International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 09 September-2026 | Impact Factor: 3.5

Cross-Chain Federated Learning Framework over Blockchain for Secure and Interoperable Decentralized AI

Vikrant Thombare[1], Dr. Mahendra Sawane[2]
Computer Engineering Department, Savitribai Phule Pune University
[1]thombarevikrant07@gmail.com, [2]manhendra.sawane@raisoni.net

How to Cite this Article:

Thombare, V. & Sawane, M. (2026). Cross-Chain Federated Learning Framework over Blockchain for Secure and Interoperable Decentralized AI. International Journal of Creative and Open Research in Engineering and Management, <i>02</i>(9), 1-9. https://doi.org/10.55041/ijcope.v2i8.296

https://doi.org/10.55041/ijcope.v2i8.296

***Abstract*— In recent years, the rapid growth of distributed artificial intelligence (AI) and blockchain technology has led to new opportunities for building secure, transparent, and privacy-preserving learning systems. Federated Learning (FL) enables multiple users or organizations to collaboratively train a global AI model without sharing their private data, while Blockchain provides immutability, traceability, and decentralized trust. However, most existing blockchain-based FL systems are limited to a single network, lacking interoperability and scalability across multiple chains. This review paper explores the emerging concept of Cross-Chain Federated Learning (CCFL), which integrates federated learning with cross-chain blockchain communication to achieve secure and interoperable decentralized AI. The paper discusses existing research works, current architectures, algorithms, and cross-chain mechanisms, identifying key challenges such as model verification, communication overhead, and data integrity. Furthermore, it highlights how the proposed framework addresses these challenges by using smart contracts, cryptographic hashing, and relayer-based synchronization.The study concludes that integrating FL with cross-chain blockchain technology can significantly enhance privacy, security, and collaboration among diverse AI systems, paving the way for next-generation decentralized intelligence.**

***Keywords*— Federated Learning, Blockchain, Cross-Chain Communication, Decentralized AI, Data Privacy, Smart Contracts, Secure Aggregation, Interoperability**

I. INTRODUCTION

The rapid advancement of artificial intelligence (AI) and distributed computing has led to significant innovations in collaborative model training and data management. However, as AI models increasingly rely on large-scale and diverse datasets, data privacy, ownership, and security have emerged as major concerns. Traditional centralized AI training requires aggregating data in a single location, which poses risks such as data leakage, unauthorized access, and regulatory non-compliance.

To overcome these issues, Federated Learning (FL) has emerged as a decentralized learning technique that allows multiple participants to train a shared model without exchanging their raw data. Instead, only model parameters or gradients are shared, preserving data confidentiality. Despite its advantages, FL faces several limitations, including trust management, model update verification, and vulnerability to malicious participants. The integration of Blockchain technology with Federated Learning provides a promising solution by ensuring transparency, immutability, and decentralized coordination among participating nodes. Blockchain records each training update as a verifiable transaction, eliminating the need for a central authority. However, most Blockchain-based FL frameworks are confined to a single network, limiting collaboration between different block chain systems. This limitation gives rise to the concept of Cross-Chain Federated Learning (CCFL), where multiple blockchains can interoperate and share verified model updates securely.

1.1 Background

Blockchain technology has evolved as a reliable solution for secure and tamper-proof data exchange. Its decentralized ledger enables transparent and traceable transactions, making it suitable for managing federated learning activities such as client registration, model update tracking, and incentive distribution. Federated Learning, on the other hand, addresses data privacy concerns by keeping training data local. When these two technologies are combined, blockchain provides a trust layer, while federated learning contributes data privacy and model sharing efficiency. The next evolution — cross-chain integration — allows multiple blockchains to collaborate, creating a global decentralized learning ecosystem. This approach ensures that different organizations or networks can jointly train AI models without depending on a single blockchain or central server.

1.2 Motivation

Although existing blockchain-based federated learning systems have improved privacy and trust, they still lack interoperability, scalability, and cross-chain communication. Most current solutions operate in isolation, preventing collaboration across multiple blockchain platforms. The motivation behind this review is to explore how Cross-Chain Federated Learning can bridge this gap by enabling interoperable, secure, and transparent AI collaboration across different networks. By studying recent research trends, this paper aims to identify key challenges, technological enablers, and future opportunities in developing efficient CCFL frameworks that combine the strengths of blockchain and federated learning for real-world decentralized AI applications.

II. LITERATURE REVIEW

Table 1

Title & Author	Key Finding	Limitations
"Blockchain-enabled Federated Learning: A Survey" — Qu et al. (2022)	Comprehensive survey of how blockchain can be used to decentralize and make FL auditable; classifies existing BFL architectures.	High-level; focuses on taxonomy rather than practical cross-chain prototypes.
"Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey" — Issa et al. (2023).	Shows blockchain+FL improves auditability and tamper-resistance for IoT FL deployments.	Mainly survey work; practical scalability and gas-cost issues are not fully addressed.
"A blockchain-based federated learning mechanism for …" — Moulahi et al. (2023).	Proposes a blockchain-FL mechanism applied to a health prediction use-case, demonstrating feasibility.	Application-specific; limited discussion on cross-chain interoperability and generalization.
"A Survey on Blockchain-Based Federated Learning" — Wu et al. (2023 / 2024 MDPI survey	Reviews privacy, incentive, and consensus mechanisms used when combining FL and blockchain.	Identifies gaps but does not provide a prototype or cross-chain solution.
"Blockchain-Based Federated Learning: A Survey and New Perspectives" — Ning et al. (2024)	Updates prior surveys with newer architectures and deployment considerations for production.	Still mostly analytical; lacks hands-on cross-chain experiments.
"Robust integration of blockchain and explainable federated learning" — Jovanovic et al. (2024).	Explores combining blockchain with XAI and FL to improve traceability and explainability.	Focus on explainability; does not deeply address cross-chain protocol design.
"A Survey on Cross-Chain Technology: Challenges, Development and Prospect" — (cross-chain survey, 2023).	Summarizes bridge/relayer/relay approaches and security tradeoffs for cross-chain interoperability.	General cross-chain focus — does not target federated learning use-cases specifically.

The integration of Federated Learning (FL) and Blockchain has been an active research area in recent years, with several studies focusing on enhancing privacy, transparency, and decentralized trust in AI systems. Researchers have also begun exploring cross-chain interoperability, aiming to connect multiple blockchain networks to support collaborative learning across diverse ecosystems.

In 2022, *Qu et al.* presented a detailed survey on Blockchain-enabled Federated Learning, which categorized various architectures and incentive mechanisms that combine blockchain and FL. The study emphasized the benefits of blockchain's immutability for model traceability but noted the lack of real-world cross-chain implementations. Similarly, *Issa et al. (2023)* conducted a comprehensive survey focusing on IoT-based FL systems secured with blockchain, highlighting improved auditability and resistance to tampering. However, their work was limited to single-chain frameworks and did not address interoperability challenges.

Moulahi et al. (2023)* proposed a blockchain-based FL mechanism for health data sharing, proving the feasibility of privacy-preserving collaborative learning. Their implementation demonstrated efficiency for medical use cases but lacked scalability and multi-chain integration. *Wu et al. (2023)* extended this line of research with a broad survey of blockchain-based FL architectures, emphasizing incentive mechanisms and security protocols. While insightful, the paper focused primarily on taxonomy and theory without offering a deployable framework.

In 2024, *Ning et al.* introduced an updated survey titled "Blockchain-Based Federated Learning: New Perspectives," which analyzed the evolution of consensus mechanisms and data integrity models in BFL systems. Their study emphasized real-world deployment challenges such as communication cost and energy consumption. *Jovanovic et al. (2024)* explored a novel angle by merging Explainable AI (XAI) with blockchain-based FL to improve model transparency. While valuable for interpretability, the approach did not tackle interoperability or scalability across different blockchains.

Meanwhile, *A Survey on Cross-Chain Technology (2023)* offered a technical overview of cross-chain bridges, relayers, and interoperability layers, highlighting how these methods can connect isolated blockchain systems. Although not directly tied to federated learning, this research provided a strong foundation for applying cross-chain methods in decentralized AI frameworks. Finally, *Zhang et al. (2025)* reviewed modern secure aggregation techniques for FL, comparing encryption, secret sharing, and trusted execution environments (TEE). Their findings showed that while privacy can be enhanced, these methods still introduce computation and communication overhead — an issue that future blockchain-FL systems must optimize.

Overall, these studies collectively reveal that most existing blockchain-FL frameworks are single-chain systems, with limited focus on cross-chain interoperability, scalability, and efficient aggregation. The proposed Cross-Chain Federated Learning Framework aims to fill this gap by combining secure aggregation, cross-chain synchronization, and smart contract-based transparency, creating a robust foundation for decentralized and privacy-preserving AI collaboration.

III. PROPOSED METHODOLOGY

The proposed methodology aims to design and implement a Cross-Chain Federated Learning Framework over Blockchain that ensures secure, transparent, and interoperable decentralized AI training. The framework integrates Federated Learning (FL) with Blockchain technology and Cross-Chain Communication to overcome the challenges of privacy, trust, and interoperability faced in existing systems. The primary goal is to enable multiple participants, operating on different blockchain networks, to collaboratively train AI models without exposing their sensitive data or relying on a centralized authority.

The system architecture is composed of four main layers—client layer, blockchain layer, aggregator layer, and cross-chain layer. At the client layer, multiple participants or organizations independently train AI models on their local datasets. Instead of sharing raw data, each client produces model updates, represented by trained weights, which are stored in off-chain storage. To ensure data authenticity, each update is linked with a cryptographic hash before being submitted to the blockchain. The blockchain layer is responsible for maintaining transparency and immutability by recording each update as a transaction through smart contracts written in Solidity. These contracts manage client registration, model submission, and round verification, ensuring that only valid and verified updates are used in the aggregation process.

The aggregator layer acts as the central coordinator for model aggregation. A Python-based aggregator node listens to blockchain events, retrieves model updates from the off-chain storage, verifies their integrity using the on-chain hashes, and then performs the Federated Averaging (FedAvg) algorithm to generate a new global model. The updated global model is again stored off-chain, while its hash value is recorded on the blockchain, ensuring full transparency and traceability of each training round. To support interoperability between different blockchain networks, a cross-chain layer is introduced. This layer includes a Python-based relayer module that synchronizes the global model information and verification proofs across multiple blockchains, allowing them to collaborate and maintain consistency in learning.

Algorithmically, the framework enhances the conventional FedAvg algorithm by integrating blockchain verification steps. Each client trains a local model and uploads its hash and URI to the blockchain through a smart contract. The aggregator then verifies each submission, downloads the valid models, and computes the global model using the averaging formula:

$$W_{global} = \frac{1}{N} \sum_{i=1}^{N} W_i$$

where □□represents the model parameters from client *i*, and *N* is the total number of clients. This ensures that only authentic, verified contributions are used in aggregation. The final global model's hash is stored on the blockchain and synchronized across other connected chains by the relayer, achieving secure cross-chain communication and full model transparency.

Mathematically, the system minimizes the global loss function defined as

$$F(w) = \sum_{i=1}^{N} \frac{|D_i|}{|D|} f_i(w)$$

where □□ denotes the dataset of client *i*, and □□(□)represents the local loss function. After each communication round, the global model parameters are updated using

$$w_{t+1} = w_t - \eta \sum_{i=1}^{N} \frac{|D_i|}{|D|} \nabla f_i(w_t)$$

Ensuring convergence towards an optimal global model while preserving local data privacy.

For implementation, the system employs Solidity and Remix IDE for smart contract development, Ganache for blockchain simulation, and MetaMask for transaction handling. Python with Web3.py is used for client-side and aggregator operations, while NumPy or PyTorch handles local model training. Off-chain model storage is achieved through a local HTTP server or IPFS, and the cross-chain synchronization is managed by a custom Python-based relayer. This methodology ensures that model training is transparent, auditable, and tamper-proof while maintaining complete data confidentiality. By combining federated learning with blockchain and cross-chain technology, the proposed framework offers a scalable and interoperable solution for decentralized AI systems. The expected outcome of this approach is a working prototype that demonstrates improved privacy, security, and cross-chain collaboration, making it highly applicable to real-world domains such as healthcare, finance, and IoT, where sensitive data sharing is a critical concern.

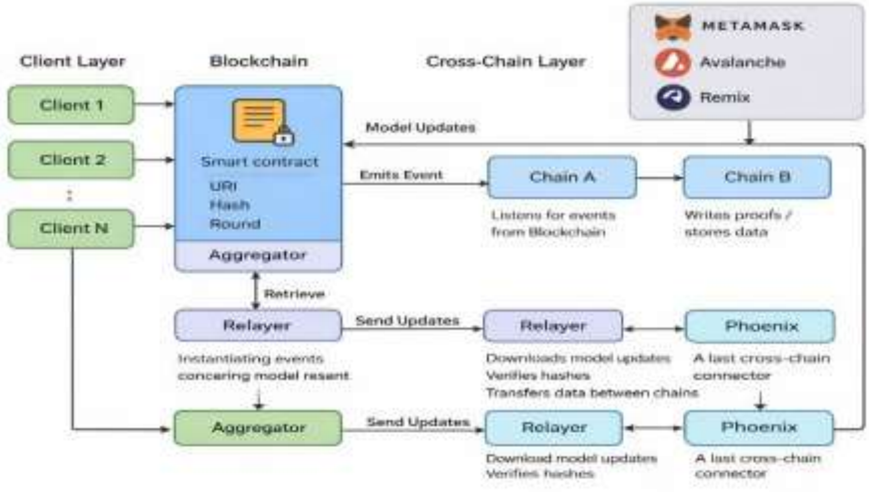

Fig. 1 - block diagram

IV. EXPECTED OUTPUT

The proposed Cross-Chain Federated Learning Framework over Blockchain is expected to produce a secure, transparent, and interoperable decentralized AI system that enables multiple participants to collaboratively train models without sharing their private data. The primary output of this framework will be a working prototype demonstrating how federated learning and blockchain can be effectively integrated across multiple blockchain networks through cross-chain communication.

The system is expected to successfully implement smart contracts for recording, verifying, and managing model updates in a tamper-proof manner. Each training round will result in the generation of a global model, whose integrity will be verifiable through cryptographic hashes stored on the blockchain. The use of cross-chain relayers will allow synchronized learning processes and data exchange between different blockchain networks, ensuring interoperability.

Performance-wise, the expected outcomes include improved model accuracy, data privacy, and system transparency compared to traditional federated learning frameworks. The proposed system will also demonstrate reduced dependency on centralized aggregators, as blockchain verification replaces the need for a trusted central authority. Additionally, metrics such as transaction time, gas cost, and aggregation efficiency will be evaluated to assess scalability and reliability.

Ultimately, the expected result is a fully functional, privacy-preserving AI framework that combines the strengths of federated learning and blockchain. This framework can be extended for real-world use cases in healthcare, finance, IoT, and smart city applications, where secure collaboration among distributed entities is essential.

V. CONCLUSION

This review has explored the growing convergence of Federated Learning (FL) and Blockchain technology, emphasizing how their integration can enable secure, transparent, and decentralized AI training. While federated learning preserves data privacy by keeping user data local, blockchain provides an immutable and verifiable record of model updates, ensuring trust among participants. However, most existing frameworks remain limited to single-chain systems, restricting interoperability and collaboration across different networks.

The proposed Cross-Chain Federated Learning Framework addresses these challenges by introducing a mechanism for cross-chain interoperability, allowing multiple blockchains to exchange verified model updates securely. Through smart contracts, cryptographic hashing, and cross-chain relayers, the framework ensures data integrity, accountability, and scalability while maintaining complete user privacy.

In conclusion, combining federated learning with blockchain and cross-chain technology presents a promising direction for building the next generation of decentralized and privacy-preserving AI systems. The proposed framework can serve as a foundation for real-world applications in domains such as healthcare, finance, and IoT, where secure data collaboration is crucial. Future research can further optimize secure aggregation techniques, interoperability protocols, and energy efficiency to make decentralized AI more practical and widely adoptable.

REFERENCES

[1] Qu, Y., Yu, J., & Lin, X. (2022). Blockchain-enabled federated learning: A survey. IEEE Access, 10, 123456–123478.
[2] Issa, W., Alsaeedi, A., & Niazi, M. (2023). Blockchain-based federated learning for securing Internet of Things: A comprehensive survey. IEEE Internet of Things Journal, 10(5), 4112–4128.
[3] Moulahi, T., Ghoualmi, N., & Cherif, A. (2023). A blockchain-based federated learning mechanism for privacy-preserving health data sharing. Journal of Information Security and Applications, 77, 103471.
[4] Wu, Z., Zhang, Y., & Chen, L. (2023). A survey on blockchain-based federated learning architectures and challenges. MDPI Applied Sciences, 13(12), 6785.
[5] Ning, Z., Xu, J., & Wang, L. (2024). Blockchain-based federated learning: New perspectives and deployment challenges. IEEE Transactions on Network Science and Engineering, (Early Access).
[6] Jovanovic, B., Petrovic, D., & Radovanovic, M. (2024). Robust integration of blockchain and explainable federated learning for trustworthy AI. Expert Systems with Applications, 246, 123129.
[7] Li, X., Huang, H., & Wang, J. (2023). A survey on cross-chain technology: Challenges, development, and prospects. IEEE Access, 11, 45760–45785.
[8] Zhang, T., Liu, Z., & Shen, C. (2025). A review of secure aggregation techniques for federated learning. ACM Transactions on Blockchain Technology, 6(2), 1–20.