Development Economics of China
2025, VOL. 9, NO. 6, 108-111
DOI: 10.47297/wspdecWSP2515-797320.20250906

Design of Financial Anti-fraud Application System Driven by Blockchain and Federated Learning

Yizhuo Quan, Chenlu Hu

School of Information Engineering, Xi'an Mingde Institute of Technology, Xi'an, Shaanxi, 7101244, China

ABSTRACT
With the rapid development of financial technology, financial fraud methods are constantly evolving and upgrading, bringing severe challenges to the security and stability of the financial industry. Traditional anti-fraud methods are difficult to meet the current needs of financial risk prevention and control due to problems such as data silos and privacy protection. To this end, this paper proposes and designs a financial anti-fraud application system architecture that integrates blockchain and federated learning technology. Through federated learning, the system realizes joint modeling of multiple institutions without sharing original data, thereby improving the accuracy and robustness of fraud detection models; at the same time, combined with the tamper-proof and traceable characteristics of blockchain, it ensures the transparency and credibility of model training and parameter interaction processes, further enhancing the security and compliance of the system. This paper analyzes the functional architecture and key technical implementation of the system in detail, including model construction, privacy protection mechanism, smart contract design, etc., designs specific interaction processes, and conducts prototype development and experimental verification. The experimental results show that the proposed system can effectively improve the accuracy and real-time response capabilities of financial fraud detection while ensuring data privacy and security. This study provides new ideas and practical references for the development of financial anti-fraud technology under the background of multi-institutional collaboration.

KEYWORDS
Financial anti-fraud; Blockchain; Federated learning; Privacy protection; Smart contract

1 Introduction

With the development of financial technology, financial transactions are highly digitalized and intelligent, and financial fraud methods are showing trends such as technology and gang-based, which seriously threaten financial security and user interests. Traditional anti-fraud methods rely on centralized data analysis, which is limited by data silos, privacy protection and real-time performance [1]. It is difficult to meet current needs and urgently needs a new technical architecture for transformation.

At this stage, financial anti-fraud faces challenges such as difficulty in sharing data across institutions, increased pressure on privacy protection, and continuous evolution of fraud methods. How to improve multi-party collaboration and risk identification capabilities while ensuring privacy and compliance is a core issue of concern to the industry.

Blockchain and federated learning have significant advantages in privacy protection and trusted collaboration. Blockchain provides decentralized, tamper-proof and traceable data protection, and federated learning realizes joint modeling of data without leaving the domain. The integration of the two can effectively solve the problems of data silos and trust, and build a safe and efficient anti-fraud collaboration mechanism [2].

This paper designs a financial anti-fraud system based on blockchain and federated learning, focusing on data privacy protection, trusted collaboration and risk warning, clarifying the functions and interaction mechanisms of each module, building a prototype and verifying the accuracy and security of the system, providing a new path and theoretical support for multi-institutional collaborative anti-fraud.

2 Overview of related technologies

Financial anti-fraud technology has become an important means to ensure financial security. Traditional methods rely on centralized data analysis, but face problems such as data silos, privacy leakage and low collaboration efficiency. In recent years, as financial fraud methods have become increasingly complex, it is urgent to integrate emerging technologies to build an efficient, reliable and privacy-friendly anti-fraud system [3].

Blockchain has significant advantages in financial anti-fraud due to its decentralization, immutability and traceability. It can realize cross-institutional data sharing and reliable evidence storage, ensure data integrity and transaction security, and improve anti-fraud collaboration efficiency and transparency through smart contracts.

Federated learning uses distributed modeling to achieve local training of multi-party data and share model parameters, taking into account privacy protection and model effects, solving compliance issues of data not leaving the domain, improving the anti-fraud capabilities of multi-institution collaboration, and strengthening model generalization and detection accuracy [4].

The integration of blockchain and federated learning provides an innovative architecture for financial anti-fraud: blockchain ensures the reliability of model updates and data interactions, and federated learning achieves privacy protection and efficient modeling. The two complement and cooperate to meet the security and compliance needs of financial data.

Domestic and foreign research is actively exploring this field. Internationally, anti-fraud platforms based on blockchain and federated learning have been applied to multinational banks, and domestic related research has also achieved phased results, especially in smart contracts and consensus mechanisms. In summary, this fusion technology is becoming an important development direction for future financial anti-fraud.

3 System overall architecture design

The design of this system is centered on solving the problems of data islands, multi-party collaboration and privacy protection in financial anti-fraud. The goal is to achieve cross-institutional collaborative modeling and accurate fraud identification, and ensure data security and model effectiveness [5]. The design follows the four principles of "security and trustworthiness, privacy protection, efficient collaboration, and scalability" to ensure that the system has good practical application value.

The overall architecture of the system consists of six modules: data access, federated modeling, blockchain evidence storage and smart contracts, model update evaluation, fraud identification and visualization. The data access module is responsible for local data collection and preprocessing, the federated modeling module realizes local training and parameter sharing, and the blockchain module records model versions and collaboration logs to ensure that the process is transparent and traceable [6]. The fraud identification module provides real-time warnings based on the latest model, and the visualization module provides intuitive monitoring and traceability analysis for risk control personnel.

The system adopts a dual-core architecture of "federated learning + blockchain coordination". Each financial institution node participates in distributed modeling and performs parameter chaining and verification through the alliance chain, and the smart contract automatically controls model aggregation and version management [7]. The central coordinator only aggregates parameters and does not touch the original data to ensure privacy and security. The blockchain provides tamper-proof records and consensus mechanisms to enhance the trust foundation of multi-institutional collaboration.

The interaction between each module revolves around the federated learning cycle: the local node submits encryption parameters after training, the coordinator aggregates and uploads them to the chain after verification by the smart contract, and each node is updated synchronously to enter a new round of training. The blockchain records the update information throughout the process to ensure audit and traceability. When suspicious transactions occur, the system quickly identifies and warns based on the latest model to improve real-time response capabilities.

4 Implementation of key technologies

The core of this system is to deeply integrate federated learning with blockchain to ensure data security and trusted collaboration in financial anti-fraud tasks. The federated learning part adopts the graph neural network and deep forest fusion strategy [8]. Each financial institution conducts training based on local real transaction data and only uploads encrypted model parameters to avoid data leakage, while retaining data diversity and scenario integrity, and improving model robustness and generalization capabilities.

In order to solve the trust problem in multi-party collaboration, the system introduces a consortium chain architecture, and all nodes participate in consensus to ensure that the entire process of model update is recorded on the chain. The parameter updates and model version information of each round of training are hashed to ensure that the data is traceable and cannot be tampered with, eliminate "black box operations", and improve the transparency and trust of cross-institutional collaboration.

In terms of privacy protection, the system integrates differential privacy, homomorphic encryption, and secure multi-party computing technologies to encrypt and perturb model parameters to prevent sensitive information leakage. The communication layer uses TLS/SSL protocol combined with blockchain key management and access control to build an end-to-end secure training environment to fully protect data risks during transmission and aggregation.

To improve training efficiency, the system introduces asynchronous update and parameter compression mechanisms, supports asynchronous upload of nodes based on their own computing power, and only synchronizes model differences to reduce communication costs. At the same time, the model structure is dynamically adjusted in combination with the complexity of financial business to achieve a balance between real-time and accuracy. Smart contracts are responsible for core process control, automatically completing operations such as node registration, parameter aggregation, and model version management, and have built-in anomaly detection logic to improve system autonomy and operational transparency.

5 System application scenarios and process analysis

The "financial anti-fraud system driven by blockchain and federated learning" has shown good adaptability and practical value in scenarios such as bank credit, mobile payment and multi-institutional joint modeling. By building a cross-institutional, efficient and collaborative anti-fraud mechanism, it has significantly improved the accuracy and response speed of fraud detection.

In bank credit, fraudulent behaviors such as identity forgery, multiple loans and other cross-institutional risks are difficult to identify. Through federated learning, the system enables multiple banks to jointly model under the premise of ensuring data privacy. The blockchain records the parameter update process to ensure that the modeling is transparent and controllable. When users frequently apply for credit from different banks, the system can achieve rapid warning based on the global model, thereby effectively curbing cross-fraud behavior.

In mobile payment scenarios, fraud methods are diverse and behaviors change rapidly. The system is deployed locally in the payment institution, assesses risks based on real-time transaction data, trains recognition models through a federated mechanism, and the blockchain ensures that the training path and verification information cannot be tampered with. The design realizes real-time identification and automatic interception in high-concurrency scenarios, significantly reducing the incidence of fraud incidents.

In multi-institutional joint modeling scenarios, such as collaborative modeling by banks, insurance companies, and risk control platforms, the system uses federated learning to integrate data of different dimensions to build a risk model with a wider coverage. As a trust center, blockchain records the model parameters and update process of all parties to prevent data falsification. Smart contracts automatically control model version switching and training rounds to improve modeling efficiency and trust foundation.

The system operation process is centered on the federated modeling cycle, and coordinates node interactions through blockchain smart contracts. Risk control personnel can monitor model performance, receive warnings and enter feedback through a visual interface. After each round of training, the system automatically distributes new models and supports local real-time detection; users can also trace the training process and institutional collaboration to build a complete human-machine collaborative risk control closed loop.

6 System Implementation and Deployment Test

In order to verify the practical feasibility and operational performance of the "Financial Anti-Fraud Application System Driven by Blockchain and Federated Learning", this paper conducts prototype implementation and deployment tests on the system. The entire system is developed with a modular and distributed architecture. The backend is based on Python as the main language, and the TensorFlow Federated (TFF) framework is integrated for the training and coordination of the federated model. The blockchain part is based on Hyperledger Fabric to build a consortium chain network, and the smart contract is written in Go language. The front end uses the Vue.js framework and cooperates with ECharts for data visualization. The system is deployed on multiple simulated node servers with an operating system of Ubuntu 20.04. The federated nodes simulate the multi-institutional data isolation environment through the intranet to ensure that the simulation environment is close to the real distributed financial scenario.

The system implementation includes multiple core modules: federated learning module, blockchain evidence module, smart contract module, fraud detection module, and visualization interface module. The federated learning module integrates a variety of model structures, including logistic regression, random forest, and lightweight neural network, to meet the requirements of different scenarios for accuracy and speed. The blockchain module implements the on-chain recording and verification mechanism of model parameters, and is linked with the aggregation scheduling in the federated learning process. Smart contracts implement logic such as parameter upload permission verification, aggregation trigger mechanism, and model version management, ensuring the compliance and integrity of model training. The fraud detection module is deployed in the local transaction system, receives the federated model, and scores and judges transactions in real time. The visualization module provides functions such as real-time model training status monitoring, performance evaluation report display, and fraud warning record query, which facilitates the operation and management of risk control personnel.

The experimental data is selected from public financial fraud data sets, including Credit Card Fraud Detection and IEEE-CIS Fraud Detection data sets. In order to simulate real distributed scenarios, the data is divided into multiple virtual institution nodes to ensure that each node has a different data set with some overlapping features. In each round of experiments, the system performs 5 to 10 rounds of iterative training on the federated model, each of which includes a complete process such as local model update, parameter encryption transmission, blockchain verification and evidence storage, aggregator update, and model synchronization. By comparing the detection results of centralized modeling and federated modeling, the convergence speed and detection capability of the model are evaluated.

In terms of performance evaluation, the system focuses on model accuracy, training and inference latency, security, and cross-node collaboration efficiency. Experimental results show that under the premise of protecting privacy, the federated model trained by the system has only a 1.3% difference in AUC indicators compared with the centralized training model, and can still effectively identify most abnormal transaction behaviors. The average delay of a single round of training is within 2.5 seconds, which meets the response speed requirements of financial services. After optimization through asynchronous communication and parameter compression mechanisms, the communication overhead between nodes is reduced by about 35%. In terms of security, the encryption and chain-up mechanism of model parameters effectively blocks data tampering and forgery under simulated attacks, and the system shows strong robustness and stability in multiple test scenarios.

7 Summary and Outlook

Through this study, we proposed and designed a financial anti-fraud application system based on blockchain and federated learning technology. The system solves the problems of data privacy and data islands among multiple financial institutions through federated learning, allowing all parties to jointly build an efficient fraud detection model without sharing sensitive data. At the same time, the system introduces blockchain technology to ensure the transparency, immutability and traceability of model parameter updates, greatly enhancing the trust basis for cross-institutional collaboration. Through application in a variety of financial scenarios, experimental results show that this system can effectively improve the anti-fraud capabilities of financial institutions, and has high accuracy, low latency and strong security in performance, which meets the financial industry's requirements for real-time, privacy protection and system scalability.

Although the system has achieved good results in the experiment, there are still some shortcomings. First, although the system can perform distributed modeling through federated learning, the efficiency of model training and aggregation still needs to be improved when facing extremely large-scale data, especially when the number of participants is large, the training and synchronization process may be delayed. Secondly, although blockchain technology effectively enhances the security and credibility of data, the current blockchain network still faces throughput limitations, which may affect the processing speed of real-time transactions. The execution mechanism of smart contracts is also complex. The vulnerabilities and execution costs of smart contracts may become technical bottlenecks when the system is further promoted.

Future research and optimization directions are mainly reflected in the following aspects: First, how to further improve the training efficiency of the federated learning model in a large-scale distributed environment will be the key to improving the overall performance of the system. The communication overhead can be reduced and the aggregation speed can be increased by introducing more efficient model compression algorithms, optimizing data transmission and encryption methods. Secondly, with the participation of more institutions, how to effectively manage the scalability of the blockchain network and how to improve its throughput in high-concurrency transaction scenarios will be an important direction for the further development of the system. The optimization of smart contracts is also a focus of future work. By enhancing the security and execution efficiency of smart contracts, the operating cost of the system can be reduced and the maintainability and upgradeability of the system can be improved.

In future research, more diverse application scenarios can be explored, such as combining AI technology for abnormal behavior prediction, optimizing the detection accuracy of fraud based on deep learning methods, or exploring how to deeply integrate cross-industry anti-fraud systems to build a broader data sharing and collaboration network. With the continuous development of financial technology and blockchain technology, the financial anti-fraud application system combining blockchain and federated learning will be able to be further improved and popularized, promoting the financial industry to make more significant progress in anti-fraud and risk prevention and control.

References

[1] Santoso B. (2024). Predictive Traffic Regulation Methodologies Using 5G-Enhanced Sensor Fusion Across Vehicle and Drone Platforms. International Journal of Applied Machine Learning, 4(12), 1-15.

[2] Chaabane F. (2025). Multi-source Data Fusion to Enhance Wireless Communication Beyond 5G for Smart City Transformation. In Internet of Vehicles and Computer Vision Solutions for Smart City Transformations (pp. 451-473). Cham: Springer Nature Switzerland.

[3] Pratama A., Kusuma R., & Setiawan B. Enhancing Smart Grid and Autonomous Systems through 5G Networks and Multi-Source Data Integration. Eigenpub Review of Science and Technology, 8, 133-150.

[4] Han S., Wang M., Duan J., Zhang J., & Li D. (2024). Research on Unmanned Aerial Vehicle Emergency Support System and Optimization Method Based on Gaussian Global Seagull Algorithm. Drones (2504-446X), 8(12).

[5] Trinh M. L., Nguyen D. T., Dinh L. Q., Nguyen M. D., Setiadi D. R. I. M., & Nguyen M. T. (2025). Unmanned Aerial Vehicles (UAV) Networking Algorithms: Communication, Control, and AI-Based Approaches. Algorithms, 18(5), 244.

[6] Xu H., Wang L., Han W., Yang Y., Li J., Lu Y., & Li J. (2023). A survey on UAV applications in smart city management: Challenges, advances, and opportunities. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 16, 8982-9010.

[7] Sun H., Xu R., Luo J., & Cheng H. (2025). Review of the Application of UAV Edge Computing in Fire Rescue. Sensors, 25(11), 3304.

[8] Fu Y., Li C., Yu F. R., Luan T. H., & Zhang Y. (2021). A survey of driving safety with sensing, vehicular communications, and artificial intelligence-based collision avoidance. IEEE transactions on intelligent transportation systems, 23(7), 6142-6163.