ACCSCIENCE PUBLISHING

Artificial Intelligence in Health

PERSPECTIVE ARTICLE

The role of Omnichain in advancing federated learning for artificial intelligence training in healthcare

Dongfang Wu[1,2]*, and Yichen Wang[1,2]

[1]Global Health Research Center, Duke Kunshan University, Kunshan, Jiangsu, China

[2]Global Health Institute, Duke University, Durham, North Carolina, United States of America

Abstract

Health data serves as a crucial foundation for artificial intelligence (AI) training in the healthcare sector. The pivotal procedure for acquiring numerous and effective health data lies in incentivizing participants to contribute their health data while adhering to privacy regulations like the General Data Protection Regulation. Federated learning achieves privacy protection by transmitting only parameters rather than data to the model. When integrated with blockchain smart contracts, this approach facilitates the automation of incentives according to health data quality, thereby mitigating human's subjective intervention. Consequently, the synergy of these two methodologies offers new promise for the training of AI models in healthcare. However, this advantage encounters performance degradation due to the heterogeneity among diverse blockchains. This article posits the concept of Omnichain as a potential solution to this challenge by analyzing its operational mechanisms and future developmental trajectories and providing potential perspectives for its combination with hybrid federal learning solutions such as differential privacy and secure multi-party computation to promote its application in the sphere of AI in healthcare.

Keywords: Omnichain; Federated learning; Artificial intelligence training; Healthcare; Training performance

***Corresponding author:**
Dongfang Wu
(dongfang.wu@duke.edu)

Citation: Wu D, Wang Y. The role of Omnichain in advancing federated learning for artificial intelligence training in healthcare. *Artif Intell Health*. 2025;2(3):39-43. doi: 10.36922/aih.5753

Received: November 4, 2024

1st revised: December 23, 2024

2nd revised: January 24, 2025

Accepted: February 25, 2025

Published online: March 7, 2025

1. Introduction

Health data is a vital asset in healthcare and thoroughly exploiting it for artificial intelligence (AI) training yields substantial value in diagnosis, medication, and patient care. Nonetheless, two concurrent challenges deserve consideration: (i) how to ensure adherence of health data collection to privacy regulatory frameworks such as General Data Protection Regulation;[1] and (ii) how to incentivize individuals or institutions to share their health data, with the aim to ensure continuity and reliability of AI training quality.[2]

Federated learning, an emergent paradigm in machine learning for AI, allows algorithms to be trained across multiple distributed devices or servers with local data samples. In contrast to traditional machine learning, participants in federated learning

do not exchange local data. Rather, they transmit the parameters of their local training results to a central server, thereby achieving a collaborative AI model training objective.[3]

However, the concern within federated learning is incentivizing entities to contribute valid health data while penalizing malicious actors. The latency and subjectivity inherent in manual evaluations do not provide an optimal solution. The immutable and self-executing nature of smart contracts within blockchain addresses this issue by enabling all participants to ascertain results instantly without the need for intermediaries, thus facilitating a reliable reward distribution mechanism for federated learning to create an automated and standardized process.[4]

Consequently, these two advantages position federated learning and blockchain as inherently complementary. Each participant is assigned a blockchain identity, known as the public address, wherein health data is stored, manifesting in a distributed manner. Participants declare their public address to engage in the federated learning process and, thereby, receive rewards according to smart contract criteria. Thus, in the healthcare sector, where pertinent ethical and sensitive considerations regarding health data are paramount, implementing real-time federated learning for health information privacy protection and utilizing blockchain to develop more intelligent incentive strategies holds significant promise.

2. Omnichain paradigm in federated learning

This innovative amalgamation of federated learning and blockchain effectively addresses the privacy concerns surrounding health data during the training process while significantly enhancing the motivation of participants to contribute health data. However, AI practitioners have encountered challenges with this integration due to the heterogeneity among different blockchains. For instance, when a federated learning framework that was originally developed in Solidity language and deployed on Ethereum mainnet seeks to migrate to Solana, it may be reimplemented in Rust language. Meanwhile, implementing federated learning on diverse blockchains necessitates reconfiguring environments to accommodate various consensus mechanisms. The aforementioned factors result in performance degradation for federated learning.[5] This situation underscores the need for a unified blockchain environment that ensures a consistent execution standard for conducting federated learning on health data across different blockchains.

The emergence of the concept of the Omnichain addresses this critical issue. Omnichain constructs a novel foundational layer, known as Layer-0, that interconnects all blockchains, regardless of their smart contract technologies, thereby allowing all federated learning processes to operate atop this infrastructure.[6] This represents a highly compatible super multi-chain ecosystem that mitigates the limitations of individual blockchains, ultimately serving the needs of AI training. During the construction of the Omnichain, Cosmos SDK is a pivotal technology whose standardized development toolkit enables seamless communication and transactions among unique parallel blockchains. With this interoperability, the Cosmos SDK opens up a world of possibilities, allowing data, tokens, assets, and logic to be transmitted across multiple blockchains in a highly secure and trustworthy manner.[7]

As illustrated in Figure 1, Omnichain supported by the Cosmos SDK facilitates communication among disparate blockchains. Omnichain connects various blockchains and allows users to deploy smart contracts directly onto it by unified smart contracts tailored for diverse blockchains on the Omnichain. Furthermore, the federated learning process is capable of directly interfacing with the Omnichain and executes these contracts to establish incentive mechanisms. Simultaneously, smart contracts can be distributed across multiple blockchains without needing to consider the barriers arising from differing consensus mechanisms or programming languages, eventually mitigating performance degradation arising from blockchain heterogeneity while ensuring the integrity of privacy and incentive mechanisms, which ultimately aids in the training of AI models.

Notably, this process does not impede the independent generation of blocks by individual blockchains, indicating that the construction of Layer-0 does not necessitate the implementation of Layer-1 through a forking mechanism. This advancement effectively dismantles barriers between different blockchains, resulting in a qualitative leap in both the fluidity and functionality of information exchange. For example, once a federated learning model completes a round of training updates on Ethereum, the trained model can be transmitted to Solana through Omnichain to continue training. This approach eliminates the need for reliance on a single-point oracle or centralized bridge and likewise reduces the opportunities for attackers to exploit cross-chain bridge vulnerabilities.

Moving a further step, Omnichain can also be integrated into existing hybrid solutions. Differential privacy (DP) is a strategy aimed at mitigating the risks of side-channel attacks or differential analyses of parameter updates in federated learning. Injecting mathematically quantifiable noise into the parameter reporting and aggregation processes eventually increases the difficulty

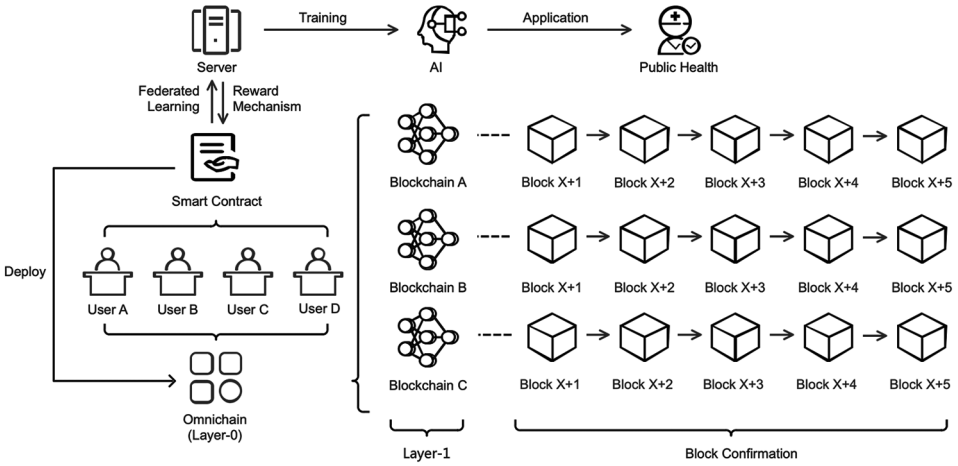

Figure 1. Omnichain applied in federated learning
Source: Image created by authors.

of inferring individual data points.[8] However, when data sources are scattered across different public chains, Layer-2 sidechains, or specific consortium blockchains, ensuring privacy in distributed cross-chain training requires a DP mechanism capable of seamlessly adapting to multi-chain data transmission and sharing. The interoperability of the Omnichain protocol relieves a federated learning platform from being confined to a single-chain dataset or a single network. Within a unified ledger, developers can incorporate DP parameter-tuning strategies into cross-chain data exchange interfaces. Then, the DP-processed parameters can be securely transmitted to a central aggregation point, which may be a federated learning service contract on a main chain or at a Rollup layer.

When federated learning faces even stricter privacy and compliance requirements, especially in healthcare, DP alone may still fail to meet regulatory standards. In such cases, the introduction of Secure Multi-Party Computation (SMC) offers stronger security guarantees for federated training.[9] Through SMC, participants can operate on encrypted local parameters or intermediate computation results without exposing data in plain text, ensuring that no single entity can reconstruct the original data of another party. To implement SMC protocols within an Omnichain framework, the corresponding execution logic must be extended. The Omnichain protocol, leveraging decentralized cross-chain verification and light client proofs, eliminates the need for trusted intermediaries in inter-chain information exchange. Building on this foundation, SMC protocols can be realized by deploying mutually trustworthy computation contracts on various chains and employing full-chain consensus to verify the integrity of relayed data, thus enabling trustless transmission and secure computation of encrypted parameters. With Omnichain, SMC solutions can achieve parallel, sharded secure computation across multiple chains. For example, a high Transactions Per Second execution chain could handle distributed key generation and secret sharing; another privacy-focused chain might perform encrypted gradient aggregation and decryption threshold checks; and the main chain or a Rollup layer could conduct final model verification and record-keeping. Because Omnichain interoperability allows each computation step to be executed on the chain best suited to the task, the combination of federated learning, SMC, and Omnichain can demonstrate new potential in terms of performance and scalability.

3. Discussion

The integration of Omnichain with federated learning addresses the performance degradation issues arising from blockchain heterogeneity in training AI models within the public health sector. The potential use case lies in overcoming the phenomenon of chain isolation imposed by federated learning frameworks confined to a single blockchain. Consider a healthcare federated learning project training privacy-processed patient medical record metadata on Ethereum's Layer-2 solution Polygon. At the same time, the project seeks to incorporate Internet of Things device training data collected through a Solana blockchain, which offers robust Decentralized Physical Infrastructure Network compatibility, and it also wishes to utilize hashed research and evidentiary records from a specific industry consortium chain that stores pharmaceutical R&D data. Under a traditional single-chain paradigm, these three requirements would remain isolated, forming data silos. By leveraging full-chain interoperability protocols, however, the

federated learning model can seamlessly access and aggregate these diverse data sources – while respecting privacy and permission constraints – thus enhancing the model's generalization capabilities and training quality. In parallel, the concept of a taxonomy driven by practical services can be applied here. By approaching the discussion from the perspective of concrete services, we can deduce the unique advantages that Omnichain offers, thereby realizing synergy between a fully integrated blockchain framework and federated learning across diverse domains, such as health data circulation and management, privacy and security, token-based incentive mechanisms, collaborative orchestration, and regulatory oversight. This approach ultimately advances the real-world adoption of the hybrid solution. For example, in the realm of health data circulation and management, indexing services built on Omnichain can standardize data drawn from multiple blockchains, thereby streamlining cross-chain data flow and providing high-quality datasets for federated learning.

However, Omnichain remains undeveloped. Before its development, cross-chain bridges represented a bold yet flawed endeavor. Users were required to lock assets on the source chain and incur gas fees to receive corresponding wrapped assets on the target chain, thereby creating liquidity challenges.[10] In addition, cross-chain bridges predominantly focused on value transfer rather than imperative information transfer, which is essential for training AI. In contrast, Omnichain emerges as a novel paradigm extending from cross-chain bridges, utilizing universal smart contracts to create an infrastructure that spans multiple chains and can be directly deployed across various blockchains, including Ethereum Virtual Machine – compatible and other mainstream platforms, thereby mitigating the silo effect of disparate blockchains. Nevertheless, the high-throughput requirements of federated learning in the training process remain in tension with the existing gas pricing mechanisms of Omnichain, and the block generation speed of Omnichain further constrains the deployment of federated learning solutions.[11] This necessitates that Omnichain, much like various Layer-2 solutions of Ethereum, progresses toward achieving low-cost and rapid transaction capabilities.

4. Conclusion

This article proposes the integration of Omnichain concept into the existing frameworks of federated learning and blockchain, with the objective of minimizing performance degradation while maintaining privacy protection during AI training in the healthcare sector. By deploying smart contracts tailored for diverse blockchains on the Omnichain, the federated learning framework may decrease redundant deployments, thus enabling support for multiple blockchains directly from the Omnichain. This design enhances the efficiency of the AI training paradigm that combines federated learning with blockchain in healthcare. However, it is important to note that the Omnichain is still in its nascent developmental stage, and its speed and cost remain significant constraints on its integration with federated learning. This presents a crucial area for future research and attention.

Acknowledgments

We are deeply grateful to the Duke University Writing Studio for tremendous assistance in polishing the academic language of our work.

Funding

None.

Conflict of interest

The authors declare that they have no competing interests.

Author contributions

Conceptualization: Dongfang Wu
Writing–original draft: Dongfang Wu
Writing–review & editing: Yichen Wang

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Availability of data

Not applicable.

References

1. Truong N, Sun K, Wang S, Guitton F, Guo Y. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Comput Secur*. 2021;110:102402.

   doi: 10.1016/j.cose.2021.102402

2. Zhan Y, Li P, Qu Z, Zeng D, Guo S. A learning-based incentive mechanism for federated learning. *IEEE Internet Things J*. 2020;7:6360-6368.

   doi: 10.1109/JIOT.2020.2967772

3. Mammen PM. Federated learning: Opportunities and challenges. arXiv [Preprint]. 2021.

   doi: 10.48550/arXiv.2101.05428

4. Nguyen DC, Ding M, Pham QV, *et al*. Federated learning

meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet Things J*. 2021;8(16):12806-12825.

doi: 10.1109/JIOT.2021.3072611

5. Zhu J, Cao J, Saxena D, Jiang S, Ferradi H. Blockchain-empowered federated learning: Challenges, solutions, and future directions. *ACM Comput Surv*. 2023;55(11):1-31.

doi: 10.1145/3570953

6. Zheng J, Lee DKC, Qian D. An in-depth guide to cross-chain protocols under a multi-chain world. *World Sci Annu Rev Fintech*. 2023;1:2350003.

doi: 10.1142/S2811004823500033

7. Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput Surv*. 2021;54(8):1-41.

doi: 10.1145/3471140

8. El Ouadrhiri A, Abdelhadi A. Differential privacy for deep and federated learning: A survey. *IEEE Access*. 2022;10:22359-22380.

doi: 10.1109/ACCESS.2022.3151670

9. Acar A, Celik ZB, Aksu H, Uluagac AS, McDaniel P. Achieving Secure and Differentially Private Computations in Multiparty Settings. In: *2017 IEEE Symposium on Privacy-Aware Computing* (*PAC*). Washington, DC, USA: IEEE; 2017. p. 49-59.

doi: 10.1109/PAC.2017.12

10. Harris CG. Cross-chain Technologies: Challenges and Opportunties for Blockchain Interoperability. In: *2023 IEEE International Conference on Omni-layer Intelligent Systems* (*COINS*). Berlin, Germany: IEEE; 2023. p. 1-6.

doi: 10.1109/COINS57856.2023.10189298

11. Zarick R, Pellegrino B, Banister C. Layerzero: Trustless omnichain interoperability protocol. arXiv [Preprint]. 2021.

doi: 10.48550/arXiv.2110.13871