "Application of SmartPLS in Analyzing Critical Success Factors for Implementing Knowledge Management in the Education Sector," *APTISI Transactions on Management (ATM)*, vol. 8, no. 1, pp. 49–57, 2024.
- [3] A. A. Ayare, V. A. Jadhav, M. K. Banatwala, S. V. Changlere, A. Mote, P. Joshi, A. A. A. Mr, V. A. J. 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.
- [4] L. Balduf, S. Henningsen, M. Florian, S. Rust, and B. Scheuermann, "Monitoring data requests in decentralized data storage systems: A case study of ipfs," in *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2022, pp. 658–668.
- [5] S. T. S. Alfian, F. Ichsanudin, N. Ndruru *et al.*, "Bitcoin and digital currency: Difficulties, open doors and future works," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 50–57, 2022.
- [6] D. F. G. Farinha, "An information system for the preservation of networked crypto art," Ph.D. dissertation, University of Saint Joseph Macau, 2025.

- [7] E. Grimson, "Report to the president for year ended june 30, 2024, open learning," MIT Open Learning, Tech. Rep., 2024.
- [8] R. Ahli, M. F. Hilmi, and A. Abudaqa, "Moderating effect of perceived organizational support on the relationship between employee performance and its determinants: A case of entrepreneurial firms in uae," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 199–212, 2024.
- [9] K. Huang, C. Parisi, L. J. Tan, W. Ma, and Z. W. Zhang, *Web3 Applications Security and New Security Landscape*. Springer, 2024.
- [10] V. Agarwal, M. Lohani, A. S. Bist, L. Rahardja, M. Hardini, and G. Mustika, "Deep cnn–real esrgan: An innovative framework for lung disease prediction," in *2022 IEEE Creative Communication and Innovative Technology (ICCIIT)*. IEEE, 2022, pp. 1–6.
- [11] K. Ito, "Cryptoeconomics and tokenomics as economics: A survey with opinions," 2024, arXiv preprint arXiv:2407.15715.
- [12] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.
- [13] 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.
- [14] J. Heikal, V. Rialialie, D. Rivelino, and I. A. Supriyono, "Hybrid model of structural equation modeling pls and rfm (recency, frequency and monetary) model to improve bank average balance," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 4, no. 1, pp. 1–8, 2022.
- [15] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Duta bahasa provinsi ntt berpotensi ikut memajukan sektor pa," 2025, accessed: 2025-06-19. [Online]. Available: <https://www.kemendikdasmen.go.id/berita/3793-duta-bahasa-provinsi-ntt-berpotensi-ikut-memajukan-sektor-pa>
- [16] I. Maria *et al.*, "Unlocking success: Human resource management for startupreneur," *Startupreneur Business Digital (SABDA Journal)*, vol. 3, no. 1, pp. 89–97, 2024.
- [17] E. Pebriyanti and O. Kusmayadi, "Brand ambassador and brand personality on decision to purchase nature republic in karawang," *APTISI Transactions on Management (ATM)*, vol. 6, no. 1, pp. 83–90, 2022.
- [18] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Upaya kemendikbudristek dalam membangun sdm unggul dan menja," 2025, accessed: 2025-06-19. [Online]. Available: <https://www.kemendikdasmen.go.id/berita/4673-upaya-kemendikbudristek-dalam-membangun-sdm-unggul-dan-menja>
- [19] B. Any, T. Ramadhan, E. A. Nabila *et al.*, "Decentralized academic platforms: The future of education in the age of blockchain," *Blockchain Frontier Technology*, vol. 3, no. 2, pp. 112–124, 2024.
- [20] Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, "Kompetisi pariwisata indonesia ke-14, polban gelorakan pariwi," 2025, accessed: 2025-06-19. [Online]. Available: <https://www.kemendikdasmen.go.id/berita/4795-kompetisi-pariwisata-indonesia-ke-14-polban-gelorakan-pariwi>
- [21] S. Septiani, P. Seviawani *et al.*, "Penggunaan big data untuk personalisasi layanan dalam bisnis e-commerce," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 5, no. 1, pp. 51–57, 2024.
- [22] C. H. Morales-Alarcón, E. Boderó-Poveda, H. M. Villa-Yáñez, and P. A. Buñay-Guisnián, "Blockchain and its application in the peer review of scientific works: A systematic review," *Publications*, vol. 12, no. 4, p. 40, 2024.
- [23] A. Ekawaty, E. A. Nabila, S. A. Anjani, U. Rahardja, and S. Zebua, "Utilizing sentiment analysis to enhance customer feedback systems in banking," in *2024 12th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2024, pp. 1–6.
- [24] C. Patsakis, "What's inside a node? malicious ipfs nodes under the magnifying glass," in *ICT Systems Security and Privacy Protection: 38th IFIP TC 11 International Conference, SEC 2023, Poznan, Poland, June 14–16, 2023, Revised Selected Papers*, vol. 679. Springer Nature, 2024, p. 149.
- [25] I. Shantilawati, O. I. Suri, R. A. Sunarjo, S. A. Anjani, and D. Robert, "Unveiling new horizons: Ai-driven decision support systems in hrm-a novel bibliometric perspective," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 252–263, 2025.
- [26] B. Prünster, A. Marsalek, and T. Zefferer, "Total eclipse of the heart–disrupting the InterPlanetary file system," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3735–3752.
- [27] U. Rahardja, N. Lutfiani, A. S. Rafika, and E. P. Harahap, "Determinants of lecturer performance to

- enhance accreditation in higher education,” in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2020, pp. 1–7.
- [28] S. Sridhar, O. Ascigil, N. Keizer, F. Genon, S. Pierre, Y. Psaras, E. Rivière, and M. Król, “Content censorship in the interplanetary file system,” 2023, arXiv preprint arXiv:2307.12212.
- [29] D. E. Rose, J. Van Der Merwe, and J. Jones, “Digital marketing strategy in enhancing brand awareness and profitability of e-commerce companies,” *APTISI Transactions on Management*, vol. 8, no. 2, pp. 160–166, 2024.
- [30] L. Balduf, S. Henningsen, M. Florian, S. Rust, and B. Scheuermann, “Monitoring data requests in decentralized data storage systems: A case study of ipfs,” *arXiv preprint arXiv:2104.09202*, 2021, case-study on IPFS privacy and network monitoring in blockchain context.
- [31] S. Sridhar, O. Ascigil, N. Keizer, F. Genon, S. Pierre, Y. Psaras, E. Rivière, and M. Król, “Content censorship in the interplanetary file system,” *arXiv preprint arXiv:2307.12212*, 2023, censorship attack, DHT vulnerabilities and mitigation in IPFS :contentReference[oaicite:1]index=1.
- [32] M.-V. Vladucu, H. Wu, J. Medina, K. M. Salehin, Z. Dong, and R. Rojas-Cessa, “Blockchain on sustainable environmental measures: A review,” *Blockchains*, vol. 2, no. 3, pp. 334–365, 2024.
- [33] A. Nuche, O. Sy, and J. C. Rodriguez, “Optimizing efficiency through sustainable strategies: The role of management and monitoring in achieving goals,” *APTISI Transactions on Management*, vol. 8, no. 2, pp. 167–174, 2024.
- [34] Z. Wu, B. Kondracki, N. Nikiforakis, and A. Balasubramanian, “Secrets are forever: Characterizing sensitive file leaks on ipfs,” in *2024 IFIP Networking Conference (IFIP Networking)*. IEEE, 2024, pp. 522–528.
- [35] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, “Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.
- [36] D. Trautwein, A. Raman, G. Tyson, I. Castro, W. Scott, M. Schubotz, B. Gipp, and Y. Psaras, “Design and evaluation of ipfs: A storage layer for the decentralized web,” *arXiv preprint arXiv:2208.05877*, 2022, evaluation of IPFS performance and scalability :contentReference[oaicite:2]index=2.
- [37] R. G. Munthe, M. Susan, and B. M. Sulungbudi, “The role of internal marketing in building organizational commitment and reducing turnover intention affecting the improved performance of life insurance agents in indonesia,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 1, pp. 56–71, 2024.
- [38] T. Tashev, “What is ipfs? interplanetary file system explained,” *Webopedia*, 2025, explains IPFS decentralization, content addressing, resistance to censorship :contentReference[oaicite:10]index=10.
- [39] N. Lutfiani, A. Ivanov, N. P. L. Santoso, S. V. Sihotang, and S. Purnama, “E-commerce growth plan for msme’s sustainable development enhancement,” *CORISINTA*, vol. 1, no. 1, pp. 80–86, 2024.
- [40] H. Chen, Y. Lu, and Y. Cheng, “Fileinsurer: A scalable and reliable protocol for decentralized file storage in blockchain,” *arXiv preprint arXiv:2207.11657*, 2022, iPFS-based insured storage layer for blockchain apps :contentReference[oaicite:3]index=3.
- [41] A. Grabowska, “Decentralized file storage systems: Studying decentralized file storage systems (e.g., ipfs, filecoin) for secure, censorship-resistant storage and sharing of digital content,” *Journal of AI-Assisted Scientific Discovery*, vol. 2, no. 2, 2024, survey on IPFS/Filecoin censorship-resistance :contentReference[oaicite:4]index=4.
- [42] S. Maulana, I. M. Nasution, Y. Shino, and A. R. S. Panjaitan, “Fintech as a financing solution for micro, small and medium enterprises,” *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 1, pp. 71–82, 2022.
- [43] U. o. V. Department of Computer Science, “Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain,” *Future Internet*, vol. 16, no. 3, p. 98, 2024, iPFS+blockchain + encryption for availability and privacy :contentReference[oaicite:5]index=5.
- [44] unknown, “Ipfs-based blockchain solution for secure and efficient data sharing,” *ResearchGate / journal*, 2025, framework encrypt-fragment-hash store via IPFS + blockchain :contentReference[oaicite:6]index=6.
- [45] E. Pradivta, A. S. Rafika, A. Faturahman, and W. N. Wahid, “Peran nilai-nilai islam dalam transformasi sosial pada era teknologi,” *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 2, no. 1, pp. 24–33, 2025.
- [46] M. Mardiana, F. Ariyanto, D. Andayani, and A. Adiwijaya, “Pendekatan teologi islam dalam menghadapi

- masalah sosial modern,” *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 2, no. 1, pp. 34–43, 2025.
- [47] B. Nielson, “Unraveling the mysteries of the interplanetary file system (ipfs),” *The Blockchain Academy*, 2024, overview of IPFS benefits including censorship resistance :contentReference[oaicite:7]index=7.
- [48] D. Ambolis, “Ipfs blockchain use cases that could redefine the web,” *Blockchain Magazine*, 2025, iPFS use cases for censorship-resistance in blockchain ecosystems :contentReference[oaicite:8]index=8.
- [49] B. E. Sibarani, C. Anggreani, B. Artasya, and D. A. P. Harahap, “Unraveling the impact of self-efficacy, computer anxiety, trait anxiety, and cognitive distortions on learning mind your own business: The student perspective,” *APTISI Transactions on Technopreneurship (ATT)*, vol. 6, no. 1, pp. 29–40, March 2024. [Online]. Available: <https://doi.org/10.34306/att.v6i1.377>
- [50] M. . F. Foundation, “Web3’s library of alexandria: News and civic documents to be backed up on decentralized web,” *Axios News*, 2022, use of IPFS+blockchain to resist censorship of civic documents :contentReference[oaicite:9]index=9.