Blockchain and Federated Learning: Securing Decentralized Machine Learning Systems

By **Dr. Peter Murphy**

Professor of Computer Science, Dublin City University, Ireland

1. Introduction to Decentralized Machine Learning

Overall, our work continues the nascent exploration of blockchain and distributed ledger technologies for enhancing privacy and security, and argues that it could be fruitfully combined with the fostered decentralization in machine learning. We do not advocate blockchain as the new best mechanism for securing every machine learning update, but we provide a working prototype as a step towards the use of the technology in practice for the first layer of a decentralized machine-learning system.

With this objective, alongside a thorough description of the setting and mechanics of decentralized training using federated learning, we make two main contributions. First, we provide a concrete methodology to apply a permissioned blockchain to secure federated learning in a privacy-friendly and performance-aware fashion – even amid a non-collaborative adversary. Second, we propose to extend the use of blockchain to securely share knowledge between models in a similar privacy-preserving fashion. We implement a first proof of concept of this blockchain-based approach, develop a mechanism to provide strong and efficient security guarantees, and experimentally evaluate its performance.

Training large machine learning models on centralized servers requires users to share massive data that often contain sensitive information, enabling malicious entities to snoop on private details. This situation gave rise to decentralized machine learning, which keeps the training data private through devices such as user-owned models or on-premises training methods. More recently, it has led to novel approaches such as federated learning, which instead attempts to fine-tune a globally shared model based on locally computed updates. Despite their data privacy, though, these decentralized settings also pose significant trust and security challenges. In particular, how do the users, and more broadly any observer, know that the updates made on the model actually improve it—and have been computed correctly, without introducing backdoors? To enforce this trust in decentralized machine learning, in this paper, we propose the use of blockchain technology.

1.1. Definition and Importance of Decentralized Machine Learning

Specifically, DML aims to overcome the traditional FL [Federated Learning] in which the users need to download and install the algorithm to carry out self-learning, which is called Centralized Machine Learning (CML). In the domain of deep learning, DML mainly focuses on using the basic model, vector aggregation, and matrix aggregation techniques to handle the centralized aggregated models of all the round learning steps in FL. In the external domain of deep learning, DML mainly focuses on optimizing the security technology for network connection, such as using Secure Sockets Layer/Transport Layer Security (SSL/TLS) for ensuring remote keystroke and screen mirror, and so on. In the direct privacy-protection domain, DML mainly focuses on using the homomorphic encryption and privacy-preserving mediated neural network technology for ensuring privacy-preserving computation.

Due to the increasing availability of big data storage and computing resources, and the improvement of machine-learning algorithms, smart learning models have arisen in which the more data you have, the more accurate the models. However, the recent privacy scandals alert us to the concern that it is best that users keep their private data. Decentralized Machine Learning (DML) distributes the machine to the data, gives the algorithm to the distributed data subjects for self-learning, and then summarizes the models via secure aggregation. DML can help avoid personal privacy leakage, provide social intelligence feedback, and train boycotted models that are less likely to have unfair discrimination, and so on.

2. Fundamentals of Blockchain Technology

A hash function is a mathematical function that takes an input 'a' and converts it into an almost-unique identifier of a fixed length. For two inputs 'a' and 'b' that are distinct, their hash values h(a) and h(b) will very rarely be the same. When building blockchains, however, a cryptographic one-way hash function is employed. The hash value of the previous block is stored in the current block, meaning that each block is linked to the previous, and the previous to the block previous to that one, backwards, creating the decentralized, tamper-proof sequence. Finally, blockchain systems feature consensus protocols as their primary mechanism to ensure trust in an untrusting setting. These protocols are used to agree on the order of transactions across the instances of a database in a transaction processing system.

A blockchain is, in essence, a linked list in which every item of data is linked to the previous item in a way that is permanent and universal. New items (called "blocks") may only be added to the list, and never removed. To make changes to items of data on the blockchain, it is necessary to create a new block to reflect this change, linked to the previous block, almost like a branch on a tree. This structure makes a blockchain both secure and tamper-proof; all data on the blockchain is immutable, and everyone looking at the same blockchain should arrive at the same values for the items within. A blockchain is typically used to establish and maintain a continuously growing list of records hardened against tampering and revision, and it offers a secure, instant, and sustainable consensus among multiple parties.

2.1. Key Concepts and Components

Federated Learning (FL) is a machine learning system where the model is trained in a distributed manner across FLPs, who own the data or models. The learning process is summed up in Fig. 1. In the training round, the central server aggregates functions over input models within a certain adjustment space with each FL party (FLP) that has a device. The N models' aggregations are shared with the central server. The central server then updates the global model and delivers the updated model to participants. The federated learning process is carried out in multiple communication rounds, such as through a local mini-batch with local examples. In FL, core to the learning process are the following aspects: the server aggregates the model parameters according to the local gradients, and FL participants have some control over model parameters during the learning process to, for example, improve performance and optimize the communication load according to network conditions.

2.1.1. Federated Learning (FL)

This section introduces essential concepts and components of FL and blockchain that are relevant to the discussions below. Noting that the deep learning model is a typical ML model used in FL, this paper uses the terms deep learning model and deep learning party interchangeably, as appropriate, to simplify the presentation.

3. Federated Learning: Collaborative Machine Learning

Moreover, the quality of a model for a given user is not only determined by the local data set, but by the combined set of global data sets. Without access to the global data, as would be the case for a user storing personal data in a personal data bank, the model quality might remain sub-optimal. Considering the great advantages of it compared to traditional machine learning, we use federated learning as a proof of case for our work to design the secured decentralized machine learning.

Federated learning is a machine-learning setting where multiple clients pool their data together in order to collaboratively train a single joint model. Rather than gathering copies of all the trained data at a central location and training the model there, the model is trained locally on each of the personal data sets and the models are collectively aggregated. In other words, the federated learning concept seeks to give users control over their data and future applications, even when training a collective model. It is uniquely capable of addressing collective learning for which the model lives in a centralized setting, but where the data is not all available in a single repository. We consider the setting in which the data generated by the users are themselves tied to the user. Therefore, constructing a global data store to store all data in practice may be impossible, illegal, unethical, or cost-prohibitive.

3.1. Concept and Advantages

After a transaction is made and is added to a block, the block is then added to the network, and the user can no longer manipulate that transaction record. After a while, more blocks are connected to the block containing the transaction record. The network recognizes the block and the record will be considered confirmed. Each record in a blockchain is considered as being immutable because the user can no longer modify it.

There are other systems to establish the consensus among the blocks. Another widely used consensus is called Proof of Stake (PoS in short) which is based on the wealth of the data miner inside the network. Therefore, it is also energy-efficient by requiring less computational power. Naturally, the traders of who create block will be incentivized by block rewards and transaction fees. This ensures blockchain security and the safety features of the ledger.

When a new block is added to the blockchain, it is added by data miners who are users who solve complicated mathematical puzzles that require lots of computational power. This process is called Proof of Work (PoW in short) and it is used to establish a consensus that the blocks are legitimate and then only add these blocks to the blockchain. This makes the blocks immutable and very hard to hack. Therefore, data stored in the blockchain are tamper-proof and people usually trust the data.

One of the simplest explanations for a blockchain is that it's like a global spreadsheet that keeps a record of who owns what. However, blockchain is also a groundbreaking technology that has enabled cryptocurrencies and cryptocurrency transactions. A blockchain is like a digital ledger where transactions or data are recorded. All data stored in a blockchain are organized in batches that are called blocks. Each block is then linked with previous blocks together, which creates a chain of blocks called the blockchain. The blocks are stored in a public or private network so that multiple users can access the ledger.

3.1. Blockchain Concept and Advantages

4. Integration of Blockchain and Federated Learning

The recent success of decentralized machine learning, centralized trustless consensus, and data mining in blockchain databases prove that blockchain and machine learning can effectively benefit each other. This paper investigates the complementary advantages of blockchain, which offers network data integrity services that enforce independent trust models in machine learning, and federated learning, which preserves data privacy and is communication-efficient in decentralized networks. We propose the adoption of federated learning in the synchronization of blockchain data to further enhance both data-mining efficiency and model accuracy. The paper reviews fundamental concepts of both cooperative federated learning models, which sync partial updates of user models, and non-cooperative cryptographic models, which communicate secrets generated from user data only. We model the efficient convergence of federated learning after model initialization as well as the data mining strategies as multiple rounds of on-chain data operations corrupted with malicious attacks. The empirical study reveals that federated learning can reduce the on-chain data noise in these models by approximately 30-40% under various source distributions.

In this study, blockchain serves as a secure and efficient way to guarantee access control, failure model, communication protocols, and result authentication within federated learning. Blockchain is an open and decentralized way of ensuring authenticity, reproducibility, auditability, and resilience to vote manipulation, while federated learning is an effective way of privacy-preserving machine learning, especially in a decentralized data training model. We aim to combine the benefits of blockchain and federated learning to solve the problem of relying on trustworthy centralization servers. We propose three protocols for the integration of blockchain and federated learning, which are the communication protocol to synchronize models inside a block, the blockchain voting protocol to use the blockchain to make failure model-based final decisions, and the authentication protocol to verify the validation of aggregated local model updates. More specifically, the communication protocol and blockchain voting protocol can be established with long-range wireless communication that only synchronizes local models between pairs and communicates with the blockchain.

4.1. Benefits and Challenges

An architecture named BAC-Learn is designed to address the limitations associated with current off-chain service providers by registering model updates onto PoW blockchains directly to achieve Byzantine consensus. We examine the features of BAC-Learn and discuss its shortcomings. Benefiting from blockchain immutability, audibility, and accountability, BAC-Learn ensures that the integrity and correctness of Byzantine-consensus FL model updates for heterogeneous devices cannot be compromised. Additionally, the malicious behavior of the service provider, such as model attacks and data privacy leakage, is defeated. However, BAC-Learn is unable to cope with other types of model poisoning present in FL, which are within the FYO (Find Your Own) setting or are closely related to the FYO setting. The performance bottleneck due to high volume and low throughput, limited control over block creation and consensus, low block confirmation time, elevated block generation latency, and high consensus latency are non-negligible to FL.

In federated learning (FL), in contrast to other emerging decentralized systems including cryptocurrency systems and data-sharing networks, blockchain has received relatively less attention due to its priority in conflicting requirements, such as security, throughput, and latency. In the past, a variety of off-chain service providers are provisioned to register the FL devices and verify the integrity of FL models, whose availability is difficult to guarantee. Given the limitations and inefficiencies of such off-chain designs, security issues become a serious concern.

5. Security and Privacy in Decentralized Machine Learning Systems

In particular, the current configuration of federated learning has created some of the same kinds of security challenges that we are used to seeing in other private data use implementations. This means that we need to have an equally skeptical approach when talking about federated learning. By this, we mean that we need to be more interested in the assumptions being used by the ML systems. It is not enough to say that a model was trained using federated learning any more than it is enough to say that we have implemented a cryptographically verifiable database. In both cases, we need to interrogate the actual implementation within the security and privacy guarantees it offers because there will indeed be unknown unknowns with such a simplified high-level design.

Security and privacy have always been significant challenges for data science. In our particular focus on decentralized machine learning systems, we want to highlight the key lessons that we can derive from the initial design and implementation of the privacy-preserving model training formalized as federated learning. Firstly, we note that this system is often poorly understood even in the basic assumptions despite widespread interest and investment. We would like to note that "better" isn't the same thing as "perfect", especially when the current practice is for "privacy" to be an argument that processes less data.

5.1. The current state of affairs in decentralized machine learning:

Lessons from privacy-preserving modeling in federated learning

5.1. Threats and Solutions

In the context of some simple machine learning problem, where we hope to use distributed machine learning as a service between some hegemons since the data needed to train the model is itself private, the purpose of training the model is lost if the data owners cannot ensure that the model trained using their individual data is secure. The usual context for discussing the privacy threat is in the context of adversarial learning. Our threat model is slightly different and instantiated analogously: when a single agent has been assigned the task of training a large-scale model with data input by many people, at some point they will take a decision on what quantity or set of concepts will need to be learned from the input data. Simply put, many people contributing their private data on past physical activities should not result in an agent modeling the activity without their consent.

The main goal of federated learning is to ensure that no single party gains undue indirect access to the training data, so it is not as much an algorithm for decentralized learning as it is an algorithm for keeping the data centralized while still allowing the agent with whom it is centralized to perform useful learning tasks. In blockchain, the essential goal is to keep the data centralized and secure while performing a decentralized learning algorithm. The uses above of both technologies reveal certain small problems in each technology that prevent it from being immediately effective for the other technology's purposes. We outline some of the problems in this section, and also propose some small modifications to make the integration of both blockchain and federated learning more efficient for the use cases presented. The paper then provides a new implementation that benefits from the most important aspects of both technologies.

6. Case Studies and Applications

Blockchain can be more than a protocol that solves the Byzantine general problems and secures the federated learning decentralized network. It also has a self-interest role in synthesis and promotion for the privacy and security federated AI network. The publisher can provide and serve the worker or the publisher's AI algorithm with better QoS or more private and higher quality data. We have explored those characteristics of two types of federated learning participants' perspectives, focusing on their business objectives in participating in the federated learning process, by providing more private data protection between the workers and the publisher.

The healthcare industry is the first candidate that could integrate the federated learning blockchain to improve the security and reserve the operational value for the amount of contribution with the data and deliver the secure updatable AI-assisted doctors' diagnosis progress. The patient can choose the institutions and publishers who publish the scientific articles as the data updaters. The health institution using blockchain to manage the publications and provide the secure aggregation for the federation AI manufactory, to share a more unit price to hire AI algorithm service and require the undisputed transaction to link to the Comma based smart contract. Finally, the medical industry can share the profits and promote the research and enhancement on those specific.

Given the practical utility of federated learning proved in several domains like the mobile keyboards, mobile recommender systems, and mobile photographs, we are curious about how better data security with blockchain could improve the quality or deliver lower costs to the models built. Then we go over two possible applications of blockchain in the federated learning domain. Firstly, is the secure aggregation protection for publisher institutions, and secondly, is the data owners can provide or serve the workers' AI algorithm with healthcare diagnostics data.

6.1. Real-world Implementations

The first of these techniques involves labeling blockchain participants to track their contributions. Furthermore, we build a decentralized platform which needs to outsource virtually no functionality. ChainFLeNet creates a decentralized AI model based on federated learning technologies, minimizing the leakage of differentially private information. ChainFLeNet designs the Hyperledger Fabric-based federated learning blockchain network in order to reach consensus faster, reduce the overall complexity, and meanwhile maintain a secure and robust system. The combination of properties defined allows ChainFLeNet to be a very suitable blockchain-based federated learning system for zero-knowledge proof requirements both in theory and experimental outcomes. We demonstrate the feasibility of ChainFLeNet and its effectiveness and security through real scenarios and a large number of assessments. With its advantages, on issues such as scalability and zero-knowledge proof complexity, ChainFLeNet is better than existing work. However, since ChainFLeNet needs simulations for practical scenarios to prove the guidance orientation of future work, results may differ in the presence of real heterogeneous data.

This article introduces a decentralized and secure system building on blockchain and federated learning that ensures that data is not transferred, reducing the possibility of privacy intrusion. I envision implementing AI-enabled masterpieces composed by various AI developers. Lastly, I see that this kind of system promotes the development of more sophisticated AI with acceleration by ensuring that privacy is not endangered. The first decentralized deep learning platform utilizing blockchain that uses Masked Federated Aggregation. We present a novel blockchain-based federated learning framework called ChainFLeNet, which uses the Hyperledger Fabric platform to manage the overall training process and designs blockchains in different configurations.

7. Future Trends and Research Directions

Ancillary benefit of using a permissioned broadcasting blockchain is exclusion of all exchange NPs from the validation process. The only nodes needing to actively participate in its management — the broadcaster and the four selected block-signing validators.

Another promising area is big data markets: the current concept essentially assumes all data buyers to be registered individuals interested in one-time deals. The use of blockchains could facilitate long-term bidding and private movie-style markets. The use of a blockchain for a market would require having at least the necessary crate access rules provided enforced in the smart contracts. Such an organization could be used to scale personalized dietary recommendation services for allowed individuals. The use of these AI-informed services is particularly important for suitable nutritional management in patients with cancer.

One promising research direction for the use of blockchains with federated learning can be thus formulated in terms of differential privacy threshold selection. A decentralized organization of health systems from multiple countries may wish to conduct an AI trial, while the local participating entities are individually constrained in applying flexibility to the AI model training. In such a case, the use of a blockchain could provide technical guarantees and streamline a consortium governance and control, ensuring a jointly agreed outcome.

For example, the assertion that blockchains are just another kind of a distributed database to store the model updates can be quickly silenced after reviewing the practicality of such systems. Also, the proactive discussion examples on both blockchains organization-level guidelines provide additional networking feints by recruiting all who contribute.

From the market-perceptive point of view, the lack of engagement or priority of AI in all the blockchain consortiums surveyed to date may indicate biases not in favor of promoting this confluence and API foundation. We also presented how the two architectures can be internally networked with thinking in the context of deploying to large-scale global clinical AI systems in health. The presented considerations on the current workings in blockchain research may help to scotch some yet active false narratives around the current developments.

In this work, we have examined the two pillars of the force that may reshape the clinical AI landscape within the next decade. While much of the activity around blockchain in the context of federated learning and privacy-preserving computation is still at the proof-of-concept phase, the internetworking is the next essential step to transform this vision into a reality. The one question is whether the aspects of the blockchain architecture stand in the way of this vision or on its path.

7.1. Emerging Technologies

Technologies become transformative when we succeed in creating secure, privacy-preserving, and compliant systems. We introduced trustware vision exploiting the convergence of federated learning, privacy-preserving cryptographic primitives, trusted execution enclaves, and blockchains. In advising the responsible development and deployment of these technologies, we presented ethical guidelines for the integration of machine learning and privacy technologies. Finally, we believe that this vision of trustworthy and responsible development establishes human values as the guiding principles for the future of work, health, and our society at large.

The emerging blockchain technology represents a mechanism for building secure, decentralized applications that remove the intermediary and thus foster privacy and trust in applications. Notably, the integration of machine learning and blockchains has great potential. It can enable novel decentralized machine learning systems for secure and private data management and inference. Federated Learning is a novel decentralized machine learning approach that enables and accelerates the creation of secure and privacy-aware machine learning applications. We have reviewed the two approaches—via the lenses of 11 challenges that must be addressed to engineer trustware vision.

8. Conclusion

The critical role of knowledge discovery platforms such as those based on machine and deep learning encourages researchers to contribute significantly to these technologies. Unfortunately, the ML models representing the majority of today's implemented artificial neural networks and deep learning structures have several drawbacks, mainly associated with significant data propagations over insecure channels and massive vulnerability to adversarial attacks and adversaries. However, deep learning, the most advanced but by far the newest area of machine learning technologies, introduces the novelty framework for the elimination of the said vulnerabilities constructing models with a federated scheme which secures individual parts of today’s most elaborate models in separate containers by hosts. Despite the contributions made by the Coordination Intelligence Community, some critical FL vulnerabilities have relied on the related risk ensemble model created over each given learning step, while attacking against the entire model could increase the modeling complexity to its maximum.

This chapter presented the current state of the art of blockchain-secured decentralized machine learning methods. We further motivated the necessity of protecting ML models, techniques to protect federated learning, specifically the usage of BCT in this task, and ethical considerations. Furthermore, end this chapter validating the use case on energy forecasting and microgrid optimization, shedding some light into the complexity of integrating multiple parties with varied levels of data-sharing interests in the success of the FL operation. We believe this chapter sets the stage for researchers in deep learning, machine learning, blockchain, and their intersections, to further advance this important initial work and help secure the further development of the new wave of decentralized machine learning infrastructures.

9. References

1. A. Mohamed, K. Yan, M. Chen, Q. Yang and X. Li, "Secure Federated Learning Framework with Blockchain for IoT," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5416-5423, 1 April1, 2021.
2. Tatineni, Sumanth. "Customer Authentication in Mobile Banking-MLOps Practices and AI-Driven Biometric Authentication Systems." *Journal of Economics & Management Research. SRC/JESMR-266. DOI: doi. org/10.47363/JESMR/2022 (3)* 201 (2022): 2-5.
3. Shaik, Mahammad, and Ashok Kumar Reddy Sadhu. "Unveiling the Synergistic Potential: Integrating Biometric Authentication with Blockchain Technology for Secure Identity and Access Management Systems." *Journal of Artificial Intelligence Research and Applications* 2.1 (2022): 11-34.
4. L. Liu, K. Li, M. Cui, J. Xu, W. Gao and C. S. Jensen, "FLChain: A Blockchain-Based Secure Federated Learning System for Healthcare," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1287-1298, 1 February1, 2021.
5. S. Wang, Y. He, X. Wang and Y. Liu, "Blockchain-Enhanced Secure Federated Learning with Differential Privacy Preservation," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2021.3083668.
6. S. Jia, Z. Qin, J. Zhou, Y. Liu and Y. Zhang, "Blockchain-Enabled Federated Learning: A Comprehensive Review and Future Directions," in IEEE Internet of Things Journal, vol. 8, no. 9, pp. 6953-6969, 1 May1, 2021.
7. Z. Cheng, J. Cao, S. S. Kanhere, and Y. Zhang, "Blockchain-Based Federated Learning: A Survey," in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1239-1264, 1 May1, 2021.
8. Z. Li, J. Chen, K. He, J. Zhang, and K. B. Letaief, "Blockchain-Enabled Federated Learning: Challenges and Opportunities," in IEEE Wireless Communications, vol. 28, no. 2, pp. 88-95, 1 April1, 2021.

9. J. Xu, Z. Qin, S. Wang, S. Li, Y. Liu and X. S. Shen, "Blockchain-Enabled Secure Federated Learning for IoT-Enabled Autonomous Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 3329-3338, 1 July1, 2022.
10. W. Zeng, S. Wang, Z. Wang, J. Wang, J. Cai and H. Zhang, "Secure Federated Learning with Blockchain for Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 1195-1204, 1 February1, 2021.
11. H. Liu, Z. Zhang, M. Li, X. Shen, and X. Lin, "Blockchain-Assisted Secure Federated Learning in Mobile Edge Networks," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5158-5166, 1 April1, 2021.
12. H. Yu, J. Wang, C. Yao, X. Liao, X. Zhou and X. Fu, "BlockFL: Blockchain-Based Federated Learning Framework for Industrial IoT," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2022.3194775.
13. X. Xu, H. Zhu, H. Hu, C. Lin, and L. Zhou, "Blockchain-Enhanced Federated Learning: A Survey," in IEEE Transactions on Computational Social Systems, vol. 9, no. 4, pp. 1354-1368, 1 July1, 2022.
14. Q. Wang, Y. Ren, Y. Chen, Z. Chen, Z. Wang, and H. Zhou, "Blockchain-Enhanced Privacy-Preserving Federated Learning in Wireless Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 7104-7112, 1 October1, 2021.
15. C. Li, M. Pan, Y. Liu, S. Yi, and Z. Qin, "FedProx: Blockchain-Enabled Federated Learning with Differential Privacy Preservation for IoT," in IEEE Internet of Things Journal, vol. 9, no. 2, pp. 869-880, 1 January1, 2022.
16. J. Wang, X. Fu, Y. Yang, L. Ma, X. Zhou and J. Cai, "Blockchain-Based Secure Federated Learning in Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 7002-7011, 1 October1, 2021.
17. H. Zhu, X. Xu, H. Hu, C. Lin, and L. Zhou, "Blockchain-Enhanced Federated Learning: A Survey," in IEEE Transactions on Computational Social Systems, vol. 9, no. 4, pp. 1354-1368, 1 July1, 2022.
18. L. Zhou, J. Yang, W. Liang, K. Zhang, and X. Shen, "Secure and Privacy-Preserving Federated Learning with Blockchain for 6G Communication," in IEEE Network, vol. 35, no. 5, pp. 150-157, 1 September1, 2021.
19. M. Zhang, Y. Ren, J. Liu, Z. Chen, Y. Xu, and H. Zhou, "Blockchain-Based Federated Learning Framework for Industrial Wireless Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 6590-6600, 1 September1, 2021.
20. Z. Chen, Y. Ren, M. Zhang, J. Liu, Y. Xu, and H. Zhou, "Secure Federated Learning with Blockchain in Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 4765-4773, 1 July1, 2021.