Two-Layered Blockchain Architecture for Federated Learning over the Mobile Edge Network

Lei Feng, Zhixiang Yang, Shaoyong Guo, Xuesong Qiu, Wenjing Li, and Peng Yu

Abstract

Federated learning (FL) is seen as a road toward privacy-preserving distributed artificial intelligence while keeping raw training data on local devices. By leveraging blockchain, this article puts forward a blockchain and FL fusioned framework to manage the security and trust issues when applying FL over mobile edge networks. First, a two-layered architecture is proposed that consists of two types of blockchains: local model update chain (LMUC) assisted by device-to-device (D2D) communication and global model update chain (GMUC) supporting task sharding. The D2D-assisted LMUC is designed to chronologically and efficiently record all of the local model training results, which can help to form long-term reputations of local devices. The GMUC is proposed to provide both security and efficiency by preventing mobile edge computing nodes from malfunctioning and dividing them into logically isolated FL task-specific chains. Then a reputation-learning-based incentive mechanism is introduced to make participating local devices more trustful with a reward implemented by a smart contract. Finally, a case study is given to show that the proposed framework performs well in terms of FL learning accuracy and blockchain time delay.

Background and Motivation

Background of FL in Mobile Edge Networks

The rapid development of the cellular Internet of Things (IoT) has resulted in an explosion in the number of edge devices. Some advanced data acquisition techniques like crowdsensing make edge devices the basic data sensing and collection units. However, the large amounts of data transferred between these IoT edge devices and cloud computing data centers result in undesired transmission time delay and network resource occupation. To resolve this problem, computing and communication are being seamlessly merged at the edge of the mobile network. Device-to-device (D2D) communication enables the direct exchange of information between edge IoT terminals, while mobile edge computing (MEC) syncs powerful computing resources to the base station (BS) or edge data center. The fusion of communication and computation over the mobile edge network heralds a huge boost to the collaborative work among IoT devices [1].

A representative example of collaborative work is computing the migration between IoT terminals and MEC servers, which can shorten the service latency due to the advantage of ubiquitous wireless access and edge computing resources over the mobile network. However, the environment of the mobile network is usually dynamic, which results from the time-varying channel, mobility, bandwidth availability, and so on. Artificial intelligence (AI) can mitigate these negative impacts. Machine learning (ML) can automatically extract the mapping relationship between the optimal migration decision and high-dimensional input. ML can also predict the future short-term trend of the environment to reserve enough resources for edge computing, such as terminal mobility and traffic load predication. It is known that the general key to successful ML is based on rich historical data. However, conventional ML schemes aggregate all of a user's data for centralized training, which raises concerns about the privacy and misuse of personal data. To address these concerns, federated learning (FL) is seen as a road toward privacy-preserving distributed ML. In FL, the privacy of users who participate in collaborative work remains intact, as none of the raw data is transferred out of their local devices. The workflow of FL can be simply summarized as follows:

- Participant devices obtain their local model updates according to on-device data samples.They are then uploaded to a central server.
- The central server computes the global model via these aggregated local model updates.
- The local devices download the updated global model and revise the local models.
- The learning cycle repeats until the required accuracy is reached [2].

Motivation for the Fusion of FL and Blockchain

There are some issues to work through when applying FL over mobile edge networks.

Security: In FL, a centralized computing node like the MEC server, which owns all of the user's data, may mislead the global model due to intentional or unintentional behavior [3]. Any malicious activities resulting in a deficient global model is harmful to the next local model updates. All of the FL work becomes erroneous.

Trust: Not all local nodes that participate in FL have a good reputation. Untrustworthy local nodes may cheat and temporarily update low-quality models due to high-speed mobility or energy constraints, adversely affecting FL.

Efficiency: If there are massive amounts of local devices that are accessing across separate geographic regions, the global computing work may be moved to a cloud data center rather than

The authors are with Beijing University of Posts and Telecommunications; Shaoyong Guo is the corresponding author.

Digital Object Identifier:
10.1109/MNET.011.2000339

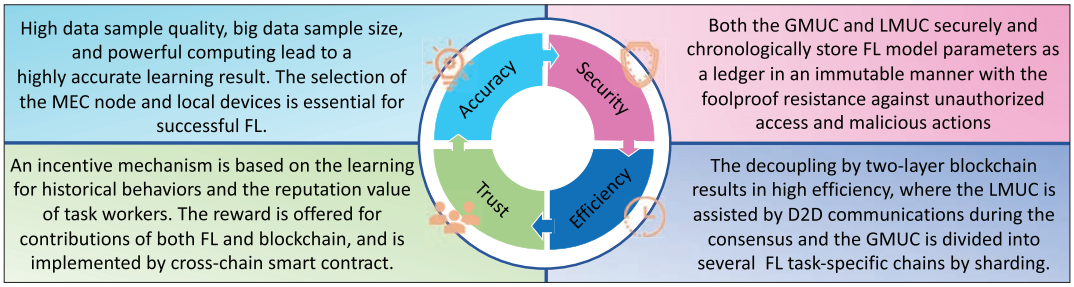

FIGURE 1. Highlights of the two-layered blockchain architecture for federated learning.

the MEC servers, resulting in high latency. In this case, the training process will become inefficient, especially in an online learning environment.

Reward: FL is distributed AI where the selected participants are willing to share their data training results. An incentive reward should be offered to those who provide computing and assistive communication to complete a specific task.

Blockchain was first proposed with bitcoin, which has emerged as a type of chronological, decentralized, provenance-preserving, and immutable ledger technology. All participants can be uniquely recognized in the blockchain network [4]. With the characteristics of tamper-proofness, anonymity, and traceability, blockchain has been significantly investigated for enhancing security in the IoT area [5, 6], such as for vehicular networks and smart grids. The decentralized consensus mechanism [7], tamper-proof records [8], and smart contract for incentives in blockchain enable trust trading or data recording among distributed participants without central authorities [9]. The fusion of blockchain and FL in the mobile edge network can solve the issues mentioned above.

Contributions

Several studies have already explored the issue of fusing FL and blockchain. The authors in [10] introduce an on-device FL architecture called BlockFL, where the local model updates are shared securely through blockchain technology. The local model updates are recorded in blocks, while local devices simultaneously etch the global model updates from the latest block. However, it may be infeasible when all partaking devices chained to the local model updates and calculate the same and accurate global model if the scheduled time is limited. Moreover, the incentive is only proportional to the data size, which cannot completely prevent node fraud. The authors in [11] proposed another blockchain empowered FL named "FLchain" to promote security in the mobile network. It introduces the notion of "the global model state trie" to form a MEC-enabled blockchain. The chained MEC node stores local model updates collected from mobile devices and calculates the global model according to the state trie. Nonetheless, the trust of local nodes participating in FL is still a problem that needs further investigation.

For the sake of trust, security, and efficiency of distributed AI in the mobile edge network, this article introduces a novel blockchain-FL fusion framework. The contributions of this article are summarized as follows.

A two-layer blockchain architecture for FL that simultaneously considers the local devices and MEC nodes is proposed. It consists of two types of blockchains: the local model update chain (LMUC) and the global model update chain (GMUC). The LMUC contains the local devices served by the same MEC node with a good reputation for each FL task computing, while the GMUC contains all of the MEC nodes. This decoupled design provides both trust and efficiency in the mobile edge network.

The blocks in the LMUC are used to record the local model undate results of the FL participants. Blockchain protocols essentially exhibit an inherent speed-security trade-off that depends on the latency of the underlying mobile edge communication network. Therefore, D2D communication is introduced to establish the links of the LMUC that can quickly complete the transmission part during consensus.

The GMUC used to train the FL global model is enhanced by trust and efficiency. The task-specific chain is defined to partition the GMUC according to the FL task attributes and MEC distributions. This sharding design can improve the transaction efficiency performance. Moreover, the reputation of local devices is proposed to serve as the learning parameters recorded in the GMUC ledger to form an endogenous trust.

Smart contracts are used to automatically reward those mobile edge devices participating in FL, which realizes value exchange among raw data provision, model computing, communications-assisting blockchain, and so on. It can be naturally triggered by the efficient cross-chain techniques between the GMUC and LMUC.

The highlights of the two-layer blockchain architecture for FL are summarized in Fig. 1.

Overview of Blockchain-FL Fusion Framework over the Mobile Edge Network

In this section, a two-layered blockchain-FL fusion framework over the mobile edge network is proposed.

Architecture Overview

The physical infrastructure consists of MEC nodes, BSs, and local devices. The MEC nodes are assumed to be deployed beside BSs and chained onto the GMUC. The illustrative architecture is shown in Fig. 2. Each MEC node and its connected local devices constitute the LMUC. The local model is updated based on the newly obtained data and the last global model from the previous learning epoch. This article considers that the formation of the LMUC is assisted by D2D communications among local devices to reduce latency and traffic to the BS generated by

the blockchain. In the LMUC, a full device is one that participates in both FL task computing and the blockchain program, where some devices are only responsible for transferring the data of local model updates. The data throughput on the GMUC is far greater than that of the LMUC. A Byzantine fault tolerance (BFT)-type consensus algorithm is needed to reduce the communication delay as much as possible, for instance, practical BFT (PBFT) and reduced BFT (RBFT). To improve the safety factor of the local model and implementation, the full devices involving the MEC node run the consensus mechanism. Once one full device completes the consensus mechanism, it produces a block that stores all of the verified local model updates. The generated block that stores the local model updates in this epoch is added to the ledger of the LMUC and broadcasted to each local device by cellular or D2D communications. Then the MEC node plays the role of the cross-chain communicator between the LMUC and the GMUC to transfer the recorded data in this ledger.

If all of the MEC nodes in the GMUC participate in the FL model training, the efficiency will be low because of the high transmission and consensus delay among the MEC nodes over vast physical distances in the blockchain. To improve that, this article applies blockchain sharding to the GMUC. The task-specific chain is proposed to chain the MEC nodes that only participate in the associated FL tasks. The ledgers of the task-specific chain used to record global model updates and local device reputations are space-independent and can be processed without relying on the GMUC. The key point to improve the efficiency of the blockchained FL is that only the disposal blockchains within the same shard are synchronous and consistent, while the processing among different shards can be asynchronous. For instance, a global record of the reputations of all local devices can be established through the transactions among these shards. With this framework, both global and local model updates are stored on the two-layer blockchain and cannot be tampered with.

Workflows

As shown in Fig. 3, the workflows and design principles of the proposed two-layer blockchain architecture for FL in the initial epoch are described by the following five steps.

Step 1: FL Task Publishing. The task publishers with specific data requirements first broadcast the FL computation tasks. The relevant MEC nodes in the GMUC can be selected to join the published task. Then the FL task-specific chain containing relevant MECs is formed by GMUC sharding.

Step 2: LMUC Creating. According to the reputation of local devices stored in the GMUC, each MEC selects appropriately associated local devices to participate in the FL training. Then the global model is downloaded to each local device node from the MEC through BS cellular communication. Finally, D2D resource scheduling is performed to form an underlying network for the LMUC, where the selected local devices are chained with low latency.

Step 3: Local Model Update. Each participating local device calculates local model updates according to its data sample. The local model update results are shared among full devices through D2D communication and cellular links. The consensus mechanism is run by the local devices acting as miners until the nouns are found. Then the block recording the local device training results is generated and broadcasted by the successful miner. The details of this procedure are provided later.

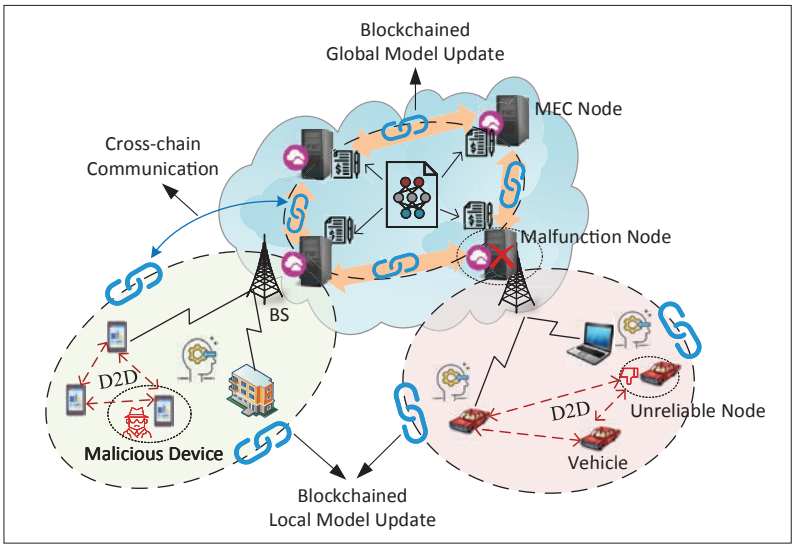

FIGURE 2. Illustrative two-layer blockchain architecture for federated learning over the mobile edge network.

Step 4: Cross-Chain Communication. Each participating MEC node transmits the ledger from its associated LMUC to a task-specific chain in the GMUC. The cross-chain communication techniques are leveraged to support this work. The GMUC and LMUC can be designed as homogeneous blockchains that use the same security and consensus methods to alleviate the difficulty and complication.

Step 5: Global Model Update. The MEC nodes within the same task-specific chain distribute their received LMUC blocks with each other and complete cross-verification to form the aggregate local model updates. The MEC node runs a BFT algorithm and calculates the global model. The MEC node runs a BFT-type algorithm and calculates the global model. The global model updates are recorded with the aggregate local model updates and contributions of the local device in the learning process to generate a new block. Then the blocks are shared with other MEC nodes. The details of this procedure are given below.

The non-initial epoch mainly consists of Steps 3 to 5, and they repeat until the stopping criteria of FL are reached.

Mechanism for Trusted and Secure FL Model Training via Blockchain

Efficiency- and Security-Enhanced Global Model Update via Task-Specific Blockchain

The GMUC that connects all of the MEC nodes into one blockchain can reliably avoid central MEC malfunction problems in mobile edge networks. The learning accuracy of FL could be guaranteed even if one or more central MEC nodes fail. However, although the MEC node is more

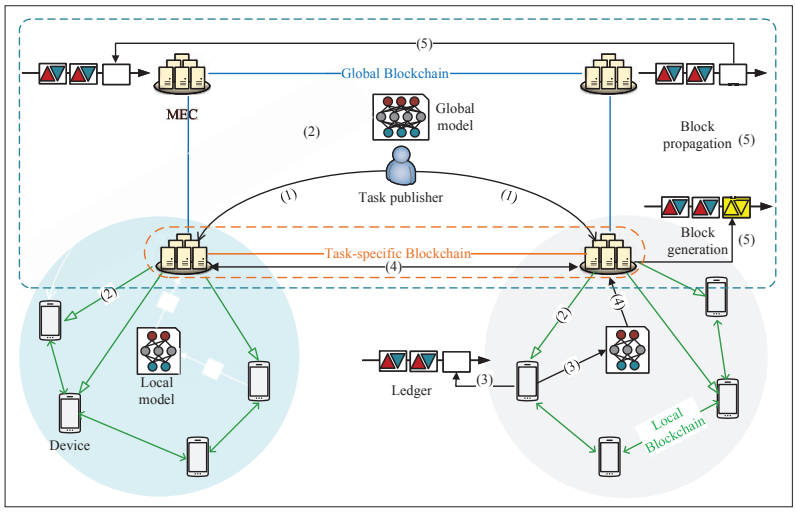

FIGURE 3. Working sequence of two-layer blockchain architecture for federated learning.

reliable than local devices, the basic consensus mechanism is still needed. A BFT-type consensus mechanism is adopted in the GMUC. Consistency in consensus security requires that any transaction which has been recorded on the blockchain and reached a consensus cannot be changed. This means that once a node in the network reaches a consensus on one blockchain, an attacker cannot generate a blockchain fork by effective means. Liveness in consensus security requires that the global model nodes will eventually agree on the legitimate data submitted by honest MEC nodes, and it will be recorded in the GMUC. The legal data includes legitimate transactions submitted by honest nodes, a correctly executed smart contract, its intermediate state variables, and so on. The active node ensures that the honesty can resist denial of service attacks, maintaining continued and reliable operation of blockchain. Nevertheless, there is a balance between efficiency and security in blockchain. The trade-off depends on the latency of the underlying mobile edge communication network. If all of the MEC nodes in the GMUC participate in every FL mission, the fusion work will be inefficient.

To solve the issue of efficiency, this article introduces a strategy called task sharding, which logically slices the GMUC according to various types of FL tasks. Each shard is defined as the task-specific chain that consists of only a subnet of the MEC nodes. The ledgers of the task-specific chain used to record global model updates and local device reputations are space-independent and can be processed without relying on the GMUC. There are two strategies of sharding: isolation and cooperation. The isolation sharding strategy means that each shard is obtained according to different FL tasks. By doing so, the system can consequently learn multiple global models belonging to different task shards, and the consensus is also applied on a per shard basis [12]. The cooperative sharding strategy is a way to make shards work together for one specific FL task. The FL task is first decomposed into several sub-tasks, and then each sub-task is proceeded by one task-specific chain. The shards share their global learning models and collaborate on training one certain FL task. An inter-shard consensus mechanism like trie can be designed appropriately to handle transactions between different shard task-specific chains. For instance, the GMUC can uniformly maintain the reputation records for the local devices aggregated from different shards. Up to this point, the GMUC provides both security and efficiency for FL over the mobile edge network.

Efficient Local Model Update Data Sharing via D2D-Assisted Blockchain

FL is collaboratively distributed AI, in which the data privacy of local devices is protected since none of the raw data is transferred out of local devices. The LMUC securely stores all of the learning models that are transmitted with integrity. It is difficult to manipulate with any malicious attacks. The main concerns lie in the efficiency of applying blockchain and the trust of local devices. Therefore, this article selects the devices as the FL task worker via a reputation-based scheme managed by the GMUC and uses the D2D communication to assist the transmission of the LMUC.

First, each MEC node or local device needs to register with the LMUC, and an identity public/private key pair is generated for each of them. Second, the task publisher generates a request submission transaction that includes its FL computing task with specific resource requirements. A cryptographic hash strategy is used for the content of the transaction. Then the transactions are broadcast to the LMUC and checked to recognize attacks according to the public key derived from the transaction. If resource is available, a response transaction including resource information and reputation opinions is generated and broadcast to the LMUC. The local devices that take part in the FL computation tasks are selected according to reputation opinions from interaction histories and resource information. Once the local devices are determined, the tasks are then assigned as planned. Task packets that are encrypted can be transferred to the selected devices based on D2D communication. When a packet has been received by the local device, it first checks whether the content has been changed. Then the tasks are decrypted and handled. When an FL task is completed, a payment transaction is produced and exchanged among nodes in the LMUC. The task publisher will pay and reward the local devices and update their reputation values. Finally, both the MEC node and the local devices have an identical transaction generated. This transaction is recorded in their transaction pool and broadcast to others in the LMUC. Further, the contribution of each local device is fully visible in the LMUC.

Incentive Strategy Based on Smart Contract

It is essential for improving the reliability of FL to design an efficient incentive strategy. The local devices that contribute more computing and communication effort in the model training should be rewarded properly. Therefore, an incentive strategy based on smart contract theory is employed in this section.

The reward influencing factors are shown in Table 1. There are two types of rewards: FL reward [11] and blockchain reward. The quality and size of the data sample, computing resources, energy consumption, and satisfaction of the FL task will affect the FL reward of the local

Types of reward	Influencing factors	Description
FL reward [11]	Data sample quality	High-quality data brings out good learning accuracy. The number of local model iterations relies on the local data accuracy.
	Data sample size	The device with a bigger data sample size earns a greater reward.
	Computation resources	The device with supporting powerful computation resources, such as CPU cycle frequency, can reduce the global iteration time, thus increasing the profit of the task
	Energy consumption	The device expects to save energy when executing the FL task for maximizing its utility.
	Task satisfaction degree	The satisfaction of the task publisher is inversely proportional to the total time spent in one global iteration.
Blockchain reward	Mining	The local devices provide computing power and energy to generate blocks to allow the LMUC to reach a consensus.
	Communication cost	The bandwidth and transferred data size spent by local devices during D2D communication that help to establish the LMUC.

TABLE 1. Reward influencing factors.

device. At the same time, the blockchain rewards received by local nodes are influenced by mining and communication costs. The FL task publisher provides a reward for training data samples to the devices and for the secure verification of blockchain, which are referred to as FL and mining reward. The local devices directly receive the reward from their associated MEC by the cross-chain smart contract scheme between the GMUC and LMUC. Furthermore, the amount of the FL data reward is normally proportional to the data quality, data sample size, and satisfaction of the task, which are affected by the number of local model iterations and the learning accuracy. The conventional blockchain reward is paid to miners when they generate the blocks [13].

For the convenience of the FL task publisher to reward the devices, it is necessary to have the quantitative criteria for designing the contracts [11]. This article proposes a learning-based solution. Specifically, the task publisher does not exactly know the current state of a given device due to information asymmetry. To solve this, the historical statistics of reputations stored in the GMUC and the behaviors of devices recorded by the FL task publisher can be used as the input to form a deep-learning-trained network. The output of this network is the clustering of local devices. The task publisher designs specific contracts for different types of devices and offers different incentive packages depending on the specific FL task requirements. The device will not be rewarded if the participating load device fails to complete the learning task or misbehaves, causing the task publisher to treat the interaction as a negative event and thus refuse to pay. The objective of the incentive scheme maximizes its profit in the FL task within the given cost constraint.

Based on the above reward investigations, the incentive mechanism can be designed referring to [14]. Each FL computing local device is assumed to be self-interested, and the valuation of the local device is zero without reward. The correct clustered devices can obtain a larger reputation value since they contribute more to the FL tasks. Poisoning attacks launched by malicious devices decrease the local data accuracy, thus worsening the local model update. Fortunately, with the help of a smart contract, malicious workers will not be selected to sign the contract items that require the reputation value to be higher than theirs. Therefore, the proposed mechanism based on contract can incentivize high-quality and large-sample-size data and no behavior-impaired local devices to join the FL task.

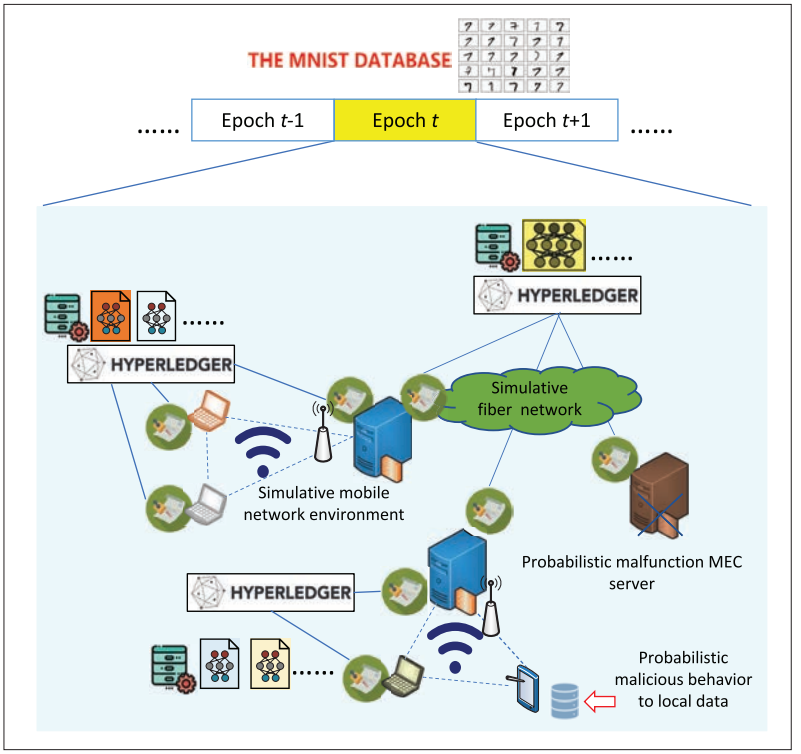

FIGURE 4. FL Case based on MNIST data and Hyperledger.

Case Study

Simulation Setting

To evaluate the performance of the proposed two-layered blockchain scheme for FL, this article implements a simulation case based on a well-known digit classification dataset named MNIST by using Tensorflow for digit classification, as exhibited in Fig. 4. Malicious local devices appear randomly, which are characterized by tampering with the label of the training set. Malfunctioning MEC nodes also appear randomly with a fixed number, resulting in poor FL results in each training epoch. The blockchain system is established on the hyper-ledger fabric. As an open source distributed ledger technology (DLT) platform, it applies a highly modular framework that enables

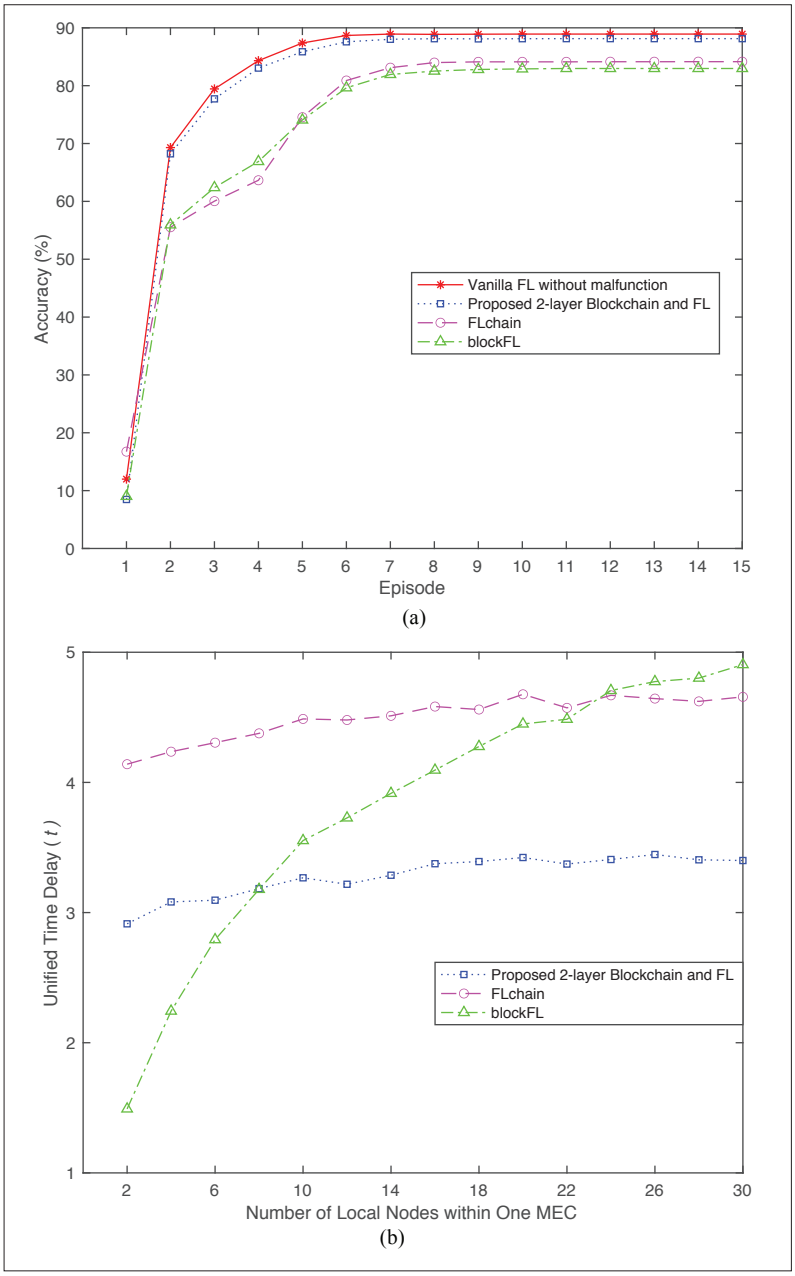

FIGURE 5. Performance evaluation results: a) federated learning accuracy vs. episode; b) unified time delay vs. number of local devices.

configuration and scalability for a wide range of industry use cases.

In the constructed simulation network, several MEC nodes and their associated BSs are deployed with a virtual geographic distribution to construct the GMUC. Let t denote the unified time unit spent in storing a block by one node. The propagation delay caused by the physical distance between the interconnected MEC nodes is assumed to follow a normal distribution with the mean of 2 t and the standard deviation of 1.1 t. The transmission powers of the BS and local device are 43 dBm and 23 dBm, respectively. The distance-dependent channel gain is exponentially distributed, and the Shannon formula is used to calculate the transmission delay. The D2D propagation delay between local nodes within one LMUC is set as a normal distribution with a mean of 0.5 t and a standard deviation of 0.25 t.

To evaluate the proposed two-layered blockchain for FL, which is the ideal vanilla FL without malfunctioning MEC [15], both FLchain and blockFL are selected as the compared schemes [10, 11].

Simulation Results

Figure 5a shows the performance of the FL learning accuracy for the proposed scheme and its comparisons. The number of MEC nodes is set as three, while 10 local nodes participate in one MEC node. As shown in Fig. 5a, the learning accuracy obtained by the proposed scheme is higher than FLchain and blockFL, which is very close to the ideal case, which is vanilla FL without MEC malfunction and local node cheating. This verifies that the two-layer blockchain and FL method can prevent the malfunctioning of MEC with the help of distributed model computing in the GMUC and the malicious behavior of MEC to modify local model updates since it is chained to the LMUC. The simulation results also show that the proposed method can avoid selecting malicious local nodes to participate in the FL task due to the designed reputation scheme, which significantly improves the learning accuracy.

Figure 5b shows the unified time delay vs. the number of local nodes within one MEC, which aims to reflect the efficiency of blockchain storage and transmission. The blockFL that connects all local devices into a single chain through the MEC node has a comparative advantage when the number of local nodes is small. However, as the number of local nodes increases, the time delay increases significantly since the blockchain consensus process becomes less efficient. Moreover, the delay fluctuation of the proposed two-layer blockchain and the FL fusion scheme is also not sensitive to the increasing number of local nodes because of the D2D assistance in the LMUC. The proposed scheme performs better than FLchain in delay performance. The reason for this is that in this article, the sharding strategy in the GMUC is FL task-specific rather than channel-specific. The global model that updates for one FL task does not need to be synchronously transferred to all MEC nodes. Therefore, the two-layered blockchain architecture for FL proposed in this article is verified to efficiently reduce the time delay efficiently with stable performance when the number of FL participants increases.

Conclusion

This article investigates a novel integrated framework of two-layered blockchain for FL, which consists of two types of blockchains: LMUC and GMUC. This decoupled design provides both trust and efficiency in the distributed AI over the mobile edge network. The blocks in the LMUC are used to record the local model updates of the FL participants in a chronological and tamper-proof manner. Furthermore, D2D is introduced to assist the transmission of the LMUC to reduce the delay and traffic produced during blockchain consensus and data recording. The GMUC can securely obtain the global model updates by mitigating the training failure caused by malfunctioning MEC nodes and malicious local devices. The MEC nodes in the GMUC are organized into different shards to improve efficiency. Moreover, a smart contract implemented by the cross-chain between the

LMUC and GMUC is introduced to reward the contributions from both the blockchain and FL. The learning-based incentive mechanism forms endogenous trust, and the participating local devices in each FL task are reliably selected by the good reputation recorded in the GMUC. The case study verifies that the accuracy and efficiency of the proposed blockchain-FL fusion framework are higher than those of the compared schemes. In future work, the authors will consider the mobility of local devices in the LMUC and complex network attack scenarios. In addition, a more intelligent, efficient, safe, and reliable algorithm mechanism will also be the focus of future research.

The case study verifies that the accuracy and efficiency of the proposed blockchain-FL fusion framework are higher than those of the compared schemes. In future work, the authors will consider the mobility of local devices in the LMUC and complex network attack scenarios. In addition, a more intelligent, efficient, safe, and reliable algorithm mechanism will also be the focus of future research.

Acknowledgment

This work was funded by National Key R&D Program of China (2018YFE0205502). Corresponding author: Shaoyong Guo.

References

[1] P. Popovski et al., "Wireless Access for Ultra-Reliable Low-Latency Communication: Principles and Building Blocks," *IEEE Network*, vol. 32, no. 2, Mar./Apr. 2018, pp. 16–23.
[2] A. Zappone, M. Di Renzo, and M. Debbah, "Wireless Networks Design in the Era of Deep Learning: Model-Based, AI-Based, or Both?" *IEEE Trans. Commun.*, vol. 67, Oct. 2019, pp. 7331–76.
[3] M. Shayan *et al.*, "Biscotti: A Ledger for Private and Secure Peer-to-Peer Machine Learning," Nov. 2018.
[4] K. Salah *et al.*, "Blockchain for AI: Review and Open Research Challenges," *IEEE Access*, vol. 7, 2019, pp. 10,127–49.
[5] X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-Hoc Network," *IEEE Access*, vol. 7, 2019, pp. 58,241–54.
[6] J. Kang *et al.*, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," *IEEE Internet of Things J.*, vol. 6, June 2019, pp. 4660–70.
[7] R. Doku, D. B. Rawat, and C. Liu, "Towards Federated Learning Approach to Determine Data Relevance in Big Data," *Proc. 2019 IEEE 20th Int'l. Conf. Info. Reuse and Integration for Data Science*, July 2019, pp. 184–92.
[8] S. Samarakoon *et al.*, "Federated Learning for Ultra-Reliable Low-Latency v2v Communications," *Proc. 2018 IEEE GLOBECOM*, Abu Dhabi, UAE, 2018, pp. 1–7.
[9] X. Bao *et al.*, "Flchain: A Blockchain for Auditable Federated Learning With Trust and Incentive," *Proc. 2019 5th Int'l. Conf. Big Data Computing and Commun.*, QingDao, China, Aug. 2019, pp. 151–59.
[10] H. Kim *et al.*, "Blockchained On-Device Federated Learning," *IEEE Commun. Letters*, 2019. DOI:10.1109/LCOMM.2019.2921755.
[11] U. Majeed and C. S. Hong, "Flchain: Federated Learning via Mec-Enabled Blockchain Network," *Proc. 2019 20th Asia-Pacific Network Operations and Management Symp.*, Matsue, Japan, 2019, pp. 1–4.
[12] P. Thakkar *et al.*, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform," *Proc. 2018 IEEE 26th Int'l. Symp. Modeling, Analysis, and Simulation of Computer and Telecommun. Systems,* Milwaukee, WI, 2018, pp. 264–76.
[13] J. Sidhu, "Syscoin: A Peer-to-Peer Electronic Cash System With Blockchain-Based Services for E-Business," *Proc. 2017 26th Int'l. Conf. Computer Commun. Networks,* Vancouver, BC, Canada, July 2017, pp. 1–6.
[14] Y. Zhang *et al.*, "Offloading in Software Defined Network at Edge With Information Asymmetry: A Contract Theoretical Approach," *J. Signal Processing Systems*, vol. 83, Sept. 2015, p. 241–53.
[15] J. Konečný *et al.*, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," arXiv eprints, arXiv:1610.02527, Oct. 2016.

Biographies

Lei Feng received his B.Eng. and Ph.D. degrees in communication and information systems from Beijing University of Posts and Telecommunications (BUPT) in 2009 and 2015. He is a lecturer in the State Key Laboratory of Networking and Switching Technology, BUPT. His research interests are resources management in wireless networks and smart grid.

Zhixiang Yang received his B.Eng. degree from Beijing Jiaotong University in 2018. He is currently working toward a Ph.D. degree at BUPT. His research interests include wireless network resources management and backscatter communication.

Shaoyong Guo received his Ph.D. degree from BUPT. He received his B.S. degree in information and computing science from HeBei University. His research interests include blockchain application technology, mobile edge computing, and IoT in energy Internet.

Xuesong Qiu is a professor at BUPT and serves as the vice-president of the Institute of Network Technology, BUPT. He has hosted a series of state research projects on network management. He has earned more than 13 China state-level, provincial, and ministerial-level science and technology prizes. His major research interests include network and service management, and information and communication technology of smart grid.

Wenjing Li is a professor at BUPT and serves as a director in the Key Laboratory of Network Management research center. Meanwhile, she is the leader of TC7/WG1 in the China Communications Standards Association. Her research interests are wireless network management and automatic healing in SONs.

Peng Yu received his B.Eng. and Ph.D. degrees from BUPT in 2008 and 2013, respectively. He is currently an associate professor at the State Key Laboratory of Networking and Switching Technology, BUPT. His research interests are autonomic management and hybrid energy allocation in GreenNet.