Blockchain Frontier Technology (BFRONT)
Vol. 5, No. 2, 2026, pp. 172∼181
E-ISSN: 2808-0009 P-ISSN: 2808-0831, DOI:10.34306

Blockchain Integration to Enhance Federated Learning Model Integrity

Yane Devi Anna[1], Sherli Triandari[2*], Sigit Anggoro[3], Ardirra Yolandita[4], Adele Valerry[5]
[1]Department of Accounting, Universitas Ekuitas, Indonesia
[2, 4]Faculty of Science and Technology, University of Raharja, Indonesia
[3]Department of Information System, Universitas Jenderal Achmad Yani, Indonesia
[5]Department of Science and Technology, ILearning Incorporation, Colombia
[1]yane.devi@ekuitas.ac.id, [2]sherli@raharja.info, [3]sigit.anggoro@lecture.unjani.ac.id, [4]ardirra@raharja.info, [5] vallery.adele@ilearning.co
***Corresponding Author**

Article Info

Article history:

Submission, 16-10-2025
Revised, 14-11-2025
Accepted, 29-12-2025

Keywords:

Blockchain
Federated Learning
Model Integrity
Smart Contracts
Transparency



ABSTRACT

Federated Learning is a distributed machine learning approach that enables model training without transferring raw data, thereby preserving user privacy. To improve conciseness, overlapping explanations of FL's privacy benefits across the Abstract, Introduction, and Literature Review have been consolidated, highlighting its importance in **sensitive domains** while removing redundancy. This allows greater emphasis on the study's **novelty**, particularly the Smart Contract design featuring multi-layer verification and reputation checking mechanisms. Despite its advantages, FL faces significant challenges related to model integrity, including parameter manipulation, model poisoning attacks, and limited trust among participating nodes. This study **explores the integration** of blockchain technology to address these issues. Leveraging decentralization, immutability, and transparency, blockchain is used to validate model updates, record contributions, and manage node reputation. The study employs a literature review and technical architecture design for a blockchain-integrated FL system. The **results indicate** that blockchain implementation enhances the reliability and security of FL training, especially in low-trust environments, with strong relevance for healthcare, finance, and IoT applications.

This is an open access article under the CC BY 4.0 license.



DOI: https://doi.org/10.34306/bfront.v5i2.929
This is an open-access article under the CC-BY license (https://creativecommons.org/licenses/by/4.0/
©Authors retain all copyrights

1. INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) and Machine Learning (ML) technologies has led to the emergence of new approaches in data processing, one of which is Federated Learning (FL) [1, 2]. FL is a distributed model training method that allows data to remain on local devices, thereby preserving user privacy [3]. This approach is highly relevant to sensitive sectors such as healthcare, finance, and the IoT, where data protection is a top priority. However, despite its advantages in terms of privacy, FL still faces serious challenges regarding model integrity and trust among training nodes [4, 5].

One of the main issues in FL is the potential for attacks such as model poisoning and parameter manipulation by untrusted nodes [6]. In environments involving multiple parties both individuals and institutions, it is difficult to ensure that every participant provides valid and honest contributions during the training process [7]. Therefore, a mechanism is needed to enable transparent, tamper proof auditing, verification, and contribution tracking. This topic directly aligns with the IEEE scope in computing and communication systems, particularly

within secure and distributed machine learning architectures [8]. The study's emphasis on Blockchain integration to ensure transparency, immutability, and trust in FL contributes to ongoing IEEE research directions in privacy preserving AI, IoT, and decentralized network infrastructures [9, 10].

In this context, blockchain technology emerges as a potential solution to enhance the security and integrity of FL systems [11]. At the national level, the Government of Indonesia has formally recognized blockchain technology as part of the national digital infrastructure, supporting its adoption for secure, transparent, and accountable digital systems [12]. With its core characteristics decentralization, transparency, and immutability blockchain has great potential to be integrated into FL architectures to securely record every process and contribution [13]. The use of blockchain can create a trust layer that ensures each model parameter update is chronologically recorded and immutable while enabling reputation evaluation for all participating nodes [14, 15]. Hence, this study aims to explore how blockchain integration can strengthen model integrity in FL and propose a conceptual technical architecture as a solution to the existing challenges [16]. To enhance readability and conceptual focus, redundant descriptions of blockchain's benefits such as transparency, immutability, and decentralization have been condensed [17]. The revised narrative now highlights how these characteristics directly support model integrity and trust in FL systems [18]. Furthermore, the terminology "technical architecture" has been consistently replaced with "conceptual architecture" throughout the paper to accurately reflect the theoretical and design oriented nature of this research [19, 20].

Based on the identified challenges in ensuring model integrity and trust in FL systems, this study seeks to address the following research questions:

- Can smart contracts be utilized within blockchain networks to validate and secure model parameter updates in Federated Learning?
- What are the essential architectural components required to effectively integrate blockchain as a trust and verification layer in Federated Learning environments?

Ultimately, this research is expected to contribute to the development of a more secure, transparent, and accountable Federated Learning ecosystem by leveraging blockchain's capabilities in decentralization and trust management [21]. The proposed conceptual architecture will not only serve as a foundational framework for designing future blockchain-based FL systems but also provide practical insights into mitigating security threats and improving collaboration efficiency among distributed participants [16]. Moreover, this study aims to bridge the gap between theoretical models and real-world implementation by outlining how blockchain mechanisms, such as consensus algorithms and smart contract automation, can be adapted to support scalable, privacy-preserving, and verifiable learning environments [22, 23]. Through this approach, it is anticipated that the integration of blockchain and Federated Learning will pave the way for more trustworthy and ethically responsible AI systems in various domains [24, 9].

In addition, this study aligns with the United Nations Sustainable Development Goals (SDGs), particularly SDGs 9 (Industry, Innovation, and Infrastructure), SDGs 16 (Peace, Justice, and Strong Institutions), and SDGs 17 (Partnerships for the Goals). The integration of blockchain technology into Federated Learning supports the development of resilient digital infrastructure and promotes innovation by enabling secure, transparent, and trustworthy collaborative AI systems. By ensuring model integrity, accountability, and trust among distributed participants, the proposed architecture contributes to stronger institutional governance in data-driven environments. Furthermore, the decentralized and collaborative nature of blockchain-enabled Federated Learning encourages cross-institutional partnerships while preserving data privacy, making it especially relevant for sustainable digital transformation in sensitive sectors such as healthcare, finance, and smart infrastructure.

2. LITERATURE REVIEW

2.1. Federated Learning: Concepts, Advantages, and Challenges

FL is a machine learning approach that enables model training to be carried out collaboratively by multiple devices or institutions without transferring data to a central server [25]. Thus, FL is highly suitable for scenarios that require a high level of privacy, such as in the medical, financial, and edge computing fields [26, 27]. Although it offers advantages in terms of privacy, FL still faces several major challenges, particularly related to data and model integrity [28]. One of the main challenges is the potential for malicious contributions from participating nodes, such as model poisoning attacks and the submission of unauthorized parameters,

which can degrade the performance and validity of the global model [29, 30]. Therefore, mechanisms are needed to verify and maintain the integrity of each participant's contribution in FL. The explanation is illustrated in Figure 1.

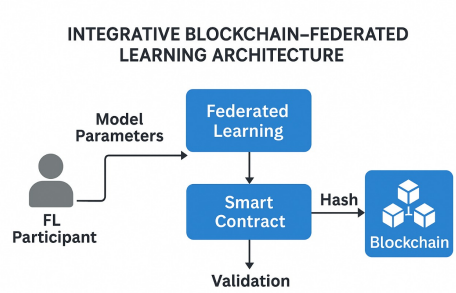


Figure 1. Integration of Blockchain as a Trust Layer in Federated Learning

Figure 1 provides an overview of the key elements of Federated Learning, covering its concept, advantages, and challenges. The figure highlights that FL enables multiple participants to collaboratively train a machine learning model without sharing raw data, thereby ensuring privacy. In addition, FL offers several advantages, particularly in sectors that require strict data protection such as healthcare, finance, and edge computing. However, the figure also emphasizes that despite its privacy benefits, FL still faces challenges related to data integrity and security. Therefore, mechanisms for validating and securing model updates are essential to maintain the reliability of the global model.

2.2. Blockchain: Features and Applications in Distributed Systems

Blockchain is a distributed technology that enables secure, transparent, and immutable data recording [31]. Features such as decentralization, distributed consensus, and cryptographic hashing make blockchain suitable for applications that require high security and auditability [32]. In recent years, blockchain has been applied in various sectors, including logistics, finance, voting systems, and supply chain management [33, 34]. In the context of Federated Learning, blockchain can be used to record and track all model update activities, maintain contribution history, and prevent data manipulation or falsification by participants [11]. Furthermore, smart contracts on the blockchain can be utilized to establish automatic verification mechanisms for submitted model parameters [35].

2.3. Current Studies and Research Gaps

The integration between Blockchain and FL is a relatively new yet rapidly growing research field [36]. Several studies have attempted to combine these two technologies to build secure, decentralized, and trustworthy AI systems [37, 38]. These studies show that blockchain can provide a trust layer within FL systems, assisting in model contribution tracking, parameter validation, and participation incentives through tokenization [39, 40]. However, several gaps remain to be addressed, such as issues of scalability, system complexity, and communication efficiency. There are still few studies that specifically examine the design of technical architectures for FL + Blockchain systems that can operate efficiently in multi-participant environments [41]. Therefore, this article seeks to fill that gap by proposing a conceptual and technical approach to integrating blockchain into Federated Learning systems [42, 43]. From a theoretical perspective, the proposed conceptual architecture is grounded in distributed trust and consensus principles inspired by Byzantine Fault Tolerance (BFT) models, which assume the presence of potentially unreliable or malicious nodes in the network. The blockchain layer functions as a consensus mechanism to mitigate Byzantine behaviors through immutable logging and decentralized verification [44]. Additionally, the incentive aspect aligns with game-theoretic concepts, where rational nodes are motivated to behave honestly to maximize their long-term reputation and reward outcomes. This formal grounding reinforces the system's theoretical robustness and aligns the conceptual design with foundational principles in distributed system reliability and trust management [45].

3. METHODOLOGY

This study employs a qualitative descriptive approach using a literature review and conceptual system design method. The primary objective of this method is to explore, analyze, and synthesize various scholarly sources discussing the integration between FL and Blockchain, as well as to design a technical architecture framework that can enhance model integrity within Federated Learning scenarios [46, 47].

3.1. Type and Research Approach

This research is exploratory and descriptive in nature, employing a technical conceptual approach. The study does not focus on direct implementation through coding or simulation but rather on developing a system framework that can serve as a reference for future implementations [48, 49]. This study is positioned as a System Framework Paper, emphasizing the conceptual integration of blockchain and federated learning within a structured theoretical model. Rather than presenting empirical data or simulation outcomes, it synthesizes existing literature to develop a framework that can guide future technical implementations [50]. The objective is to provide a conceptual foundation that identifies architectural components, trust mechanisms, and integration logic for blockchain-enabled federated learning systems [51, 52].

3.2. Data Sources and Collection Techniques

The data for this study were obtained through a comprehensive literature review from various relevant sources. These sources included international scientific journal articles from publishers such as IEEE, Springer, and ACM, as well as technology whitepapers discussing Blockchain and Federated Learning [53]. Additionally, technical documentation from open source platforms such as TensorFlow Federated, Hyperledger, and IPFS was utilized, along with case studies and reports on similar system developments [54, 55]. The data collection process involved compiling and selecting relevant literature, which was then analyzed based on key themes, including the security of Federated Learning, the role of blockchain in ensuring data integrity, and the integrative architecture of FL Blockchain systems.

3.3. Data Analysis Technique

The data were analyzed using a thematic analysis approach consisting of several structured steps. First, data reduction was conducted by filtering and refining information from relevant sources to ensure accuracy, quality, and relevance. Next, thematic categorization was carried out by grouping the extracted information according to major themes such as model security, contribution validation, and system architecture. Finally, concept synthesis was performed to develop conceptual solutions and design an integration framework that connects FL and blockchain based on the synthesized findings from the reviewed literature.

Table 1. Thematic Analysis Process

Stage	Description	Purpose/Outcome
Data Reduction	Filtering and refining information from relevant sources to ensure the inclusion of only high-quality and contextually relevant studies.	To eliminate redundant or non-relevant data and retain the most credible sources for analysis.
Thematic Categorization	Grouping the extracted information according to major themes such as model security, contribution validation, and system architecture.	To organize findings into key analytical categories that align with the research focus.
Concept Synthesis	Developing conceptual solutions and designing the integration framework between Federated Learning and Blockchain based on the synthesized findings.	To produce a comprehensive conceptual framework that connects literature insights into a unified system design.

The Table 1 above explains the thematic analysis process used in the study, which consists of three main stages data reduction, thematic categorization, and concept synthesis. In the data reduction stage, information from various sources is filtered to include only high quality and relevant studies, ensuring that the

analysis is based on credible data. The thematic categorization stage involves organizing the extracted information into key themes such as model security, contribution validation, and system architecture to align the findings with the main research focus. Finally, in the concept synthesis stage, the researcher integrates these themes to develop a comprehensive conceptual framework that illustrates how FL and Blockchain can be effectively combined into a unified system design.

4. RESULT AND DISCUSSION

4.1. Integrative Architecture Design of Blockchain Federated Learning

The study proposes a conceptual architecture that integrates Blockchain technology into FL to enhance data integrity, transparency, and trust during the model training process. The architecture focuses on the logical interaction between FL nodes and the blockchain network rather than on full technical implementation. Each model update is hashed using cryptographic functions and verified by smart contracts, which check contributor metadata such as ID, timestamp, and accuracy threshold before aggregation. A key innovation of this design lies in its multi-layer verification logic within smart contracts. These contracts not only record hashes but also validate model parameters, assess node reliability through a reputation ledger, and enforce differential privacy constraints to prevent malicious updates. This structured trust and privacy aware validation system differentiates the model from previous Blockchain FL integrations. To overcome scalability and latency challenges, the architecture adopts an off chain data management approach, storing large model parameters in distributed systems like IPFS, while keeping only hashes and validation metadata on the blockchain. This approach maintains transparency and verifiability while reducing network overhead. Overall, the proposed architecture serves as a theoretical framework that ensures data security, privacy preservation, and auditability within decentralized AI environments, aligning with IEEE's principles of efficient and trustworthy system design.

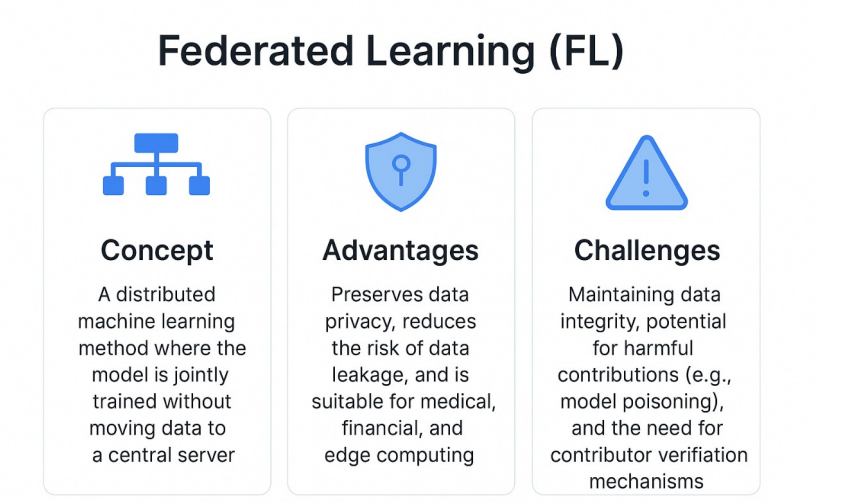


Figure 2. Integrative Architecture of Blockchain-Federated Learning

The diagram in Figure 2 illustrates the integration of Blockchain into FL, where each node trains a local model and submits the model parameters for verification via a smart contract, recording them as a hash on the blockchain. This process ensures data integrity, transparency, and security by preventing unauthorized changes, malicious contributions, and model poisoning, while also maintaining the privacy of local data. By leveraging blockchain, Federated Learning becomes more secure, reliable, and suitable for applications in sensitive sectors like healthcare, finance, and edge computing, offering a robust solution for decentralized machine learning.

4.2. Functional Advantages of the Resulting System

The integration of Blockchain and FL in the proposed architecture provides several significant advantages. First, the integrity of model parameters is preserved, as every contribution is recorded on the blockchain

and cannot be tampered with. Second, the system becomes more transparent, since the entire history of model updates can be traced by all participants through the blockchain ledger. Third, the implementation of smart contracts enables parameter validation processes to be conducted automatically and consistently, without manual intervention. Fourth, this approach opens the opportunity to implement reputation based incentive mechanisms, where nodes that consistently provide valid contributions can be rewarded, while suspicious nodes may have their contributions restricted.

Table 2. Advantages of Blockchain in Model Management

Advantage	**Description**
Model Integrity	Each model update is securely recorded on the blockchain, preventing tampering or data manipulation.
Transparency	All participants can trace the full history of model updates through the blockchain ledger.
Automated Validation	Smart contracts automatically validate parameters, ensuring consistency without manual intervention.
Reputation-Based Incentives	Nodes providing valid contributions can earn rewards, while unreliable nodes face contribution limits.

Table 2 highlights the main advantages of integrating Blockchain with Federated Learning. Blockchain ensures model integrity by preventing data tampering, promotes transparency through traceable updates, enables automated validation via smart contracts, and supports reputation-based incentives that reward reliable participants while limiting untrustworthy ones. Overall, these features enhance the system's security, trust, and efficiency.

4.3. Analysis of Challenges and Limitations

Although the proposed architecture offers solutions to the issue of model integrity in FL, several challenges must be considered. One challenge is the increased system complexity due to the addition of the blockchain layer, affecting both inter node communication and transaction management. Furthermore, public blockchains such as Ethereum have limitations in terms of throughput and transaction costs, making private or permissioned blockchains like Hyperledger potentially more suitable for this system. Another challenge is latency during the verification and aggregation processes, particularly at large scales with a high number of nodes. Therefore, real world implementation of this system requires adjustments and optimizations based on the specific needs of the sector or use case.

An important trade-off arises when adopting a private or permissioned blockchain to mitigate latency and throughput limitations. While such frameworks enhance performance and scalability, they may partially reduce decentralization by introducing controlled access and centralized governance over node participation. This shift transitions the trust model from a fully trustless consensus to a semi-trusted environment relying on preauthorized nodes for validation. Nevertheless, transparency and auditability can still be preserved through appropriate cryptographic proof mechanisms and distributed access policies. Recognizing this balance between efficiency and decentralization is essential for applying the proposed architecture in real-world multi-institutional Federated Learning scenarios. It should be noted that these observations are derived from a synthesis of existing scholarly works rather than empirical testing. Consequently, the identified challenges including latency, transaction costs, and communication complexity should be interpreted as theoretical insights guiding future experimental research.

Overall, the study's findings indicate that integrating blockchain into FL provides a potential solution to address FL's key weaknesses, namely the lack of contribution verification mechanisms and vulnerability to model manipulation. The proposed system ensures integrity, transparency, and trust crucial aspects in the development of secure and responsible collaborative AI systems. However, the full effectiveness of this system can only be demonstrated through real world implementation and testing across various contexts.

5. MANAGERIAL IMPLICATIONS

The integration of blockchain into Federated Learning provides strategic value for organizations that manage sensitive, distributed, or cross-institutional data. Managers in sectors such as healthcare, finance,

education, and IoT can utilize the proposed architecture to establish a verifiable audit trail that strengthens compliance, transparency, and accountability. The use of smart contracts to automate parameter validation reduces operational risks associated with human error, minimizes opportunities for data manipulation, and ensures that only high-quality model updates are accepted in the learning process. This contributes to more reliable decision-making within organizations by ensuring that AI models are trained using trustworthy and validated contributions.

From an operational and governance perspective, the system's reputation-based mechanism enables managers to incentivize honest participation while restricting unreliable nodes, creating a more stable and performance-oriented collaborative ecosystem. The use of off-chain storage and modular architectural components also allows organizations to optimize resource allocation and adapt the system to their technical capacity. However, implementing this integration requires managers to carefully balance the trade-off between decentralization and efficiency, especially when choosing between public and permissioned blockchain platforms. These considerations underscore the importance of managerial decision-making in ensuring the sustainable adoption, governance, and scalability of blockchain-enabled Federated Learning systems.

6. CONCLUSION

This research successfully designed an integrative architecture that combines blockchain technology with FL to enhance the integrity of the training model. By utilizing blockchain as a transparent and immutable trust layer, the system can securely record and verify each participant node's contribution. The proposed architecture conceptually demonstrates the potential to enhance integrity, transparency, and trust within Federated Learning systems through blockchain integration. While the design provides a strong theoretical foundation, these benefits remain at a conceptual stage and require empirical validation through real world implementation or simulation studies. The integration, therefore, creates a reliable and transparent framework for auditability rather than a fully verified technical solution. The use of smart contracts strengthens the automatic validation of model parameters, preventing manipulation and preserving the authenticity of the data used in the distributed learning process.

The main advantage of this integration lies in creating a learning system that not only protects user data privacy but also provides a clear and reliable audit mechanism. The transparency enabled by blockchain allows for complete traceability of the model training history while also opening opportunities for implementing a reputation based incentive system to improve the quality of contributions. This represents an important step in addressing the main challenges of FL, particularly regarding the security and reliability of the resulting model.

However, the real world implementation of this system faces several challenges, such as increased system complexity, verification latency, and performance limitations in public blockchains. Therefore, future research is recommended to focus on developing a prototype with technical optimizations, including selecting the appropriate blockchain platform and testing at a large scale. In doing so, the potential of the proposed blockchain-integrated Federated Learning architecture for scalable, efficient, and trustworthy real-world deployment can be empirically evaluated.

7. DECLARATIONS

7.1. About Authors

Yane Devi Anna (YD) https://orcid.org/0009-0001-1909-5105
Sherli Triandari (ST) https://orcid.org/0009-0007-9323-4373
Sigit Anggoro (SA) https://orcid.org/0009-0008-3161-86352
Ardirra Yolandita (AY) https://orcid.org/0009-0001-9358-3588
Adele Valerry (AV) https://orcid.org/0009-0009-1433-1058

7.2. Author Contributions

Conceptualization: YD, ST, and SA; Methodology: AY; Software: AV; Validation: AV and YD; Formal Analysis: SA and ST; Investigation: YD; Resources: AY; Data Curation: AY; Writing Original Draft

Preparation: ST and YD; Writing Review and Editing: SA; Visualization: AV; All authors, YD, ST, SA, AY and AV, 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. Shen, T. Zhu, D. Wu, W. Wang, and W. Zhou, "From distributed machine learning to federated learning: In the view of data privacy and security," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 16, p. e6002, 2022.

[2] M. Hatta, W. N. Wahid, F. Yusuf, F. Hidayat, N. A. Santoso, and Q. Aini, "Enhancing predictive models in system development using machine learning algorithms," *International Journal of Cyber and IT Service Management*, vol. 4, no. 2, pp. 80–87, 2024.

[3] T. Z. Sana, S. Abdulla, A. Das, A. Nag, M. M. Hassan, Z. Z. Fiza, A. Karim, and S. R. R. Kabir, "Advancing federated learning: A systematic literature review of methods, challenges, and applications," *IEEE Access*, 2025.

[4] D. Chen, X. Jiang, H. Zhong, and J. Cui, "Building trusted federated learning: Key technologies and challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 1, p. 13, 2023.

[5] R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, "Privacy and security in federated learning: A survey," *Applied Sciences*, vol. 12, no. 19, p. 9901, 2022.

[6] P. R. Ovi and A. Gangopadhyay, "Robust federated learning against data poisoning attacks: Prevention and detection of attacked nodes," *Electronics*, vol. 14, no. 15, p. 2970, 2025.

[7] 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.

[8] S. El-Gendy, M. S. Elsayed, A. Jurcut, and M. A. Azer, "Privacy preservation using machine learning in the internet of things," *Mathematics*, vol. 11, no. 16, p. 3477, 2023.

[9] Z. Yang, Y. Shi, Y. Zhou, Z. Wang, and K. Yang, "Trustworthy federated learning via blockchain," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 92–109, 2022.

[10] D. Hidayati, A. Andriyansah, G. P. Cesna, A. Y. Fauzi, D. Apriliasari, and U. Rahardja, "Building efficient iot systems with edge computing integration," *International Journal of Cyber and IT Service Management*, vol. 4, no. 2, pp. 72–79, 2024.

[11] L. Wu, W. Ruan, J. Hu, and Y. He, "A survey on blockchain-based federated learning," *Future Internet*, vol. 15, no. 12, p. 400, 2023.

[12] Government of the Republic of Indonesia, "Government regulation of the republic of indonesia number 28 of 2025 on the recognition and utilization of blockchain technology as national digital infrastructure," 2025, official government policy. [Online]. Available: https://indodax.com/academy/blockchain-resmi-diakui-indonesia-pp-28-2025/

[13] W. Ning, Y. Zhu, C. Song, H. Li, L. Zhu, J. Xie, T. Chen, T. Xu, X. Xu, and J. Gao, "Blockchain-based federated learning: A survey and new perspectives." *Applied Sciences (2076-3417)*, vol. 14, no. 20, 2024.

[14] G. Peng, X. Shi, J. Zhang, L. Gao, Y. Tan, N. Xiang, and W. Wang, "Bgfl: a blockchain-enabled group federated learning at wireless industrial edges," *Journal of Cloud Computing*, vol. 13, no. 1, p. 148, 2024.

[15] U. Rahardja, A. N. Hidayanto, P. O. H. Putra, and M. Hardini, "Immutable ubiquitous digital certificate authentication using blockchain protocol," *Journal of applied research and technology*, vol. 19, no. 4, pp. 308–321, 2021.

[16] X. Liang, J. Zhao, Y. Chen, E. Bandara, and S. Shetty, "Architectural design of a blockchain-enabled, federated learning platform for algorithmic fairness in predictive health care: design science study," *Journal of medical Internet research*, vol. 25, p. e46547, 2023.
[17] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: a systematic literature review," *Artificial Intelligence Review*, vol. 56, no. 5, pp. 3951–3985, 2023.
[18] J. Yang, W. Zhang, Z. Guo, and Z. Gao, "Trustdfl: A blockchain-based verifiable and trusty decentralized federated learning framework," *Electronics*, vol. 13, no. 1, p. 86, 2023.
[19] Y. E. Oktian and S.-G. Lee, "Blockchain-based federated learning system: A survey on design choices," *Sensors*, vol. 23, no. 12, p. 5658, 2023.
[20] 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.
[21] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," *Journal of Big Data*, vol. 12, no. 1, p. 55, 2025.
[22] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing, and D. Dou, "Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning," *Knowledge and Information Systems*, vol. 66, no. 8, pp. 4377–4403, 2024.
[23] Z. Xie and Z. Li, "A blockchain multi-chain federated learning framework for enhancing security and efficiency in intelligent unmanned ports," *Electronics*, vol. 13, no. 24, p. 4926, 2024.
[24] I. B. Ababio, J. Bieniek, M. Rahouti, T. Hayajneh, M. Aledhari, D. C. Verma, and A. Chehri, "A blockchain-assisted federated learning framework for secure and self-optimizing digital twins in industrial iot," *Future Internet*, vol. 17, no. 1, p. 13, 2025.
[25] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and open problems in federated learning," *Foundations and trends® in machine learning*, vol. 14, no. 1–2, pp. 1–210, 2021.
[26] J. Wen, Z. Zhang, Y. Lan, Z. Cui, J. Cai, and W. Zhang, "A survey on federated learning: challenges and applications," *International journal of machine learning and cybernetics*, vol. 14, no. 2, pp. 513–535, 2023.
[27] N. M. Eshwarappa, H. Baghban, C.-H. Hsu, P.-Y. Hsu, R.-H. Hwang, and M.-Y. Chen, "Communication-efficient and privacy-preserving federated learning for medical image classification in multi-institutional edge computing," *Journal of Cloud Computing*, vol. 14, no. 1, p. 44, 2025.
[28] J. Wu, J. Jin, and C. Wu, "Challenges and countermeasures of federated learning data poisoning attack situation prediction," *Mathematics*, vol. 12, no. 6, p. 901, 2024.
[29] L. Shi, Z. Chen, Y. Shi, L. Wei, Y. Tao, M. He, Q. Wang, Y. Zhou, and Y. Gao, "Mphm: Model poisoning attacks on federal learning using historical information momentum," *Security and Safety*, vol. 2, p. 2023006, 2023.
[30] C. Zhu, S. Roos, and L. Y. Chen, "Leadfl: Client self-defense against model poisoning in federated learning," in *International Conference on Machine Learning*. PMLR, 2023, pp. 43 158–43 180.
[31] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," *PeerJ Computer Science*, vol. 9, p. e1705, 2023.
[32] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, p. 30, 2023.
[33] M. Mvubu and M. J. Naude, "Blockchain in the logistics sector: A systematic literature review of benefits and constraints," *Journal of Transport and Supply Chain Management*, vol. 18, pp. 1–10, 2024.
[34] Y. P. A. Sanjaya and M. A. Akhyar, "Blockchain and smart contract applications can be a support for msme supply chain finance based on sharia crowdfunding," *Blockchain Frontier Technology*, vol. 2, no. 1, pp. 44–49, 2022.
[35] G. Keshavarzkalhori, C. Perez-Sola, G. Navarro-Arribas, J. Herrera-Joancomarti, and H. Yajam, "Federify: A verifiable federated learning scheme based on zksnarks and blockchain," *IEEE Access*, vol. 12, pp. 3240–3255, 2023.
[36] M. Shawkat, A. El-desoky, Z. H. Ali, and M. Salem, "Blockchain and federated learning based on aggregation techniques for industrial iot: A contemporary survey," *Peer-to-Peer Networking and Applications*,

vol. 18, no. 4, p. 192, 2025.
[37] M. S. Al Jasem, T. De Clark, and A. K. Shrestha, "Toward decentralized intelligence: A systematic literature review of blockchain-enabled ai systems," *Information*, vol. 16, no. 9, p. 765, 2025.
[38] D. Ressi, R. Romanello, C. Piazza, and S. Rossi, "Ai-enhanced blockchain technology: A review of advancements and opportunities," *Journal of Network and Computer Applications*, vol. 225, p. 103858, 2024.
[39] C. Ying, F. Xia, D. S. Wei, X. Yu, Y. Xu, W. Zhang, X. Jiang, H. Jin, Y. Luo, T. Zhang *et al.*, "Bit-fl: Blockchain-enabled incentivized and secure federated learning framework," *IEEE Transactions on Mobile Computing*, 2024.
[40] H. T. Sukmana, A. E. Widjaja, and H. J. Situmorang, "Game theoretical-based logistics costs analysis: A review," *International Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 43–61, 2022.
[41] A. P. Kalapaaking, I. Khalil, M. S. Rahman, M. Atiquzzaman, X. Yi, and M. Almashor, "Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1703–1714, 2022.
[42] Y. Abuzied, M. Ghanem, F. Dawoud, H. Gamal, E. Soliman, H. Sharara, and T. Elbatt, "A privacy-preserving federated learning framework for blockchain networks," *Cluster Computing*, vol. 27, no. 4, pp. 3997–4014, 2024.
[43] H. Zhang, S. Jiang, and S. Xuan, "Decentralized federated learning based on blockchain: concepts, framework, and challenges," *Computer Communications*, vol. 216, pp. 140–150, 2024.
[44] 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.
[45] Government of the Republic of Indonesia, "Government regulation of the republic of indonesia number 28 of 2025 on the recognition and utilization of blockchain technology as national digital infrastructure," https://indodax.com/academy/blockchain-resmi-diakui-indonesia-pp-28-2025/, 2025, accessed: December 3, 2025.
[46] B. SERROUKH, A. EL KHAZZAR, and S. RAKOMA, "Framework for blockchain-based federated learning integration into port community system: A literature review," *Revue Internationale des Sciences de Gestion*, vol. 8, no. 3, 2025.
[47] 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.
[48] M. Wahyudi, T. A. A. Sandi, W. Bismi, U. Rahardja, L. Pujiastuti *et al.*, "Performance analysis of open shortest path first multiarea using virtual link method," in *2023 11th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2023, pp. 1–5.
[49] J. Paramboor, A. K. Effendi Kamaruddin, and S. H. Vazhathodi Al-Hudawi, "A conceptual framework for enhancing academic research writing: Integrating context-specific guidance and swale's cars model," 2025.
[50] A. Eiji and S. Mehta, "Simulation-based 5g femtocell network system performance analysis," *International Journal of Cyber and IT Service Management*, vol. 3, no. 1, pp. 74–78, 2023.
[51] B. Liu and Q. Tang, "Secure data sharing in federated learning through blockchain-based aggregation," *Future Internet*, vol. 16, no. 4, p. 133, 2024.
[52] X. Yin, X. Wu, and X. Zhang, "A trusted federated learning method based on consortium blockchain," *Information*, vol. 16, no. 1, p. 14, 2024.
[53] R. G. Munthe, M. Abbas, R. Fernandez, and N. Ulita, "The impact of educational information systems on learning accessibility in higher education," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 94–103, 2024.
[54] E. Goh, D.-Y. Kim, K. Lee, S. Oh, J.-E. Chae, and D.-Y. Kim, "Blockchain-enabled federated learning: A reference architecture design, implementation, and verification," *IEEE Access*, vol. 11, pp. 145 747–145 762, 2023.
[55] Y. Li, Y. Yan, Z. Liu, C. Yin, J. Zhang, and Z. Zhang, "A federated learning method based on blockchain and cluster training," *Electronics*, vol. 12, no. 19, p. 4014, 2023.