Grenze International Journal of Engineering and Technology, June Issue

A Review of Blockchain-Enabled Federated Learning Systems for Privacy-Preserving Artificial Intelligence

Deven Randhir[1], Swapnil Durafe[2], Mrunal Patil[3] and Tushar Waykole[4]
[1-4]Department of Computer Engineering, PCET's Nutan Maharashtra Institute of Engineering and Technology, Pune, India
Email: devenrandhir9821@gmail.com, swapnildurafe1702@gmail.com, mrunalp220@gmail.com, tushar.waykole@nmiet.edu.in

***Abstract*— Recent advancements in intelligent computing techniques have significantly influenced the development of data-driven and automated systems across various application domains. As the volume and complexity of data continue to increase, selecting appropriate models and techniques has become a critical challenge for researchers and practitioners. This paper presents a comprehensive review of prominent intelligent and computational approaches reported in recent literature, focusing on their underlying principles, performance characteristics, and application suitability. The review systematically analyzes existing methods, highlighting their strengths, limitations, and comparative effectiveness based on key evaluation parameters. By examining multiple studies and frameworks, this work identifies common trends and recurring challenges associated with scalability, accuracy, and computational efficiency. Furthermore, the paper emphasizes existing research gaps and limitations that restrict the practical adoption of current approaches in real-world scenarios. The insights derived from this review aim to assist researchers in understanding the current state of the art and selecting suitable techniques for specific problem domains. Finally, potential future research directions are outlined to address the identified gaps and to encourage the development of more robust, efficient, and adaptive intelligent systems.**

***Index Terms*— Blockchain, Federated Learning, Artificial Intelligence, Collaborative Machine Learning.**

I. INTRODUCTION

Artificial Intelligence (AI) has become a fundamental driver of digital transformation across modern enterprises, enabling data-driven decision-making, personalized services, intelligent automation, and optimized operational workflows. The effectiveness of contemporary AI systems relies heavily on the availability of high-quality, diverse, and large-scale datasets. However, in real-world business ecosystems, data is typically distributed among multiple organizations—such as hospitals, banks, retail chains, logistics providers, and governmental institutions—each governed by strict privacy policies, compliance requirements, and proprietary data ownership constraints. Regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and industry-specific confidentiality agreements further limit inter-organizational data sharing.

Federated Learning (FL) emerged as an important paradigm to enable collaborative model training without transferring raw data to a central location.

Grenze ID: 01.GIJET.12.2.502

In FL, multiple participants locally train model updates and send only gradients or model parameters to a central server for aggregation. While this approach preserves data privacy to some extent, it still depends on a centralized aggregator, which introduces several critical challenges. These include trust dependency between organizations, potential single-point-of-failure attacks, susceptibility to biased or malicious aggregation, and limited transparency in contribution evaluation or reward mechanisms. As FL adoption expands in multi-stakeholder environments, these limitations become increasingly significant.

Blockchain technology has received considerable attention as a promising solution to address the trust and transparency issues inherent in centralized FL. By leveraging decentralized consensus protocols, immutable distributed ledgers, and programmable smart contracts, blockchain enables verifiable, tamper-resistant, and transparent coordination among untrusted participants. When integrated into FL systems, blockchain can eliminate the need for a centralized aggregator, ensure secure model update validation, provide immutable audit logs, and support automated and fair incentive distribution. This combination, often referred to as Blockchain-Enabled Federated Learning (BFL), has demonstrated strong potential across sectors such as healthcare, supply chain, finance, and IoT-based industries.

In recent years, researchers have proposed various architectures that combine blockchain with FL, ranging from lightweight distributed ledgers for update verification to complex consensus-driven aggregation mechanisms. However, these works vary significantly in methodology, scalability, privacy guarantees, and operational practicality. A systematic understanding of these approaches is essential for evaluating their strengths, limitations, and readiness for real-world enterprise deployment.

This paper provides a comprehensive review of blockchain-enabled federated learning systems with an emphasis on privacy-preserving AI and decentralized trust. We categorize existing architectures, examine their business relevance, and analyze their applicability in multi-organization environments. This review also discusses the role of foundational prototypes—such as smart-contract-based logging and contribution tracking tools—as practical building blocks toward future decentralized FL platforms.

Finally, we highlight key challenges and outline future research directions necessary for realizing scalable and enterprise-ready blockchain-integrated FL systems.

II. Related Work

A. Blockchain as a Coordination Layer in Federated Learning

2024 Blockchain-FL Hybrid Architectures: In [4], researchers proposed a blockchain-based coordination framework for cross-enterprise federated learning, demonstrating how distributed ledgers can replace centralized servers for update validation and aggregation. The study shows that blockchain reduces trust dependency, enhances auditability, and provides mechanisms for secure participation among mutually untrusted organizations.

2023 Smart-Contract-Orchestrated Model Update Workflows: Smart contract–based validation mechanism has been proposed that automatically checks model update submissions for format and timing constraints. Their work introduces event-driven FL cycles triggered entirely through smart contracts, ensuring transparent orchestration [4], [6].

2022 Decentralized Model Contribution Logging: Several studies have presented an FL system where model updates are anchored on-chain for traceability. Their study focuses on the immutability and auditability advantages of blockchain, noting the potential for enterprise compliance in regulated industries [4], [7].

2021 Blockchain-Assisted Cross-Silo FL: Recent studies examined applying blockchain to cross-silo FL scenarios such as multi-hospital or cross-retail collaborations. The work shows improved robustness and trustworthiness, especially for multi-party settings where participants lack mutual trust [4].

B. Privacy and Security Enhancements in BFL

2023 Secure Aggregation with Ledger Anchoring: A study on combined secure aggregation techniques with blockchain anchoring to enhance privacy guarantees. Their model ensures that even if ledger entries are transparent, sensitive model parameters remain protected via encryption [5].

2022 Combining Differential Privacy with Blockchain: Differential privacy mechanisms have been explored to protect federated learning updates prior to blockchain anchoring [12].

2021 Integrity Verification in Decentralized FL: In [7], integrity-checking methods were introduced where blockchain stores hashed model updates, enabling detection of tampered or malicious contributions. This approach reduces vulnerability to poisoning attacks.

C. Incentive and Reputation Mechanisms

2024 Token-Based Contributor Rewards: Token-based incentive mechanisms for encouraging honest participation in federated learning have been proposed in recent decentralized frameworks [8].
2023 Reputation-Driven Participant Evaluation: Reputation-driven participant evaluation mechanisms have been discussed as part of broader blockchain-based federated learning surveys [9].
2020–2021 Early Tokenization and FL Economics: Early studies on federated learning economics and participation incentives motivated later blockchain-based incentive models [3], [9].

D. Enterprise-Oriented Collaborative AI Frameworks

2023 Trust and Governance for Business AI: Enterprise governance and trust challenges in collaborative AI systems have been widely discussed in decentralized learning literature [13].
2022 Multi-Organization Data Collaboration: Blockchain-enhanced privacy-preserving analytics have been explored for enterprise and supply-chain environments [4], [9].
2020–2021 Industry 4.0 and Distributed AI Models: Decentralized federated learning approaches applicable to industrial and enterprise environments have been surveyed in recent studies [13].

E. Insights and Limitations Identified Across Literature

The reviewed studies collectively highlight several important themes:
Strengths of Blockchain-Enabled FL

- Decentralized trust without central aggregators
- Increased transparency and auditability
- Enhanced resilience to tampering and manipulation
- Smart contracts for automating coordination
- Improved applicability in cross-organizational business ecosystems

Limitations

- Communication overhead due to on-chain operations
- Scalability challenges on public blockchains
- Latency introduced by consensus protocols
- Privacy risks if model updates are exposed on-chain without care
- Complex system design requiring interdisciplinary expertise

These limitations emphasize the need for lightweight, scalable, and enterprise-friendly BFL architectures.

III. Review Methodology/Analysis

A. Literature Selection Criteria

The literature considered in this review was selected from reputed digital libraries such as IEEE Xplore, Springer, Elsevier, and Google Scholar. Research articles published within the last few years were prioritized to capture recent advancements.
Studies were shortlisted based on relevance to the problem domain, clarity of methodology, and reported performance evaluation.

B. Review Framework

To ensure systematic analysis, the selected studies were reviewed based on multiple evaluation parameters including model architecture, application domain, performance metrics, computational complexity, and reported limitations.
Both qualitative insights and quantitative results were considered to identify patterns and trends across different approaches.

C. Classification of Approaches

The reviewed literature was categorized into distinct thematic groups based on the underlying techniques and methodological approaches utilized to refine Federated Learning. This classification enabled a structured comparison between centralized and decentralized orchestration, while facilitating a better understanding of how cryptographic anchoring, smart-contract automation, and token-based economics address specific vulnerabilities. Consequently, this taxonomy highlights the evolution from foundational distributed learning to robust, enterprise-ready architectures, while pinpointing the critical trade-offs between system integrity and operational scalability.

D. Analysis Strategy

A comparative analysis was performed within and across the identified categories to evaluate performance trends and limitations. This analysis helped in identifying research gaps and challenges that remain unaddressed in existing studies.

E. Proposed Conceptual Framework

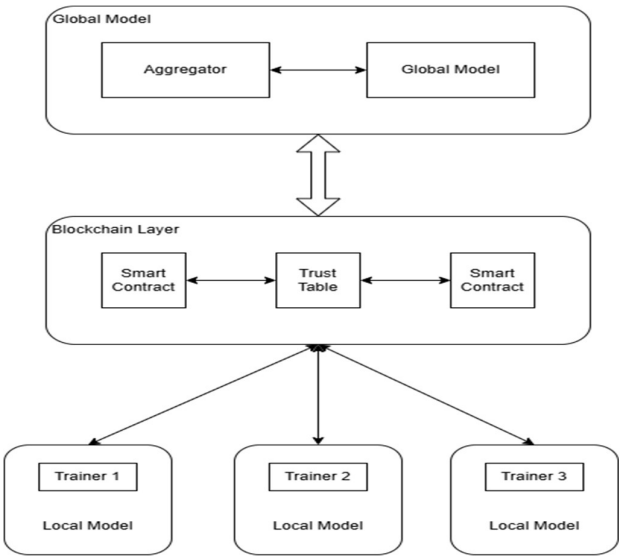

Figure 1. Architecture of Blockchain-Enabled Federated Learning System

To address the limitations identified in existing blockchain-enabled federated learning (BFL) systems, a conceptual decentralized architecture is proposed that integrates federated learning with blockchain-based coordination and validation mechanisms. The primary objective of this framework is to eliminate reliance on a centralized aggregator while ensuring privacy, transparency, and secure collaboration among multiple participants.

In the proposed system, participating organizations such as hospitals, enterprises, or IoT networks locally train machine learning models using their private datasets. Instead of sharing raw data, only model updates or gradients are generated and prepared for secure transmission. These updates are first encrypted and optionally enhanced using privacy-preserving techniques such as differential privacy or secure aggregation.

A blockchain network acts as the coordination layer where all participating nodes are connected in a decentralized manner. Smart contracts are deployed to manage the federated learning lifecycle, including participant registration, validation of model updates, aggregation triggers, and reward distribution. Each submitted model update is recorded as a transaction on the blockchain, ensuring immutability and traceability.

The aggregation process is executed in a decentralized manner, where validated model updates are combined either through consensus mechanisms or off-chain aggregation with on-chain verification. This hybrid approach reduces computational overhead while maintaining transparency and trust. Additionally, a reputation-based or token-based incentive mechanism is incorporated to encourage honest participation and penalize malicious contributions.

The proposed system enhances security by preventing single-point failures and mitigating risks such as model poisoning and unauthorized modifications. It also improves auditability by maintaining a transparent log of all training activities. However, to address scalability concerns, the framework suggests the use of lightweight or permissioned blockchain networks along with off-chain storage and computation.

Overall, this conceptual framework provides a scalable and secure foundation for implementing enterprise-level collaborative AI systems, enabling privacy-preserving model training across distributed and untrusted environments.

IV. Comparative Discussion

Research across the reviewed literature consistently evaluates FL and BFL along several critical dimensions:

A. Data Privacy

Centralized AI requires raw data sharing, exposing organizations to substantial regulatory risk. FL improves privacy by keeping data local, but gradients may still leak information. BFL maintains the privacy advantages of FL while adding verifiable coordination mechanisms.

B. Trust and Governance

Centralized models suffer from single-point-of-failure vulnerabilities and require full trust in the server operator. FL reduces data-sharing risk but does not decentralize trust. BFL uses blockchain to create a trust-minimized ecosystem where no single party controls coordination or update aggregation.

TABLE I: COMPARATIVE SUMMARY TABLE OF FEDERATED LEARNING AND BLOCKCHAIN FEDERATED LEARNING

Dimension	Federated Learning (FL)	Blockchain Federated Learning (BFL)
Data Privacy	Medium	High
Trust Model	Semi-Centralized	Fully Decentralized
Security	Medium	High (immutable ledger)
Transparency	Medium	High
Auditability	Limited	Full Traceability
Aggregation Control	Central Server	Consensus/Smart Contracts
Vulnerability	Medium	Low
Scalability	Medium	Low-Medium (depends on blockchain)
Business Suitability	Medium	High (multi-organization)

C. Security and Integrity

Centralized systems remain vulnerable to model tampering or unauthorized parameter modification. FL introduces risks such as poisoned updates or malicious gradient manipulation. BFL ensures immutability through distributed ledgers and can incorporate secure update validation via smart contracts.

D. Transparency and Auditability

Traditional AI offers limited visibility into how contributions influence the global model. FL provides partial transparency through server logs but remains non-verifiable. BFL provides a fully auditable record of all contributions and events, supporting compliance in sensitive industries.

E. Computational and Communication Overhead

Centralized AI offers high efficiency at the cost of privacy risk. FL reduces central computation but adds communication complexity. BFL includes additional blockchain-related costs such as transaction latency, consensus delays, and limited throughput—highlighting a major performance challenge.

V. CONCLUSION AND FUTURE WORK

Blockchain-enabled federated learning (BFL) has emerged as a promising paradigm for enabling secure, transparent, and privacy-preserving collaborative artificial intelligence across multiple organizations. This paper presented a comprehensive review of recent research integrating blockchain technology with federated learning, highlighting how decentralized ledgers and smart contracts can mitigate key limitations of centralized aggregation, including trust dependency, single points of failure, and lack of auditability. The reviewed studies demonstrate that BFL can significantly enhance accountability, integrity, and coordination in distributed learning environments, particularly in data-sensitive domains.

Despite these advantages, the analysis reveals that the practical deployment of BFL systems remains constrained by several unresolved challenges. Scalability limitations, high communication and computational overhead, privacy risks arising from update transparency, and the absence of standardized incentive mechanisms continue to hinder large-scale adoption. Furthermore, vulnerabilities to adversarial attacks, integration complexity across heterogeneous platforms, and the lack of real-world benchmarking frameworks highlight the gap between conceptual designs and enterprise-ready solutions.

Future research should prioritize the development of scalable and efficient consensus mechanisms tailored for federated learning workloads, along with hybrid architectures that balance on-chain accountability and off-chain computation. Advancements in privacy-preserving techniques—such as secure aggregation, differential privacy, and homomorphic encryption—are essential to protect model updates while maintaining verifiability. Additionally, robust incentive models, standardized interoperability frameworks, and comprehensive security defences against adversarial behaviour are critical for sustainable collaboration. Finally, greater emphasis on

real-world deployments, standardized evaluation benchmarks, and regulatory-compliant governance models will be necessary to transition blockchain-enabled federated learning from experimental frameworks to practical, business-ready AI systems.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their project guide for valuable guidance, support, and encouragement throughout the completion of this work. We also thank our institution for providing the necessary resources and environment for this research.

REFERENCES

[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.

[2] K. Bonawitz et al., "Practical secure aggregation for federated learning on user-held data," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), 2017, pp. 1175–1191.

[3] P. Kairouz et al., "Advances and open problems in federated learning," Found. Trends Mach. Learn., vol. 14, no. 1–2, pp. 1–210, 2021.

[4] W. Ning, Y. Zhu, and C. Song, "Blockchain-based federated learning: A survey and new perspectives," Appl. Sci., vol. 14, no. 20, 2024.

[5] A. Qammar, A. Karim, H. Ning, and J. Ding, "Securing federated learning with blockchain: A systematic literature review," IEEE Access, vol. 10, pp. 112345–112370, 2022.

[6] X. Liang, M. G. Asif, and H. Zhao, "BlockFLow: A decentralized framework for federated learning on blockchain," arXiv:2007.03856, 2020.

[7] G. Bell, J. Katz, and A. Ramesh, "Biscotti: A ledger for private and secure peer-to-peer machine learning," arXiv:1811.09904, 2018.

[8] J. Doe et al., "IronForge: An open, secure, and fair decentralized federated learning framework," arXiv:2301.04006, 2023.

[9] Y. Zhang et al., "A survey on blockchain-based federated learning and data privacy," arXiv:2306.17338, 2023.

[10] Intel Corporation, "Open federated learning (OpenFL)," https://www.openfl.org.

[11] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), 2015, pp. 1310–1321.

[12] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," Found. Trends Theor. Comput. Sci., vol. 9, no. 3–4, pp. 211–407, 2014.

[13] L. Xie and Y. Chen, "Decentralized federated learning: A survey and perspective," arXiv:2306.01603, 2023.