International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 1, Jan-Feb 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Blockchain-Enhanced Trust for Federated LLM Training

Abhishek Jyotiba*, Swati Uparkar**
*(AIDS, Shah and Anchor Kutchhi Engineering College
Email: jyotibaabhishek@gmail.com)
** (GUIDE, Shah and Anchor Kutchhi Engineering College
Email: swati.uparkar@sakec.ac.in)

----------**********----------

Abstract:
Federated Learning (FL) and blockchain technology have become key advancements in the fields of decentralized computing and artificial intelligence. The lack of trust amongst participants, especially when it comes to guaranteeing the integrity of model updates, is a significant obstacle in federated learning. In order to guarantee trust, accountability, and transparency in Federated Learning systems for training Large Language Models (LLMs), this article investigates a blockchain-enhanced framework. In distributed environments, the framework tackles issues like malicious updates, data poisoning, and loss of provenance by incorporating blockchain methods like smart contracts and immutable ledgers. This study examines the framework's design, workflow, and possible uses in addition to its effects on security, scalability, and privacy.

Keywords: **Blockchain, Federated Learning, Large Language Models, Trust, Decentralization, Smart Contracts, Data Provenance.**

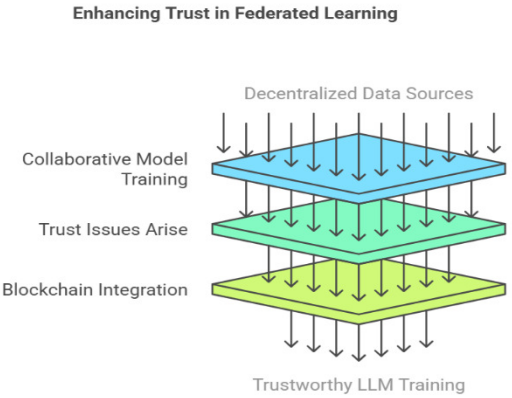
----------**********----------

I. INTRODUCTION

Without transferring raw data, Federated Learning (FL) allows cooperative training of machine learning models across dispersed data sources. Applications that are sensitive to privacy, such edge computing, healthcare, and finance, have found great success with this decentralized strategy. At the same time, natural language processing has been transformed by Large Language Models (LLMs), which have shown remarkable performance in tasks including question answering, summarization, and translation.

But in federated learning settings, participant trust continues to be a significant barrier. There are serious hazards associated with problems like malicious updates, data poisoning, and the inability to identify the source of model contributions. An immutable, transparent, and secure ledger for documenting model updates, participant contributions, and anomaly detection is provided by blockchain technology, which presents a promising solution.

This paper proposes a blockchain-enhanced framework to foster trust and accountability in Federated Learning systems for LLM training.



II. Background and Related Work

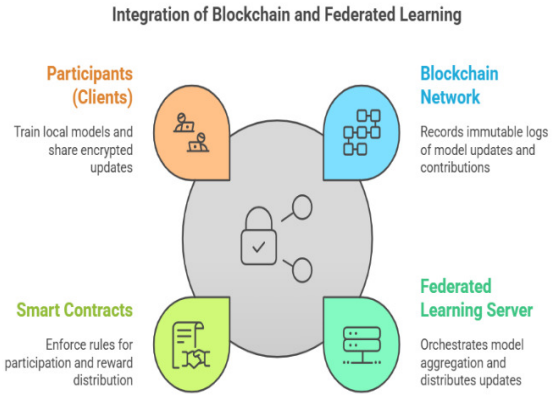
Federated Learning and LLMs: Federated Learning allows several clients to work together without sharing their raw data, which makes it easier to train models in a decentralized

manner. While privacy is maintained, issues including data heterogeneity, untrustworthy participants, and security flaws are introduced. Because of their size and complexity, LLMs demand a lot of processing power, which makes decentralized training even more difficult.

Blockchain Technology for Trust:

A decentralized ledger technology called blockchain guarantees tamper-proof, transparent, and unchangeable records. Blockchain's potential to promote trust and accountability has been demonstrated by applications in healthcare, supply chain management, and finance. But little is known about how it integrates with FL, especially when it comes to LLM instruction.

III. PROPOSED FRAMEWORK



Architecture Important elements:

Blockchain Network: Keeps unchangeable records of participant contributions, model upgrades, and anomalies found.

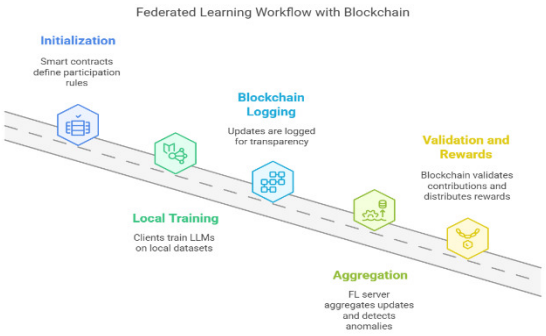
Federated Learning Server: Distributes updates and coordinates model aggregation.

Smart Contracts: Distribute rewards, validate model updates, and enforce participation restrictions.

Participants (Clients): Exchange encrypted updates and train local models.

Workflow:

Initialization: Smart contracts specify guidelines for involvement, such as systems for validating contributions and ensuring data quality.
Local Training: Clients create encrypted updates and train LLMs on local datasets.
Blockchain Logging: For transparency and traceability, updates are recorded on the blockchain.
Aggregation: To weed out malicious contributions, the FL server aggregates updates and uses anomaly detection.
prizes and Validation: Smart contracts are used to award prizes, and blockchain verifies donations.



Key Features:

Blockchain enhances data provenance by ensuring model update traceability, meaning every modification to the model is securely recorded and verifiable. This helps maintain transparency and accountability in collaborative machine learning. Additionally, anomaly detection is strengthened through smart contracts, which automatically identify and block any malicious updates, preventing unauthorized changes to the model. To encourage honest participation, incentive mechanisms are integrated, where contributors are rewarded for their genuine involvement, fostering a trustworthy environment. Lastly, scalability is achieved by leveraging lightweight blockchain technologies, which minimize computational overhead, allowing efficient model updates without excessive resource consumption.

IV. Methodology

Technical Approach:

Blockchain Protocol Selection: To reduce latency and computational expenses, use energy-efficient, lightweight protocols like Directed Acyclic Graphs (DAGs) or Proof of Stake (PoS).

Privacy and Encryption: Secure aggregation and homomorphic encryption guarantee participant privacy.

Anomaly Detection: Algorithms based on machine learning detect and stop malicious updates or data poisoning.

Smart Contracts: Establish guidelines for resolving disputes, allocating rewards, and validating contributions.

Metrics for Evaluation

Trust Score: Evaluates how reliable model updates are.

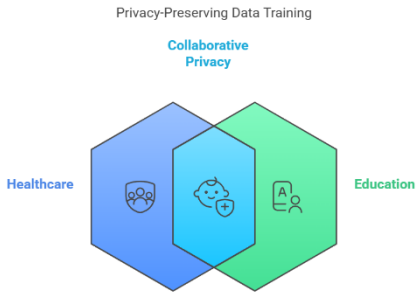
Latency: The amount of time needed to aggregate model updates.

Scalability: The number of participants that can be accommodated without performance deterioration.

Model Performance: The trained LLM's recall, accuracy, and precision.

Application:

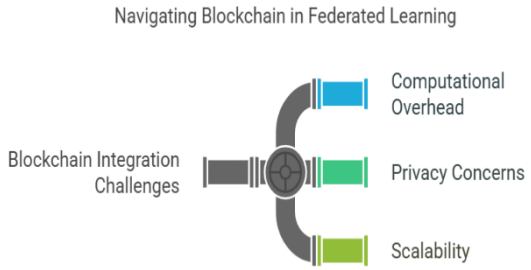
Healthcare: Provide LLMs with safe, private training on decentralized electronic health records to enhance individualized medicine & diagnostics.
Education: Provide LLMs with cooperative training on student performance data while maintaining confidentiality and guaranteeing responsibility.
Finance: Train LLMs on dispersed financial datasets to improve credit scoring and fraud detection.



Challenges and Limitations

Computational Overhead: Latency and resource constraints are introduced by blockchain integration.

Privacy Issues: It might be difficult to protect participant anonymity while preserving openness.
Scalability: It takes optimization to manage massive federated learning systems with blockchain connectivity.



V. CONCLUSION

In order to overcome trust issues in Federated Learning systems for training Large Language Models, this study proposes a blockchain-enhanced approach. The suggested method makes use of blockchain's transparency and immutability to guarantee safe, responsible, and effective group training. The approach opens the door for scalable and privacy-preserving AI systems while also enhancing trust and accountability. It draws attention to how blockchain might reduce threats like malicious updates and data poisoning while promoting a decentralized, cooperative environment for LLM development.

Future research will concentrate on investigating multidisciplinary applications in industries

including healthcare, banking, and education, minimizing computational cost with sophisticated aggregation approaches, and optimizing scalability through lightweight blockchain protocols. Important study topics will also include creating strong privacy-preserving safeguards and improving the participant incentive program.

AI governance has new opportunities thanks to the combination of blockchain and federated learning, which makes it a potential area for future development.

VI. References

1. Kairouz, P., et al. (2019). Advances and Open Problems in Federated Learning.
2. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
3. Bonawitz, K., et al. (2017). Practical Secure Aggregation for Federated Learning on User-Held Data.
4. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger.
5. Yang, Q., et al. (2019). Federated Machine Learning: Concept and Applications.
6. Xu, R., et al. (2022). Blockchain-Based Trust Framework for Federated Learning.
7. Brown, T., et al. (2020). Language Models Are Few-Shot Learners.

