A Method of Federated Learning Based on Blockchain

Shicheng Xu
TSD, Neusoft, Shen Yang, China
xushicheng@neusoft.com

Sihan Liu*
TSD, Neusoft, Shen Yang, China
294335826@qq.com

Guangyu He
TSD, Neusoft, Shen Yang, China,
hegy@ neusoft.com

ABSTRACT

Currently many enterprises face issues regarding insufficient data collection samples and data recording dimensions, thus it's hard to make efficient predictions. Since it is limited by the requirement of protecting privacy and trade secrets, data can't be effectively shared among enterprises. Federated learning is an effective method to solve this problem, but there are some performance bottlenecks, information security issues and data trust issues still existed, which need to be improved in combination with other advanced technologies to meet the practical requirements. This paper combines the blockchain technology with federated learning technology, and uses decentralized blockchain system to replace the traditional centralized federated learning architecture. We adopt training method of updating models to achieve machine learning. In this way, we can avoid transmission of intermediate computing data and achieve mechanism of node access, model evaluation, motivation and audit with combination of block chain. In terms of the algorithm, the horizontal federated learning adopts the integrated learning algorithm, and the vertical federated learning adopts the deep learning algorithm. It will be described in detail below.

CCS CONCEPTS

• Information systems; **• Data management systems**; **• Information integration**; **• Data exchange**; **• Computing methodologies**; **• Machine learning**; **• Security and privacy**; **• Human and societal aspects of security and privacy**;

KEYWORDS

Federated learning, Blockchain, Machine learning, Neural network, Random forest

ACM Reference Format:
Shicheng Xu, Sihan Liu*, and Guangyu He. 2021. A Method of Federated Learning Based on Blockchain. In *The 5th International Conference on Computer Science and Application Engineering (CSAE 2021), October 19–21, 2021, Sanya, China.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3487075.3487143

1 INTRODUCTION

Federal study (Federated Learning) is the basis of a new artificial intelligence technology, first put forward by Google in 2016, which was originally used to solve the android mobile terminal users in the problem of local update model. The design goal is to protect the terminal data and personal data privacy in big data exchange of information security and carry out efficient machine Learning with multiple parties or multiple computing nodes under the premise of ensure legal compliance. The classic federated learning problem is based on a global model of data learning stored on tens to millions of remote client devices. During the training, the client device needs to communicate periodically with the central server. It leads to performance bottlenecks, untrusted data, privacy leaks and other issues. The existed federal learning research focuses on the algorithm direction, and the research about system architecture direction is not enough, so mentioned problems have not been completely solved. Nevertheless, federated learning of large-scale practices is an important means of facilitating data sharing and overcoming related problems. This paper is committed to solve the above three problems

With the development of artificial intelligence technology, data has become an increasingly important resource. However, in many industries, it needs to protect trade secrets and customer privacy prevents data from being shared effectively. IN financial industry, risk control and credit investigation are important methods of risk management. The traditional data analysis mode faces the problems that limited data collection scope, low enthusiasm for data uploading, untimely update and high access threshold. In medical industry, the sensitivity of the data making medical institutions, insurance, drug companies, medical equipment suppliers are difficult to realize low cost and efficient data exchange and medical information sharing, which leads to a large amount of data resources in the industry not been effective use and in-depth analysis. [1-4]

Therefore, many enterprises have insufficient data collection samples and data collection dimensions, and cannot share data due to sensitive data. In order to effectively utilize and analyze sensitive data, it is necessary to find a data training mode with the advantages of security compliance, no need to migrate classified data, and no disclosure of private information. The existing multi-party cooperative data training methods include joint modeling, secure multi-party computing, federated learning and so on. Among them, based on the basic information authorized by users, joint modeling can obtain the multidimensional data associated with users and comprehensively grasp the customer information, which may easily lead to excessive acquisition and improper use of user information. Secure multi-party computing technology is based on the principle of cryptography, homomorphic encryption and other methods to train data without data decryption, which has no advantage in performance and is not suitable for the situation of large data volume. In contrast, federal learning involves multiple participants with equal status, which contribute and share the results together. Moreover, the experimental results obtained by this distributed federated learning modeling approach are similar to those obtained by integrating multi-party data for centralized

CSAE 2021, October 19–21, 2021, Sanya, China

ACM ISBN 978-1-4503-8985-3/21/10…$15.00
https://doi.org/10.1145/3487075.3487143

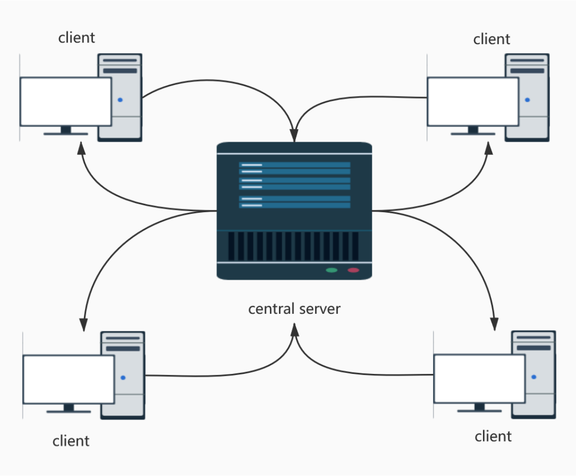


Figure 1: Classical Federated Learning Architectures.

modeling. It does not need expensive encryption hardware and has open source platform. The prospect of federated learning is most optimistic in these technologies.

The current mainstream of federal study framework is shown in figure 1

The central server is responsible for the maintenance model and global work force, a large number of participating in the framework of mobile devices are referred as the Client. The Client have equal status in the system and loose coupling, each Client stores the local data, these local data is not transmitted and exchanged in any form. Currently, federal learning technology has not been widely promoted and fully used, mainly because the following limitations have not been overcome [5-8]:

- Performance bottleneck. A classic federated learning framework with a central server at its core, has high hardware performance requirements and operational maintenance costs, and can lead to a single point of failure or become performance bottleneck. The frequent bidirectional communication between the central server and the client results is in high communication cost, and the repeated encryption and decryption operation also results in high operation cost.
- Information security issues. The information security of federated learning is based on the trust of the central server, which requires the security of the central server's computing environment and reasonable design of computing process. But the central server's computing environment and process are not transparent, which are the hidden trouble of information security.
- Data credibility problem. The existing federated learning framework is implemented by the central server for access identification, which only guarantees the trustworthiness of the participant identity but not the trustworthiness of the data. If an individual participant uses fake data to participate in the training, it may pry into the privacy of others or mislead the training model, which is difficult for other participants to detect and prevent. [9-10]

To solve the above problem, we need to combine other cutting-edge technology with the existing federal study framework for reform and breakthrough. At present, there are many explorations and practices in big data sharing and privacy protection of blockchain, such as "Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Gadekallu, T. R., Maddikunta, P. K. R., ... & Pathirana, P. N. (2020). A Survey on Blockchain for Big Data: Approaches, Opportunities, and Future Directions. arXiv preprint arXiv:2009.00858.", "Ch, R., Srivastava, G., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. Journal of Information Security and Applications, 55, 102670.", "Gadekallu, T. R., Kumar, N., Hakak, S., & Bhattacharya, S. (2020). Blockchain based Attack Detection on Machine Learning Algorithms for IoT based E-Health Applications. arXiv preprint arXiv:2011.01457.", "Bhardwaj, A., Shah, S. B. H., Shankar, A., Alazab, M., Kumar, M., & Gadekallu, T. R. (2020). Penetration testing framework for smart contract Blockchain. Peer-to-Peer Networking and Applications, 1-16.". This shows that blockchain technology combines with other technologies is feasible and advanced. In this paper, we take the blockchain combined with federal study ways to solve the above problems.

- The client participating in the calculation trains the local model according to their own local data, and the blockchain ledger maintains the central model. The client transmits the update of the local model encrypted to the central server to reduce the data transmission amount of model update. The training process between each node is independent, and the reading of the central model can be read from any node, so as to eliminate the single point of failure and data interaction bottleneck of the original architecture.
- The model update process is controlled by an intelligent contract. Only models are transformed during the update process, so there is no possibility of information leakage. The updating process of the model is disclosed, the updating condition is disclosed, and the updating process can be traced, which ensure information security.
- Combining the mature authentication technology of block chain technology for access identification ensures the credibility of the identity of participants. Model evaluation standard is set up jointly by the participants, the chain model is updated by the parties jointly control and prevented malicious or invalid update of participants to the center model, which ensure the credibility of data.

2 ARCHITECTURE DESIGN OF FEDERATED LEARNING SYSTEM BASED ON BLOCKCHAIN

The main defects of the existing federal learning come from the performance bottleneck, safety hidden trouble. And data is not credible since it's caused by the centralized architecture. Blockchain technology together with decentralized federal learning architecture can highly solve problems. Blockchain is a kind of decentralized trust database, it can use digital encryption and timestamp methods to implement point-to-point transaction without mutual trust. Its core idea is based on the decentralized characteristics of peer-to-peer

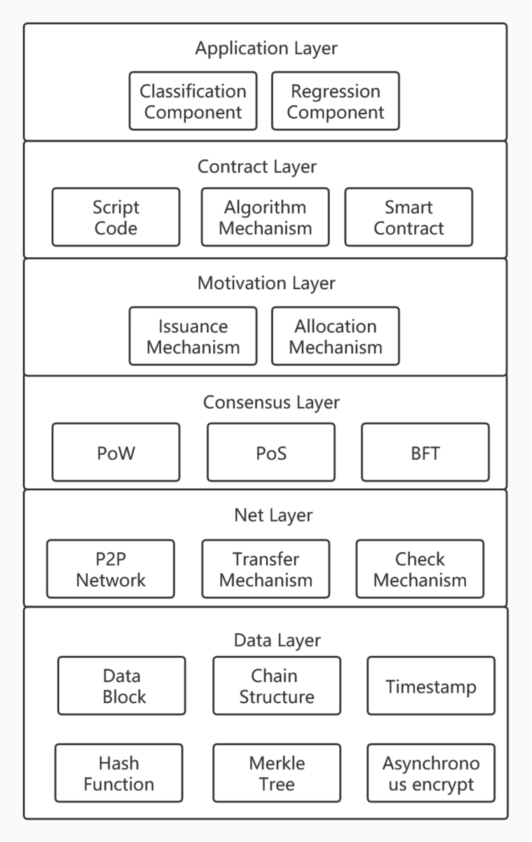


Figure 2: Architecture Design of Federated Learning System Based on Blockchain.

networks with reached consensus on each nodes and nodes collectively maintain data blocks. Each block on the data chain is checked by digital signature to prevent data tampering and forgery. This architecture can remove the dependency of the federated learning system of the central server, break the performance bottleneck and improve transparency of the computing process. [11-14]

In this paper, we adopt classic blockchain system architecture and blockchain system is divided into six levels: the data layer, the network layer, the consensus layer, the motivation layer, the contract layer and the application layer. The model of federated learning is stored in the data layer. The network layer, the consensus layer and the motivation layer support the operation of the system together. The contract layer is used to control the training and updating model, and the application layer can expand the functions of the system. [15]

The architecture design of federated learning system based on blockchain is shown in figure 2. The bottom layer of blockchain is the data layer, which mainly realizes data storage, accounts and safety transactions, the model of federated learning system is also stored in this layer. The data store is mainly based on the Merkle tree. The realization and security of accounts and transactions are based on various cryptographic algorithms and technologies. In data layer, it mainly includes data block, chain structure, timestamp, hash function, Merkle tree and asymmetric encryption. Data layer can ensure the credibility and availability of the model. The new blockchain supports the function of storing private data under the chain and storing hash on the chain, which is suitable for storing user data, and can guarantee the credibility and privacy and improve system performance. [16]

The network layer of blockchain is a distributed system based on TCP/IP communication protocol and peer-to-peer network. It does not rely on one centralized service node to transmit information, but all nodes participate in the information transmission, which can satisfy the communication requirements among nodes of the federated learning system. According to the data verification mechanism and special transmission protocol sated up by the network layer, each node in the blockchain system can participate checking and accounting. Only if most nodes in the whole network have been verified can data be stored in the blockchain. New blockchain typically has access to mechanisms that are more suitable for federated learning business scenarios.

The consensus layer mainly realizes the highly dispersed nodes in the whole network to reach consensus on transactions and data quickly, and prevents consensus attacks such as Byzantine attack and 51% attack. This algorithm is called consensus mechanism, which is one of the core technologies of blockchain. Nowadays, there are dozens of consensus mechanism algorithms such as Proof of Work, Proof of Stake, and BFT in blockchain technology. As an optional layer, the consensus layer can provide a secure operating environment for the federated learning platform when participating nodes are not trusted and prevented attacks by malicious nodes.

The main function of the motivation layer is to encourage each node in the network to conduct security verification of the blockchain and maintain the operation of blockchain system. By integrating economic factors into the blockchain technology system, the nodes that follow rules and participate will be encouraged to use , but the nodes that violate the rules will be punished. The motivation mechanism promotes the benign development of the blockchain system. The motivation layer is also an optional layer that provides rewards for participating nodes to attract as much as possible nodes to participate in federated learning.

Contract layer contains scripts, algorithms, and smart contracts, which are also simple to understand custom of the electronic contract. Smart contract can automatically execute when the constraints are completed. When it’s not in this case, it automatically cancels the contract and triggers all pre-set terms. This is also one of the core technologies that blockchain can liberate the credit system. Smart contracts can decide what models to train, what algorithms to use, and what hyper-parameters to set. The federated learning platform can truly accomplish democratized machine learning.

The blockchain application layer encapsulates verify application scenarios and cases, just like application on a computer operating system, a portal on an Internet browser, a search engine, an electronic mall, or an APP on a mobile phone. Based on the mature federated learning model training, the application layer of blockchain can further provide decentralized top-level services and expand functions of the federated learning platform. [17-20]

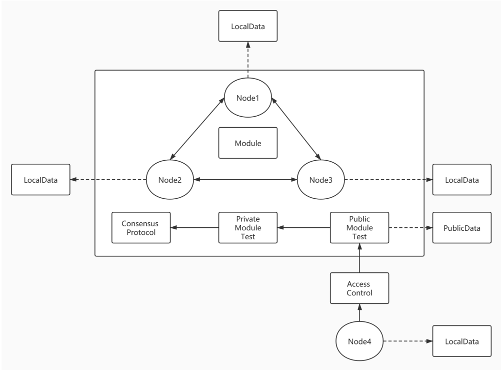


Figure 3: Federated Learning System Flow Diagrams.

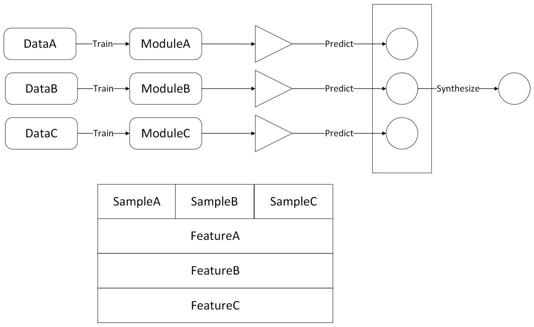


Figure 4: Horizontal Federated Learning Algorithm and Sample Schematic Diagram.

3 FUNCTIONAL DESIGN OF FEDERATED LEARNING SYSTEM BASED ON BLOCKCHAIN

In this section, the core function design of federated learning system is based on blockchain will be introduced, including model storage and evaluation, model training, motivation mechanism and audit mechanism

3.1 Model Storage and Evaluation

In order to give full usage on blockchain's excellent characteristics of decentralization, this paper adopts a model evaluation method and model updated strategy based on smart contract. The federated learning system is jointly maintained by multiple blockchain nodes. The blockchain model is kept on the blockchain ledger, and the personal data of each participant is kept offline to avoid disclosure. The training of the model adopts updated model, and updated model is controlled by smart contract. After updating the global model, the blockchain model can be distributed efficiently and the performance bottleneck of model distribution can be removed. Access conditions are set jointly by nodes that already participated in the federated learning system, and model testing and access control contracts are sated to prevent participants who wish to do evil.[21-22]

The sample process is as follows:

As shown in figure 3, node 1, node 2 and Node 3 are the existing nodes of the federated learning system, which jointly maintain the learning model in the blockchain ledger. The local data of node 1, node 2 and Node 3 are stored outside the blockchain. The model test, access control and consensus contract on the chain are implemented by smart contracts. When a foreign node 4 wants to join the federated learning system, it needs to pass the system access control first for prevent the foreign node maliciously probe the local data of the nodes in the learning system. Model updates should pass two phases of model testing that approved by consensus contracts. Taking node 4 as an example to invoke model update, public model test refers to a set of public test data to test the training effect of the model provided by node 4. In this way, some models with poor effect can be filtered out and the computing resources of the system can be saved. If node 4 passes the public model test, then the private data test phase will start. Although model test proved that the node 4 provide model is a normal model, but it is clear that the model has a high risk of overfitting, in order to ensure the node 4 provide model is really available, node 1, 2, 3 respectively using its local data to test the effect of the model provided by node 4 (including precision, recall ratio and precision ratio and recall ratio, etc.), this step is outside the chain, so as not to reveal the local data from node 1, 2, 3.Obviously node 4 just provides the model ,so the data from node 4 also won't be leaked. When the network income more nodes, the access control can be adjusted to a random n choose k mode. Consensus contract is formulated by the network existing members, and it can make user-defined setting of module update condition, such as precision rate or recall rate index (model under different business scenarios indicators tend to have very big difference) to decide whether should allow node 4 invoke once model update. This method can ensure that a block falls only if the model performance can be improved, and helps model updating in the right direction. The mode of deliver model is distributed. If a node needs to update the model to the latest state, it can get the latest module directly from the peer node rather than rely on a specific node.

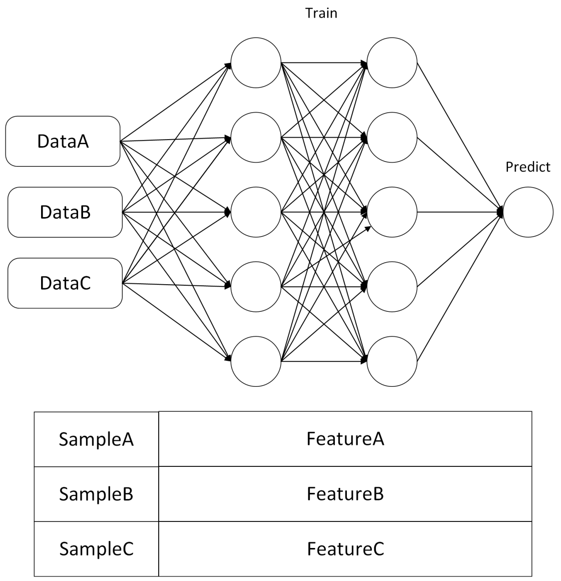
3.2 Model Training

In order to take advantage of blockchain such as consensus trust, non-tampering and decentralization, and overcome the shortcomings of centralized federated learning architecture, the performance and storage space of blockchain system should be fully considered, and we should pay attention to privacy protection. [23-24]

Therefore, this paper refers to the idea of zero-knowledge proof, adopts the model updating mode to carry out the out-of-chain training of the model, for reducing the expense of communication and storage space, and realizing the data security based on information theory. The federal learning system designed in this paper mainly supports two modes: horizontal federal learning and vertical federal learning. [25]

As shown in figure 4, horizontal Federated Learning, also known as Feature Aligned Federated Learning, is suitable for the situation where participants' data features overlap a lot and sample id overlap a bit. For example, customer data of two banks are in different regions.[26-28]

The horizontal federal learning model of this paper mainly adopts the integrated learning model, it will set weight of each



SampleA	FeatureA
SampleB	FeatureB
SampleC	FeatureC

Figure 5: Longitudinal Federated Learning Algorithm and Sample Schematic Diagram.

node with consensus protocol to provide learning machine (horizontal federal learning set the strong constraints for the participating characteristics, although it is invalid to improve the accuracy of model, model can provide a good explanatory, likes traditional machine learning ,this method even suffers the integration which can also keep explanatory).Training process can be summarized as following: First of all, each node trains model independently according to their own data, and then starts model update smart contract request. The other nodes (if there are many nodes we often adopt the random pick method) response for the smart contracts to validate the model. If the model performance increases, the nodes authorize the updating of the model. According to different business scenarios, horizontal federal learning can choose sequence integration learning methods such as AdaBoost, which utilizes the dependencies between basic learners to improve overall predictive effect. We can also choose the parallel integration learning method such as Random Forest that takes advantage of the independence between base learners to highly reduce errors by averaging.

As shown in figure 5, longitudinal federated learning, also known as sample-aligned Federated Learning, is suitable for training participants in cases where Sample ids overlap a lot and data characteristics overlap a little. For example, common customer data of Banks and e-commerce companies are in the same region.[29-30]

The longitudinal federal learning model of this paper mainly adopts the deep learning model, set up by consensus agreement of each node to provide update model regarding step length and updating parameters (have the effect of the drop out). Longitudinal federal learning extends the feature dimension, which makes it hard for the traditional machine learning model processing. At the same time, the complicated calculation relationship between different characteristics usually can't explain. Deep learning model can effectively block the characteristics of the differences between different models, and better performance Deep learning can preset higher dimensions, and set some dimensions of the corresponding input node to inactive temporarily. After waiting for the participants to provide the relevant data and be open to participate in the node, the global model can copy to the local and use their own data and network to update the global network, also get the other node model performance testing and global network of corresponding computing nodes after poor value of input , which is under the control of super parameter constraint consensus agreement to update global node.

3.3 Motivation Mechanism

Appropriate motivation mechanism can provide rewards for the participants' contribution, increase the enthusiasm of the participants, and update the initiator to maliciously to punish the federal learning business scenarios. Blockchain network has excellent POW and POS basis, model updating is obviously a good effective certificate. It can improve the performance of the model significantly and enhance from short to long time of small ascension process, this process also can meet the demand of POW proved effective . When a node brings ascends continuously for the model, it can clearly show that the nodes with better data and computing capacity should update with higher weight and step length and meet the needs of POS proved at the same time. To launch a network update, it should set a cost value to avoid invalid network launched by the node constantly updated and reduce the waste of computing power between the nodes.

3.4 Audit Mechanism

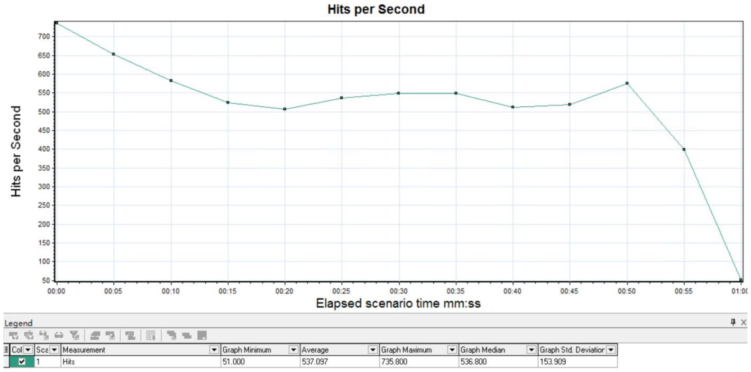
With Learning model in the training process, participants may encounter malicious submission model, model training or mislead training into local optimization model. So it requires federal learning system to have a good audit mechanism to locate the errors. Blockchain system's tamper-resistant features provide a good support for the audit mechanism. The history of model update is completely recorded in the blockchain according to the transaction order. The initiator of model update and the result of model update are also recorded in the blockchain. With data mining technology and data visualization technology, the time and node of problem occurrence can be accurately located and the audit of federated learning system can be effectively realized.

4 FUNCTIONAL DESIGN OF FEDERATED LEARNING SYSTEM BASED ON BLOCKCHAIN

In this section, an experimental design is carried out for the individual credit evaluation scenario to verify the rationality of the system design. The experimental content includes using random forest to build credit risk assessment model and comparing the effects of horizontal federated learning with different number of nodes participating. Neural network is used to build credit risk assessment model to compare the effects of longitudinal federated learning with different number of nodes participating.

Table 1: The Test Environment Hardware Configuration

CPU:	40*Intel E5-2623 V4 2.2GH virtual 32 core
Memory:	32 GB
Network Card	10 Gbps



Col	Sca	Measurement	Graph Minimum	Average	Graph Maximum	Graph Median	Graph Std. Deviatior
☑	1	Hits	51.000	537.097	735.800	536.800	153.909

Figure 6: The System Throughput Test Results

4.1 Establishment of Experimental Environment

Based on the Fabric 2.0 alliances chain system, we achieve test with different local data of peer node after taking the same algorithm for training and integrated performance comparison. The purpose is to investigate how to improve the ability of island phenomenon for the learning system based on block chain with deficiency of data samples and data dimension data.

The experimental environment is as Table 1

4.2 Data Set Selection and Preprocessing

This paper adopts the Lending Club data set for training. After removing the Current data in the repayment period, the remaining state is divided into two categories: default and non-default. The pretreatment operation includes feature normalization, outlier treatment, missing value treatment and so on. After the preliminary preprocessing, the correlation test method is adopted to remove some highly correlated variables and retain 100 eigenvectors and 65,000 pieces of data.

After preprocessing, 1/10 of the data is selected as the test data to test the training results by random sampling. The training set of the random forest is divided into 5 parts on average and distributed among 5 nodes, with independent training data among each node, so as to simulate the situation of insufficient data samples in financial institutions with the same category. The training set of neural network divides the training data set into 5 parts on average, and adopts the random null method. After reserving common fields such as funded_amnt of the current loan amount for each node training set, half of the other fields are randomly null, so as to simulate the situation that different financial institutions have different dimensional data.

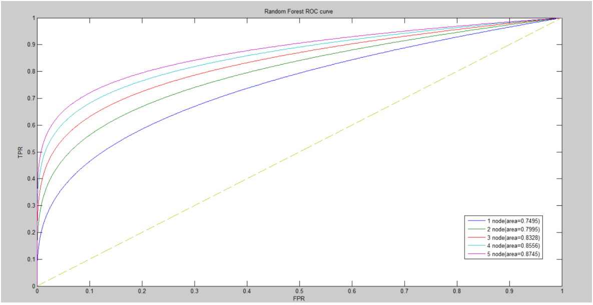


Figure 7: The ROC Curve and AUC Values of Random Forest Experiment.

4.3 Experimental Results

The experimental results will compare the effects of multi-node horizontal integration and multi-feature vertical integration of federated learning. The number of participating nodes is 1, 2, 3, 4 and 5. At the same time, the system carries out the model reading and writing experiment, including the random forest model of 100 dimensions and BP neural network model of 100 dimensions. The number of trees in random forest is 1000, and the number of node features of trees is 3. The neural network is a single hidden layer neural network, and the maximum number of iterations is 2000.

The system throughput test results are as Figure 6

The results of the random forest experiment are as Table 2

ROC curve and AUC values are as Figure 7

The results of neural network are as Table3:

ROC curve and AUC values are as follows in Figure 8

According to the experimental results of the above data, with the increase of participating integration nodes, indicators such as the accuracy rate of horizontal integration learning and vertical

Table 2: The Results of The Random Forest Experiment

Nodes number	Precision	Recall	Accuracy
1	0.73	0.73	0.72
2	0.76	0.75	0.74
3	0.79	0.80	0.81
4	0.84	0.85	0.83
5	0.88	0.86	0.85

Table 3: The Results of Neural Network

Nodes number	Precision	Recall	Accuracy
1	0.55	0.56	0.56
2	0.70	0.71	0.71
3	0.76	0.75	0.75
4	0.81	0.83	0.82
5	0.84	0.85	0.85

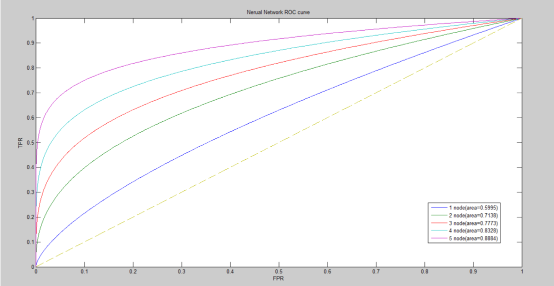


Figure 8: The ROC Curve and AUC Values of Neural Network Experiment.

integration learning have been significantly improved. In the case of 5 nodes, the model is fully integrated, and both horizontal and vertical integration learning achieve ideal results. When there are fewer nodes, the improvement of vertical integration learning is more obvious than that of horizontal integration learning, which indicates that insufficient data dimension is more likely to become the performance bottleneck of the model than insufficient data sample. In the process of updating the model, the system can always maintain high throughput and meet the performance requirements in the actual application process. The experimental results show that the federal learning system based on block chain can effectively improve the lack of data samples of the same institutions and the lack of data dimensions of different institutions, meet the requirements of data compliance in the process of cooperation between different institutions, and have high reading and writing performance, which can meet the application requirements.

In this experiment, the system is a distributed system with high throughput, and there is no single point of failure, and the performance bottleneck is overcome. The updating mode of the model is to update the model with the model, which eliminates the possibility of the central server illegally acquiring data and solves the problem of privacy protection. The model is stored on the block chain, which can't be tampered with. The traceability of the data ensures the authenticity of the data. Every participant in the model update process can directly query, and the training process is transparent. Therefore, this experiment proves that the federated learning system based on block chain is feasible and practical.

5 CONCLUSION AND PROSPECT

This paper proposes a federated learning method based on blockchain, federal learning system architecture. We design the method of model store and evaluation, training methods and motivation mechanism based on blockchain. We discuss the feasibility and superiority in blockchain combined with federal study. Federal learning can be carried out in a truly decentralized manner with the consideration of privacy protection. Through the combination of federal learning technology and blockchain technology, the three problems regarding performance bottleneck, data trustworthiness and privacy protection are solved. Both horizontal and vertical federal learning can be carried out effectively in a blockchain-based federal learning system. At the same time, through the analysis of the existing work, it is found that the performance gap between different blockchain networks is huge. To successfully deploy and run the federated learning system, it is necessary to carefully select, deploy and optimize the blockchain network. And the federated learning system is not suitable for lazy learning methods such as clustering, because this kind of method cannot update model with model. Federal learning can effectively break the data island, blockchain network can rebuild trust, the effective combination of the twins can diminish the trouble that the date lacks and share difficult for machine learning. If we want to truly apply the federated learning method based on blockchain to the production environment, further effective schemes need to be researched and practiced. The existing framework should be adjusted and expanded to improve its integrity and extensibility, and the top-level application based on federated learning model should be deeply developed.

REFERENCES

[1] Engineering - Concurrent Engineering; Study Results from Beijing University of Chemical Technology in the Area of Concurrent Engineering Reported (Detecting and Mitigating Poisoning Attacks In Federated Learning Using Generative Adversarial Networks) [J]. Information Technology Newsweekly, 2020.

[2] SHI Wenqi, SUN Yuxuan, HUANG Xiufeng, ZHOU Sheng, NIU Zhisheng (2020). Scheduling Policies for Federated Learning in Wireless Networks: An Overview. [J/OL]. ZTE Communications, 1-11. http://kns.cnki.net/kcms/detail/34.1294.TN.20200610.1010.004.html.

[3] Chen Yang, Sun Xiaoyan, Jin Yaochu (2019). Communication-Efficient Federated Deep Learning With Layerwise Asynchronous Model Update and Temporally Weighted Aggregation.[J]. IEEE transactions on neural networks and learning systems, vol. 31, no. 10, PP. 4229-4238, Oct. 2020, doi: 10.1109/TNNLS.2019.2953131.

[4] Zhu Hangyu, Jin Yaochu (2020). Multi-Objective Evolutionary Federated Learning.[J]. IEEE transactions on neural networks and learning systems, 31(4).

[5] Brisimi Theodora S, Chen Ruidi, ela Theofanie, Olshevsky Alex, Paschalidis Ioannis Ch, Shi Wei (2018). Federated learning of predictive models from federated Electronic Health Records. [J]. International journal of medical informatics, 112.

[6] Brisimi Theodora S,Chen Ruidi,Mela Theofanie,Olshevsky Alex,Paschalidis Ioannis Ch,Shi Wei. Federated learning of predictive models from federated Electronic Health Records.[J]. International journal of medical informatics,2018,112.

[7] Wu Qiong,He Kaiwen,Chen Xu. Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge based Framework.[J]. IEEE computer graphics and applications,2020.

[8] Theodora S. Brisimi,Ruidi Chen,Theofanie Mela,Alex Olshevsky,Ioannis Ch. Paschalidis,Wei Shi. Federated learning of predictive models from federated Electronic Health Records[J]. International Journal of Medical Informatics,2018,112.

[9] Yongfeng Qian,Long Hu,Jing Chen,Xin Guan,Mohammad Mehedi Hassan,Abdulhameed Alelaiwi. Privacy-aware service placement for mobile edge computing via federated learning[J]. Information Sciences,2019,505.

[10] Fang Chen,Guo Yuanbo,Wang Na,Ju Ankang. Highly efficient federated learning with strong privacy preservation in cloud computing[J]. Computers & Security,2020(prepublish).

[11] Bharat Bhushan,Aditya Khamparia,K. Martin Sagayam,Sudhir Kumar Sharma,Mohd Abdul Ahad,Narayan C. Debnath. Blockchain for smart cities: A review of architectures, integration trends and future research directions[J]. Sustainable Cities and Society,2020,61.

[12] Huanhuan Feng,Xiang Wang,Yanqing Duan,Jian Zhang,Xiaoshuan Zhang. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges[J]. Journal of Cleaner Production,2020,260.

[13] Technology - Blockchain Technology; Data from University of Turku Advance Knowledge in Blockchain Technology (A Critical Review of Concepts, Benefits, and Pitfalls of Blockchain Technology Using Concept Map)[J]. Journal of Engineering,2020.

[14] Paul J. Taylor,Tooska Dargahi,Ali Dehghantanha,Reza M. Parizi,Kim-Kwang Raymond Choo. A systematic literature review of blockchain cyber security[J]. Digital Communications and Networks,2020,6(2).

[15] Julie Frizzo-Barker,Peter A. Chow-White,Philippa R. Adams,Jennifer Mentanko,Dung Ha,Sandy Green. Blockchain as a disruptive technology for business: A systematic review[J]. International Journal of Information Management,2020,51.

[16] T. Benil,J. Jasper. Cloud based security on outsourcing using blockchain in E-health systems[J]. Computer Networks,2020,178.

[17] Expert Systems; Findings on Expert Systems Reported by Investigators at University of Malta (Detection of Illicit Accounts Over the Ethereum Blockchain)[J]. Journal of Engineering,2020.

[18] Susanne Köhler,Massimo Pizzol. Technology assessment of blockchain-based technologies in the food supply chain[J]. Journal of Cleaner Production,2020,269.

[19] Lin Liu,Wei-Tek Tsai,Md Zakirul Alam Bhuiyan,Dong Yang. Automatic blockchain whitepapers analysis via heterogeneous graph neural network[J]. Journal of Parallel and Distributed Computing,2020,145.

[20] Xuechao Yang,Xun Yi,Surya Nepal,Andrei Kelarev,Fengling Han. Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities[J]. Future Generation Computer Systems,2020,112.

[21] International Business Machines Corporation; Patent Application Titled "Distributed Learning Using Ensemble-Based Fusion" Published Online (USPTO 20200219014)[J]. Technology & Business Journal,2020.

[22] Henri Bal,Arindam Pal. Parallel and Distributed Machine Learning Algorithms for Scalable Big Data Analytics[J]. Future Generation Computer Systems,2020,108.

[23] Bey Romain,Goussault Romain,Grolleau François,Benchoufi Mehdi,Porcher Raphaël. Fold-stratified cross-validation for unbiased and privacy-preserving federated learning.[J]. Journal of the American Medical Informatics Association : JAMIA,2020.

[24] Pradip Kumar Sharma,Jong Hyuk Park,Kyungeun Cho. Blockchain and federated learning-based distributed computing defence framework for sustainable society[J]. Sustainable Cities and Society,2020,59.

[25] Machine Learning; New Machine Learning Research from Air Force Institute of Technology Outlined (Machine Learning Modeling of Horizontal Photovoltaics Using Weather and Location Data)[J]. Electronics Newsweekly,2020.

[26] Huang Li,Yin Yifeng,Fu Zeng,Zhang Shifa,Deng Hao,Liu Dianbo. LoAdaBoost: Loss-based AdaBoost federated machine learning with reduced computational complexity on IID and non-IID intensive care data.[J]. PloS one,2020,15(4).

[27] Chuan Li,Shaohui Zhang,Yi Qin,Edgar Estupinan. A systematic review of deep transfer learning for machinery fault diagnosis[J]. Neurocomputing,2020,407.

[28] Dicheng Chen,Zi Wang,Prof. Di Guo,Prof. Vladislav Orekhov,Prof. Xiaobo Qu. Review and Prospect: Deep Learning in Nuclear Magnetic Resonance Spectroscopy[J]. Chemistry – A European Journal,2020,26(46).

[29] Technology - Blockchain Technology; Reports from University Pendidikan Sultan Idris Advance Knowledge in Blockchain Technology (Blockchain Authentication of Network Applications: Taxonomy, Classification, Capabilities, Open Challenges, Motivations, Recommendations and Future ...)[J]. Journal of Engineering,2020.

[30] Information Technology - Cloud Computing; Reports from Xidian University Provide New Insights into Cloud Computing (A Collaborative Auditing Blockchain for Trustworthy Data Integrity In Cloud Storage System)[J]. Computers, Networks & Communications,2020.