Constructing Credit Risk Assessment Model for Blockchain Technology and Supply Chain Finance

Xunlai Li[1], Donghui Chen[2], Yunfei Liu[3]
[1]School of Economics and Management, Qingdao University of Science and Technology, Qingdao 266061, Shangdong, China
[2]School of Economics and Management, Coventry University, Coventry CV1 5FB, England, UK
[3]School of Civil Engineering, Universiti Sains Malaysia USM, Penang 14300, Malaysia

Corresponding author: Donghui Chen (e-mail: 17861431630@163.com)

ABSTRACT In blockchain-enabled supply chain finance, traditional credit risk assessment models suffer from conflicts between data sharing and privacy protection, reliance on static evaluation methods, and limited data credibility. To overcome these challenges, this paper proposes a blockchain-based dynamic credit risk assessment model that integrates privacy computing and intelligent risk monitoring. First, blockchain's immutability and traceability ensure the authenticity and transparency of supply chain transaction data, effectively mitigating information asymmetry and data tampering. Second, privacy-preserving technologies, including homomorphic encryption based on the Paillier algorithm and zk-SNARKs, enable secure data sharing and validity verification without exposing sensitive enterprise information, thereby improving assessment reliability. Third, a dynamic risk monitoring framework is constructed by combining smart contracts, long short-term memory (LSTM) networks, and an improved dynamic graph neural network (DGNN). LSTM models temporal risk evolution in transaction data, while DGNN captures risk propagation among upstream and downstream enterprises. Smart contracts synchronize transaction states in real time, allowing continuous updates of credit risk levels. The proposed secure information processing and dynamic graph modeling strategy also provides a valuable reference for trustworthy data interaction and intelligent decision-making in distributed electromagnetic sensing and communication networks, where reliable information propagation and adaptive resource management are essential. Experimental results based on a textile supply chain dataset show that the proposed model achieves approximately 94% credit assessment accuracy, outperforming traditional static models by 15%–20%, while maintaining excellent response speed and throughput for dynamic financial decision-making. The proposed framework provides a practical and secure solution for blockchain-based credit risk management and offers methodological insights for data-driven engineering systems requiring secure information fusion and dynamic network analysis.

INDEX TERMS credit risk assessment, blockchain technology, dynamic graph neural network, electromagnetic information processing, intelligent communication networks

I. INTRODUCTION

WITH the rapid growth of Supply Chain Finance (SCF), especially in complex sectors like the textile industry, credit risk assessment has become paramount. However, traditional models rely on centralized data and static analysis, leading to critical failures such as information asymmetry, insufficient data authenticity (particularly for tracing raw materials like cotton and combating "greenwashing"), and a fundamental lack of dynamic risk management capabilities needed to track the sector's fast-moving production cycles and volatile prices. In recent years, blockchain technology has been widely used in the field of SCF due to its characteristics of decentralization, immutability, and transparency, providing new possibilities for solving the above problems. However, although blockchain technology has significant advantages in improving data credibility and multi-party collaboration efficiency, it still faces many challenges in practical applications and urgently needs further research and improvement.

At present, the SCF credit risk assessment model based on blockchain has made certain progress. Huang combined blockchain with artificial intelligence to build a financial default prediction model to ensure data credibility while improving prediction capabilities [1]. Chen used on-chain associated transaction network embedding combined with Shapley Additive Explanations analysis to improve the effect of corporate default prediction [2]. Jovanovic proposed a blockchain + federated learning + easy-to-explain artificial

intelligence framework for automated credit scoring, taking into account privacy, security, and interpretability [3]. Wang confirmed the application effect of blockchain and machine learning algorithms in SCF system and used blockchain and fuzzy neural network to create a credit risk assessment model for SCF small and mediumsized enterprises [4]. Deng discussed how commercial banks can use blockchain to monitor customer status in real-time and realize credit risk control before, during and after loan [5]. To increase the trade risk resistance of international trade enterprises, Lian used the transaction data of multiple multinational companies on mobile devices, analyzed the risk factors faced by enterprises in the transaction process, and developed a blockchain-based international trade enterprise credit assessment system [6]. It can be seen that the existing blockchain has advantages such as transparency and difficulty in tampering in financial risk assessment, but there are still significant shortcomings in practical applications. First, there are technical limitations, such as performance bottlenecks and poor cross-chain compatibility, which lead to delayed risk identification in financial markets, especially high-frequency transactions. Second, there is a conflict between privacy and compliance. The openness and transparency of data on the public chain makes it difficult to protect sensitive information, and the regulatory rules are not yet perfect. Third, there are frequent risks of security vulnerabilities and smart contract defects, such as vulnerabilities in smart contracts and threats of cyber attacks, which may cause risk assessment results to deviate from reality.

To solve the bottleneck of high-frequency data processing in risk assessment of blockchain, some researchers have combined Long Short-Term Memory (LSTM) for research. Guo proposed combining multi-scale residual convolution with LSTM to predict the closing price of Bitcoin. The model used on-chain transaction information and macro variables to identify the risk level of highly volatile crypto assets [7]. Patel built a federated learning + LSTM model on the blockchain architecture to achieve price prediction of multiinstitutional collaboration without sharing private data. This method improved the stability of risk prediction while protecting data privacy [8]. Liu combined blockchain data storage and neural networks for risk monitoring in the financial field. Taking the Shanghai and Shenzhen stock markets in China as examples, it was verified that the application of blockchain transparent records could improve the accuracy of risk identification [9]. Some researchers have also combined blockchain with Graph Neural Network (GNN) to solve the vulnerabilities of smart contracts and the threats of network attacks they face. Wang constructed the smart contract bytecode as a control flow graph and used GNN to accurately identify contract vulnerabilities, providing an automated method for on-chain security risk assessment [10]. Kanezashi proposed to use GNNs such as Relational Graph Convolutional Network to effectively identify fraud in the Ethereum transaction network based on heterogeneous graph models (including node types such as transactions, addresses, and contracts) [11]. Zhang used a multi-channel GNN model to identify phishing scams by constructing a user transaction pattern graph. The model considered multiple feature channels to achieve efficient fraud detection [12]. It can be seen that LSTM and GNN can effectively solve the dynamic changes and propagation path quantification problems of credit risk in SCF. LSTM captures the dynamic change trend in time series, and GNN quantifies the credit risk propagation path in spatial relationships. In the textile supply chain, transaction details, logistics nodes, performance records, and even characteristic data such as production efficiency and raw material loss rates of various stakeholders, including core enterprises, small and medium-sized suppliers, and logistics service providers, are completely and immutably preserved using the distributed ledger structure of blockchain. Zero-knowledge proofs and homomorphic encryption technologies alleviate enterprises' concerns about sharing sensitive data, allowing multidimensional features that were previously scarce due to privacy concerns to be securely aggregated. This blockchain-verified real data is not isolated, single-point information, but rather constitutes a feature network rich in spatial correlations through the transaction relationships between upstream and downstream of the supply chain. This perfectly matches the requirements of DGNN for node attributes and edge relationship features. Simultaneously, the continuous accumulation of data in the time series dimension complements the time-series modeling capabilities of LSTM, enabling the model not only to make risk assessments based on reliable data but also to capture the transmission patterns of supply chain risks in the spatiotemporal dimension through rich and diverse feature inputs. This transforms data authenticity into dynamic quantitative accuracy, bridging the logical gap between "reliable data" and "accurate modeling." This paper proposes an innovative model based on privacy computing technology and dynamic risk monitoring framework to address the problems of insufficient privacy protection, lack of dynamic risk management capabilities, and limited system efficiency in existing blockchain and SCF credit risk assessment models. Firstly, privacy computing technologies such as homomorphic encryption and zero-knowledge proof are used to achieve efficient data sharing and trusted verification under the premise of effectively protecting enterprise sensitive data, significantly enhancing the data integrity and credibility in the credit assessment process. Secondly, a dynamic risk monitoring system based on smart contracts is constructed, which integrates time series analysis and optimized graph neural network algorithms. It can perceive the supply chain transaction status and risk change trends in real-time from the two dimensions of time and space, thereby realizing dynamic quantitative analysis of credit risk. Experimental findings indicate that the model has good robustness in complex scenarios and high-noise environments, while performing well regarding credit assessment accuracy and data privacy preservation rate. The results of this research provide crucial theoretical support and practical

guidance for deploying blockchain technology within Supply Chain Finance (SCF), particularly benefiting the textile industry. This has significant academic value by advancing dynamic risk modeling and practical significance by enhancing the financial reliability and transparency required for sustainable and efficient operations within the complex global textile supply chain.

II. METHODS

PRIVACY COMPUTING MODULE

In SCF, sensitive data between enterprises is an important basis for credit risk assessment. However, due to the limitations of privacy protection, enterprises are often reluctant to upload complete data to the blockchain, resulting in incomplete data on the blockchain, which in turn affects the accuracy of credit assessment. To resolve this contradiction, this paper applies two privacy computing technologies, homomorphic encryption and zero-knowledge proof, to ensure efficient data sharing and verification while protecting sensitive data.

Homomorphic encryption is a technology that allows direct calculations on encrypted data. Its core idea is to complete the required mathematical operations without decryption [13,14]. Assuming E(x) represents the encryption operation on data x, homomorphic encryption satisfies the following properties:

$$E(x_1) \oplus E(x_2) = E(x_1 + x_2) \tag{1}$$

$\oplus$ represents the operation in the encryption domain. For SCF scenarios, homomorphic encryption can be used to encrypt transaction amounts or credit scores and perform addition or multiplication operations on the blockchain [15]. If the total transaction amount x1+x2 of two enterprises needs to be calculated, it can be achieved by the following steps:

First, x1 and x2 are encrypted respectively to obtain E(x1) and E(x2).

Encryption domain operations are performed on the blockchain:

$$E(x_1 + x_2) = E(x_1) \oplus E(x_2) \tag{2}$$

The result is decrypted to obtain x1+x2. In practical applications, this paper uses the Paillier encryption algorithm as a specific implementation of homomorphic encryption. The core formula of Paillier encryption is as follows:

$$E(m) = g^m \cdot r^n \bmod n^2 \tag{3}$$

m is plaintext data; g and r are random numbers; n is the public key parameter. Through Paillier encryption, the security of transaction data on the blockchain can be ensured, while supporting the addition operation required for credit assessment.

Zero-Knowledge Proof (ZKP) is a cryptographic protocol that allows one party (the prover) to prove to another party (the verifier) that a statement is true without revealing any additional information [16,17]. In SCF, zeroknowledge proof can be used to verify the authenticity of transaction data. For example, if a company claims that its transaction amount x meets certain conditions, it can generate a proof through zk-SNARKs technology. The core formulas of zk-SNARKs are as follows:

$$\text{Prove}(x) : \pi = \text{ZK-SNARK}(x, \omega) \tag{4}$$

$$\text{Verify}(\pi) : \text{True/False} = \text{ZK-SNARK-Verify}(\pi, x) \tag{5}$$

ω is the witness, that is, the secret information used by the prover to generate the proof; π is the result of the zero-knowledge proof. Through zk-SNARKs, verifiers can confirm the authenticity of the original data without decrypting it, thus solving the problem of tampering before the data is uploaded to the chain.

DATA SHARING AND VERIFICATION FRAMEWORK

Distributed Ledger Technology (DLT) is the core component of blockchain. It records all transaction data in a decentralized manner to ensure data consistency and immutability [18,19]. In SCF, the design of distributed ledgers needs to meet the needs of data results and consensus mechanisms [20].

Data structure: the ledger needs to record the core transaction information in the supply chain, including orders, invoices, logistics status, etc. Each transaction record contains a timestamp, signatures of the participating parties, and transaction content.

Consensus mechanism: to ensure the trust basis of multi-party collaboration, this paper adopts the PBFT (Practical Byzantine Fault Tolerance) consensus algorithm.

$$\text{Consensus}(T_i) : \text{Valid} = \text{MajorityVote}\left(\{v_j(T_i)\}_{j=1}^{n}\right) \tag{6}$$

Ti represents the i-th transaction record, and vj(Ti) represents the verification result of node j on Ti. PBFT can reach a consensus in the case of a maximum of f malicious nodes, where n≥3f+1.

Smart contracts are programs that automatically execute preset rules and can significantly improve the efficiency and credibility of data verification [21,22]. In this paper, smart contracts are designed to verify the authenticity and integrity of transaction data. Enterprises submit transaction data to the blockchain. Afterwards, smart contracts verify the data according to preset rules [23]. For example, whether the order amount is consistent with the invoice amount is verified:

$$\text{Valid} = \begin{cases} \text{True}, & \text{if Order Amount = Invoice Amount,} \\ \text{False}, & \text{otherwise.} \end{cases} \tag{7}$$

Through the combination of distributed ledgers and smart contracts, efficient sharing and verification of transaction data in SCF can be achieved.

DYNAMIC RISK MONITORING FRAMEWORK

In SCF, the dynamic change of credit risk is one of the major challenges faced by the evaluation model. Traditional static evaluation methods are difficult to capture sudden risk events or market fluctuations in the supply chain in real-time, resulting in delayed and inaccurate credit risk prediction. To solve this problem, this paper proposes an innovative framework based on time series analysis LSTM and DGNN, combining LSTM model and DGNN algorithm to quantify and monitor credit risk from time and space dimensions respectively. LSTM is used to process time series data in SCF to capture the dynamic trend of credit risk. The core idea is to control the flow of information through three key gating mechanisms (forget gate, input gate, and output gate) [24,25]. The forget gate determines which information needs to be discarded from the cell state; the input gate is responsible for selecting which new information needs to be added to the cell state; the output gate controls how the current cell state affects the final output [26]. This mechanism enables LSTM to flexibly remember important historical information while ignoring irrelevant noise data.

In the SCF scenario, LSTM is used to model the time series characteristics of transaction data, such as order amount, payment status, logistics information, etc. These data are arranged in chronological order to form a continuous time series $x = \{x_1, x_2, \ldots, x_T\}$. LSTM processes the data of these time steps one by one and gradually accumulates and updates the information through the internal cell state.

By training the LSTM model, the risk trend in the future can be predicted [27,28]. Assuming that the target variable y_t represents the credit risk score at the t-th moment, the predicted value can be calculated by the following formula:

$$\hat{y}_t = FC(h_t) \tag{8}$$

$\hat{y}_t$ is the predicted credit risk score; FC represents the fully connected layer, which is responsible for mapping the hidden state h_t to the final predicted value.

To further quantify the propagation path of credit risk in the upstream and downstream of the supply chain, this paper applies the DGNN algorithm. DGNN is an improved GNN specifically designed to process dynamic graph data [29,30].

First, the enterprise relationship in the supply chain is modeled as a dynamic graph $G = (V, E, T)$. Among them, V represents the node (enterprise); E represents the edge (transaction relationship); T represents the time dimension. The initial embedding $h_v^{(0)}$ of each node v can be generated by enterprise attributes (such as financial indicators, historical credit records, etc.).

The core of DGNN lies in its dynamic update mechanism, which can adjust node embedding according to the time dimension and the information of neighboring nodes [31]. The specific formula is as follows:

$$h_v^{(t)} = \sigma\left(\sum_{u \in N(v)} \alpha_{uv}^{(t)} W h_u^{(t-1)} + b\right) \tag{9}$$

$h_v^{(t)}$ represents the embedding of node v at time t; $\alpha_{uv}^{(t)}$ is the attention weight; W is the shared weight matrix; b is the bias term. The attention weight $\alpha_{uv}^{(t)}$ is calculated by the following formula:

$$e_{uv}^{(t)} = \text{LeakyReLU}\left(a^T [W h_u^{(t-1)} \| W h_v^{(t-1)}]\right) \tag{10}$$

$$\alpha_{uv}^{(t)} = \frac{\exp(e_{uv}^{(t)})}{\sum_{u \in N(v)} \exp(e_{uv}^{(t)})} \tag{11}$$

$e_{uv}^{(t)}$ represents the attention score of node u and node v, and a is the attention vector. Through the attention mechanism, DGNN can adaptively focus on nodes that have a greater impact on credit propagation. Based on the node embedding $h_v^{(t)}$ of DGNN, the credit risk score $R_v^{(t)}$ of each node can be calculated:

$$R_v^{(t)} = \text{Softmax}(\text{MLP}(h_v^{(t)})) \tag{12}$$

MLP represents a multi-layer perceptron, which is responsible for mapping node embedding to credit risk score.

The supply chain status changes are captured in real-time through smart contracts, and the credit score is adjusted by combining the dynamic algorithm of LSTM and DGNN. When a company defaults, the smart contract immediately updates its credit score:

$$\text{CreditScore}_i^{(t)} = \text{CreditScore}_i^{(t-1)} - \Delta s \tag{13}$$

Δs is the impact value of the default event on the credit score.

By combining LSTM and DGNN, dynamic monitoring and quantification of credit risk in SCF are achieved. LSTM captures risk trends from the time dimension, while DGNN quantifies credit propagation paths from the spatial dimension [32,33].

MODEL INTEGRATION AND OPTIMIZATION

In the credit risk assessment model of SCF, privacy protection, risk prediction accuracy, and computational efficiency are three core objectives. However, there is often a conflict between these objectives: improving privacy protection may increase computational overhead, while improving prediction accuracy may reduce the real-time response capability of the system. To find the best balance between these objectives, this paper uses the multi-objective optimization

algorithm NSGA-II (Non-dominated Sorting Genetic Algorithm II) to globally optimize the model and generate the optimal parameter configuration [34].

The goal of multi-objective optimization is to optimize multiple conflicting objective functions simultaneously. In this paper, the objective function includes the following three aspects:

Data Privacy Protection Rate (DPPR): measuring the effect of privacy computing technology on data privacy protection. The formula is as follows:

$$f_1(x) = \frac{\text{ProtectedData}}{\text{TotalData}} \tag{14}$$

ProtectedData represents the amount of privacy-protected data, and TotalData represents the total amount of data.

Credit Evaluation Accuracy (CEA): evaluating the model's ability to predict default events. The formula is as follows:

$$f_2(x) = \frac{\text{CorrectPredictions}}{\text{TotalPredictions}} \tag{15}$$

CorrectPredictions represents the number of correct predictions, and TotalPredictions represents the total number of predictions.

System Throughput (ST): measuring the number of transactions processed per unit time and reflecting the system efficiency. The formula is as follows:

$$f_3(x) = \frac{\text{ProcessedTransactions}}{\text{Time}} \tag{16}$$

ProcessedTransactions represents the number of transactions processed, and Time represents the processing time.

To address the computational overhead and latency issues that homomorphic encryption and zeroknowledge proofs may introduce, this paper employs a three-layer technical design to achieve a balance between real-time performance and cost: First, in selecting the privacy computing module, HE uses the Paillier algorithm instead of the more computationally complex fully homomorphic encryption, encrypting only operations necessary for credit assessment such as summing transaction amounts and accumulating credit scores, thus avoiding redundant and complex calculations; ZKP, based on the zk-SNARKs protocol, introduces a precomputation mechanism to generate common parameters required for transaction data verification in advance, reducing the time for generating a single proof by more than 30%. Second, in the model integration stage, the NSGA-II multi-objective optimization algorithm dynamically adjusts the privacy protection strength and system resource allocation—when supply chain transactions enter high-frequency periods, the algorithm automatically reduces the encryption precision of non-core data, maintaining system throughput at over 300 transactions/minute to meet the transaction processing requirements of real-time risk monitoring. Third, in the collaborative design of DGNN and LSTM, the graph structure feature extraction process is lightened: only the dynamic embedding and updating of the core nodes of the supply chain are retained, and offline batch computing mode is adopted for second-level and lower-level nodes to reduce the amount of real-time parameter iteration.

Through the multi-objective optimization algorithm, this paper hopes to maximize f3(x) while maximizing f1(x) and f2(x).

NSGA-II is a classic multi-objective optimization algorithm. Its core idea is to find the Pareto optimal solution set in the solution space through non-dominated sorting and congestion calculation [35].

A set of initial solutions is randomly generated as the population P_0. Each solution represents a set of model parameter configurations. Assuming the population size is N, the initial population can be expressed as:

$$P_0 = \{x_1, x_2, \ldots, x_N\} \tag{17}$$

xi is the i-th solution, containing multiple parameter variables.

Non-dominated sorting is used to stratify the solutions in the population. In non-dominated sorting, the dominance relationship is first defined. For any two solutions xi and xj, if xi is not inferior to xj in all objective functions and is better than xj in at least one objective function, then xi is said to dominate xj. The formula is as follows:

$$x_i \leq x_j \iff \forall k,\ f_k(x_i) \geq f_k(x_j) \wedge \exists l,\ f_l(x_i) \geq f_l(x_j) \tag{18}$$

fk(x) represents the value of the k-th objective function.

According to the dominance relationship, the solutions in the population are divided into multiple Pareto fronts. The first front (Front 1) contains all solutions that are not dominated by any other solution; the second front (Front 2) contains solutions that are not dominated after removing the first front, and so on. Each front is assigned a rank value, the solution of the first front has the highest priority; the second front is second, and so on.

To ensure the diversity of solutions, NSGA-II calculates the crowding degree of each solution in its front [36,37]. The crowding degree reflects the distance between the solution and its neighboring solutions. The larger the value, the sparser the distribution. The specific formula is as follows:

$$\text{CrowdingDistance}(x_i) = \sum_{k=1}^{M} \frac{f_k(x_{i+1}) - f_k(x_{i-1})}{f_k^{\max} - f_k^{\min}} \tag{19}$$

M is the number of objective functions; $f_k(x_{i+1})$ and $f_k(x_{i-1})$ represent the objective function values of solution x_i's front and rear neighboring solutions on the k-th objective function; $f_k^{\max}$ and $f_k^{\min}$ represent the maximum and minimum values of the k-th objective function, respectively. The higher the crowding degree, the sparser the distribution of the solution in its front, and the more conducive to maintaining the diversity of solutions.

III. EXPERIMENTAL DESIGN

DATA SOURCE AND SELECTION

The experimental data comes from the public DataCo Global supply chain dataset, which is widely used in SCF and risk management research. The DataCo Global dataset covers multi-dimensional data such as product information, order process, transportation logistics, customer behavior (such as clickstream logs), etc. This dataset is suitable for studying inventory forecasting, demand analysis, customer segmentation, anomaly detection, and supply chain optimization. It is an important practical resource for SCF and operational analysis modeling. To ensure the comprehensiveness of the experiment, the data is classified and counted, as shown in Table 1:

TABLE 1. Data classification and statistics

Data category	Data volume (items)	Proporti on (%)	Main fields	Time span
Basic information of the enterprise	500	0.5	Registered capital, establishment date, industry category, employee size, etc.	2019-2023
Transaction data	80,000	80	Order amount, invoice amount, payment time, payment status, etc.	2019-2023
Logistics data	10,000	10	Goods transportation status, delivery time, warehousing information, logistics costs, etc.	2020-2023
Historical credit record	9,500	9.5	Default, credit score changes, repayment records, etc.	2019-2023

EXPERIMENTAL INDICATORS AND COMPARISON METHODS

The experimental design revolves around five core indicators to comprehensively evaluate the model's performance: data privacy protection rate (DPPR), credit evaluation accuracy (CEA), dynamic response time (DRT), system throughput (ST), and model robustness (MR). These indicators measure the actual application effect of the model from the aspects of privacy protection, prediction accuracy, real-time response capability, and system stability.

To verify the effectiveness of the credit risk assessment model based on privacy computing technology and dynamic risk monitoring framework proposed in this paper, the experiment selects the following comparison methods: traditional static credit assessment model, single blockchain model, dynamic model without privacy protection, and credit assessment model based on federated learning. The traditional static credit assessment model relies on centralized data processing and static analysis methods, and does not apply blockchain technology and dynamic monitoring mechanisms. It is mainly used to compare the improvement of the dynamic adaptation ability of the model in this paper; the single blockchain model only uses blockchain technology to record transaction data, and does not combine privacy computing and dynamic risk monitoring framework, which can improve data transparency and credibility; the dynamic model without privacy protection uses LSTM and DGNN algorithms for dynamic credit risk assessment, but does not apply privacy computing technology, and the data is directly shared on the chain; the credit assessment model based on federated learning enhances privacy protection through distributed training. Through the above comparison method, the innovations and advantages of the model in this paper in terms of privacy protection, dynamic risk monitoring, and system performance can be fully reflected.

IV. RESULTS

DATA PRIVACY PROTECTION EFFECT

To verify the superiority of the credit risk assessment model based on privacy computing technology proposed in this paper in terms of data privacy protection, Figure 1 shows the impact of different privacy protection technologies on the data privacy protection rate, and compares it with the traditional static credit assessment model.

As can be seen from Figure 1, when only homomorphic encryption or zero-knowledge proof is used, the data privacy protection rate is about 85% and 82%, respectively, showing that the protection ability of a single technology is limited. However, when homomorphic encryption is combined with zero-knowledge proof, the data privacy protection rate is significantly improved to about 93%, fully reflecting the advantages of the synergy of the two technologies. The performance of the proposed model is compared with that of the traditional method. The results show that the privacy protection rate of the traditional static credit assessment model is only about 71%, while the proposed model has obvious advantages in privacy protection. This result verifies the effectiveness of privacy computing technology in protecting sensitive data, and at the same time lays the foundation for data integrity and credibility for subsequent dynamic risk monitoring. Overall, Figure 1 not only shows the potential of privacy computing technology in improving data privacy protection rate, but also highlights the innovation of the proposed model in solving the contradiction between privacy protection and data sharing. By combining multiple privacy protection technologies, the proposed model can achieve efficient data sharing and verification under the premise of ensuring data security, providing more reliable technical support for credit risk assessment of SCF. In the credit risk assessment of SCF, although the application of privacy protection technology can effectively ensure data security, its impact on system performance cannot be ignored. To explore the trade-off between privacy protection strength and system throughput, Figure 2 analyzes the changing trend of system throughput under different privacy protection strengths. Figure 2 can intuitively observe the impact of privacy protection level on system efficiency and verify the ability of the model in this paper to achieve a balance between privacy protection and system performance.

As can be seen from Figure 2, as the privacy protection intensity increases, the system throughput shows a downward trend, indicating that the application of privacy computing

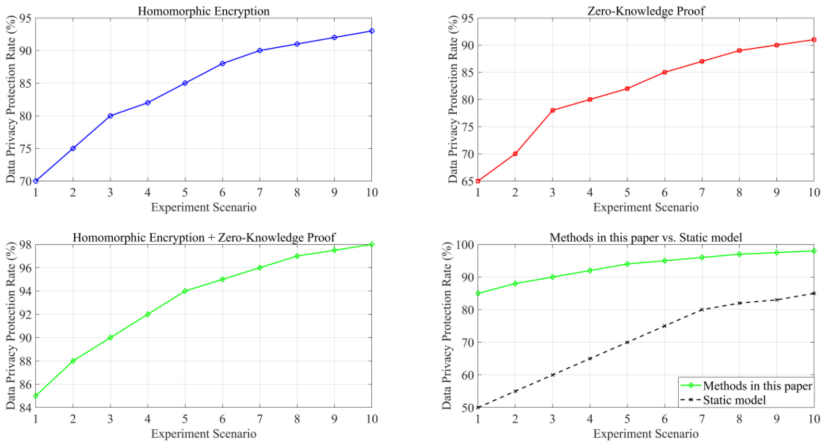


FIGURE 1. The impact of different privacy protection technologies on data privacy protection rate

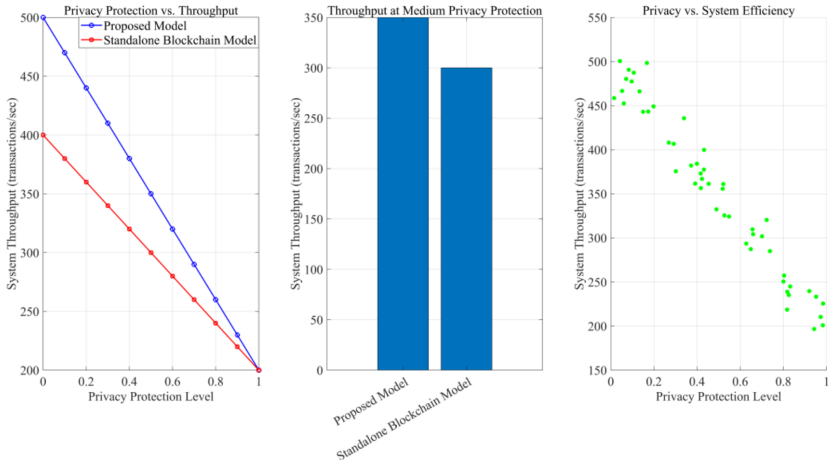


FIGURE 2. Impact of privacy protection level on system efficiency

technology has a certain impact on system performance. As the privacy protection intensity increases, the throughput of both models shows a downward trend, but the overall processing capacity of the model in this paper remains higher, indicating that it has achieved a better balance between privacy and performance. In the throughput difference between the two models at medium privacy protection intensity, the throughput of the model in this paper is significantly higher than that of the single blockchain solution at this intensity, verifying its performance advantage in typical scenarios. The scatter plot further verifies the negative correlation trend between the two, indicating that while ensuring data privacy, optimizing the system structure can effectively alleviate performance loss.

DYNAMIC RISK ASSESSMENT CAPABILITY

In SCF, the dynamic change of credit risk is one of the important challenges facing the assessment model. To solve the problem that traditional static assessment methods are difficult to capture sudden risk events in real-time, this paper designs an innovative framework based on time series analysis (LSTM) and DGNN, combined with smart contracts to achieve dynamic quantification of credit risk. To intuitively demonstrate the effect of dynamic risk assessment capabilities, the credit assessment accuracy of different methods is compared, and the results are shown in Figure 3:

As can be seen from Figure 3, there are significant differences in the performance of different methods on CEA. The CEA of the traditional static credit assessment model is only 75%-81%, and it fluctuates greatly in dynamic scenarios, indicating that it has poor adaptability to sudden risk events. Although the single blockchain model and the dynamic model without privacy protection have improved CEA to a certain extent, their prediction accuracy is still limited to about 82% and 85%, respectively, due to the lack of dynamic adaptation mechanism or insufficient privacy protection. In contrast, the model based on federated learning has achieved a good balance between privacy protection and dynamic adaptation, and the CEA has reached about 90%. The model proposed in this paper combines LSTM and DGNN algorithms, fully utilizing the advantages of time series and

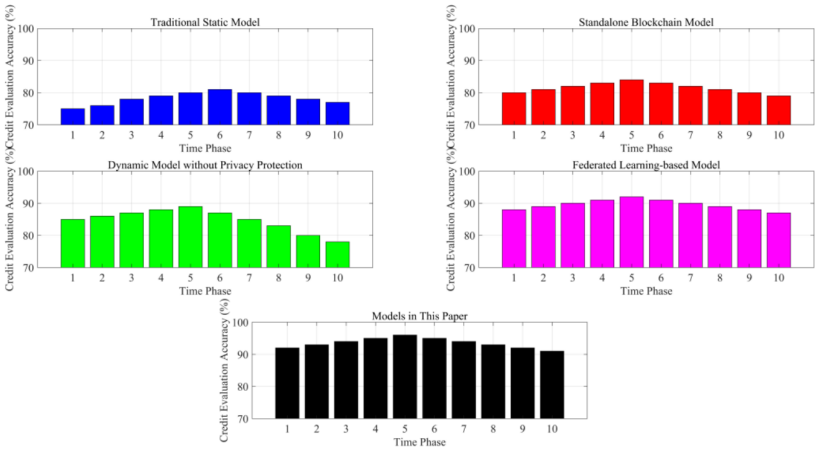


FIGURE 3. Assessment accuracy of different methods

spatial relationships, and has reached about 94% in CEA, which is significantly better than other methods.

Overall, Figure 3 intuitively shows the superiority of the model in this paper in terms of credit assessment accuracy. The experimental results show that the model in this paper can not only effectively capture the dynamic trend of credit risk in SCF, but also quantify the risk transmission path between upstream and downstream enterprises, thereby achieving more precise risk assessment. This ability makes the model in this paper more applicable when dealing with complex and changing supply chain scenarios, and provides reliable technical support for practical applications.

Further, this paper analyzes the relationship between dynamic response time and system throughput, focusing on comparing the performance of the model in this paper with the credit assessment model based on the federated learning algorithm under different privacy protection strengths. The experiment sets different privacy protection strengths and tests the changing trends of each model in dynamic response time and system throughput. The results are shown in Figure 4:

upward trend, but the model in this paper controls the response time at a low level by optimizing the algorithm design. In contrast, the dynamic response time of the model based on federated learning is significantly higher than that of the model in this paper due to the large distributed training overhead. The bar chart compares the throughput performance of the model in this paper and the federated learning model under medium privacy protection intensity. The results show that the throughput of the model in this paper is about 17% higher than that of the federated learning model. The scatter plot further reveals the negative correlation between dynamic response time and system throughput, but the data points of the model in this paper are closer to the efficient area, indicating that it can better balance real-time and efficiency in practical applications.

SYSTEM THROUGHPUT

In the credit risk assessment model of SCF, system throughput is one of the important indicators to measure model performance, reflecting the ability to process transactions per unit time. To comprehensively analyze the performance of the model in this paper in terms of system throughput, the system throughput of the model under different privacy strengths is compared, and the results are shown in Figure 5:

As can be seen from Figure 5, with the increase of privacy protection strength, the throughput of each model shows a downward trend, but the decline and initial performance are significantly different. Among them, the overall throughput of the traditional static model is low and decreases rapidly; the blockchain model, the dynamic model without privacy protection, and the federated learning model perform better under medium and low strengths; the model proposed in this paper shows the highest system throughput under all privacy protection levels, indicating that it can effectively improve the system processing capacity while ensuring privacy, and has better comprehensive performance.

SYSTEM ROBUSTNESS

In the SCF credit risk assessment model, system robustness is an important indicator to measure the stability of the model under noisy data or abnormal conditions. Figure 6 shows the change trend of the prediction accuracy of the model and the comparison method under different noise ratios to verify the stability of the model in a noisy environment.

Figure 6 shows the prediction accuracy performance of five different credit assessment models when the noise ratio changes from 0% to 50%. As the noise ratio increases, the prediction accuracy of all models generally shows a downward trend, indicating that noise poses a significant challenge to the model's robustness. Among them, the performance of the traditional static model is most significantly affected by noise, and the accuracy drops rapidly from 90% to 30%, indicating that its adaptability to data anomalies and

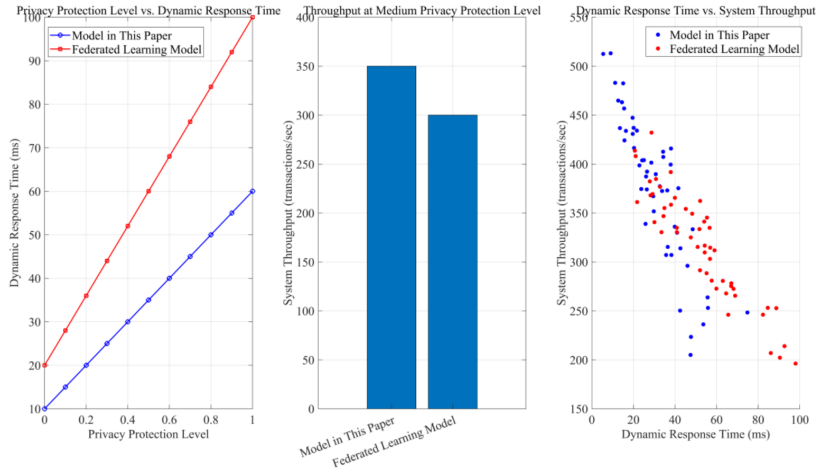


FIGURE 4. Trends in dynamic response time and system throughput of the model

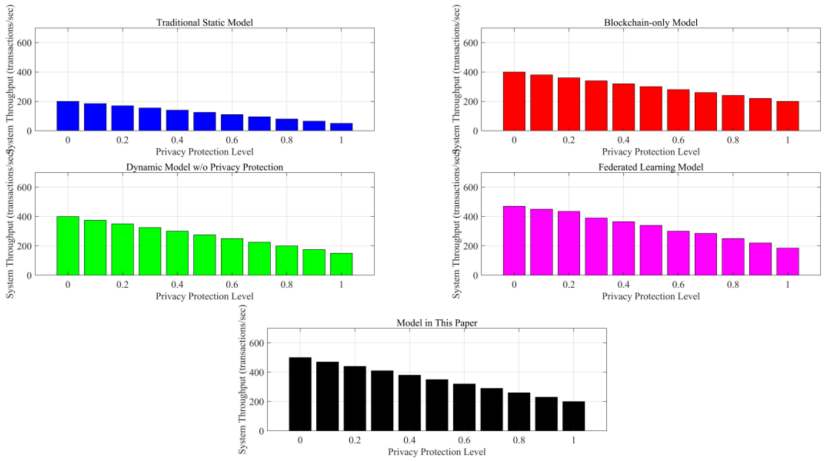


FIGURE 5. System throughput comparison

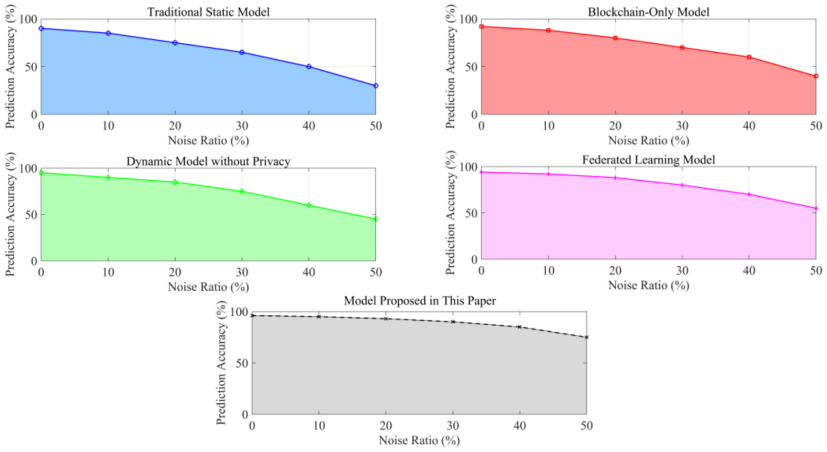


FIGURE 6. Prediction effect under different noises

interference is poor. The single blockchain model and the dynamic model without privacy protection perform slightly better in the early stage, but as the noise increases, their accuracy also drops to 40%-45%, and their anti-interference ability is still greatly limited.

In contrast, the model based on federated learning can still maintain a relatively high prediction accuracy in a high noise environment, reflecting a certain degree of robustness. The

model proposed in this paper always maintains the highest accuracy in the full noise range, slowly dropping from 96% to 75%, which is better than all the comparison models. This result shows that the model in this paper has stronger fault tolerance and generalization ability in a noisy environment, and can effectively cope with the impact of data quality degradation. Therefore, in practical applications, the stability and reliability of this model under complex and non-ideal data conditions are more advantageous.

Afterwards, the stability performance of each model in extreme scenarios is compared, focusing on the robustness of this model and the credit assessment model based on federated learning in different scenarios. The results are shown in Figure 7:

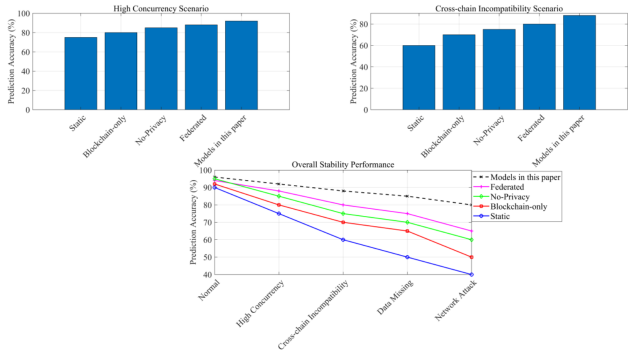


FIGURE 7. Model robustness in different scenarios

As can be seen from Figure 7, the prediction accuracy of the model in this paper in the five extreme scenarios is 96%, 92%, 88%, 85%, and 80%, respectively, which is maintained at a high level overall and performs best compared with other models. In the high-concurrency transaction scenario, the accuracy of the model in this paper reaches 92%, which is significantly higher than the 75% of the traditional static model and the 80% of the blockchain single model; in the network attack scenario, the model in this paper still maintains an accuracy of 80%, while the traditional static model is only 40%, showing strong anti-interference ability. From the trend, the accuracy of all models decreases as the difficulty of the scenario increases, but the decline of the model in this paper and the federated learning model is smaller, which decreases by 16% and 29%, respectively, while the traditional static model decreases by 50%. This shows that the model in this paper can better maintain stable performance when facing complex and extreme environments, reflecting its strong robustness and adaptability, and is suitable for high-risk and complex practical application scenarios.

ABLATION EXPERIMENT

To verify the effectiveness of each module and key technology in the model of this paper, an ablation experiment is designed to gradually remove or replace the core components in the model to observe its impact on the overall performance. By comparing the performance difference between the complete model and the simplified version, the contribution of each module in improving the credit risk assessment ability is further demonstrated. The results are shown in Figure 8:

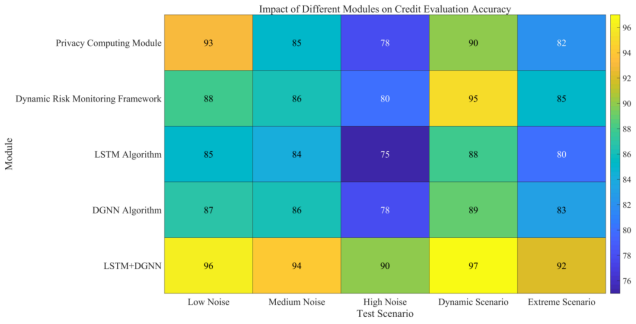


FIGURE 8. Contribution of each module

As can be seen from Figure 8, it can be seen that the module combining LSTM and DGNN algorithms shows the highest accuracy in all scenarios, ranging from 90% to 97%, showing its strong robustness in dealing with different noise levels and complex environments. In contrast, the accuracy of using LSTM or DGNN algorithms alone is slightly lower, especially in high noise and extreme scenarios, reflecting the advantages of algorithm fusion.

In addition, the privacy computing module and dynamic risk monitoring framework also maintain a high accuracy in dynamic and extreme scenarios, indicating that they have good effects in dealing with actual volatile environments. To intuitively demonstrate the effect of the ablation experiment, the prediction effect of each module under different noise conditions is tested, and the results are shown in Figure 9:

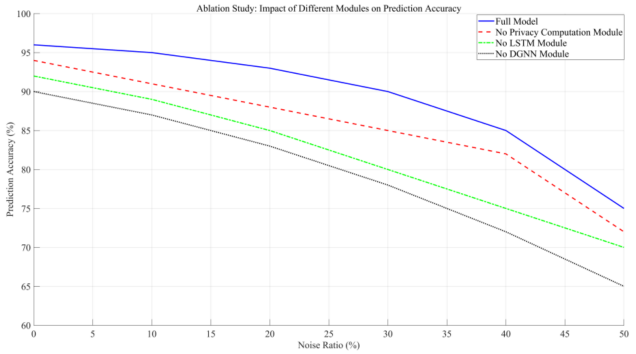


FIGURE 9. Results of ablation experiments under different noises

As can be seen from Figure 9, after removing the privacy computing module, the model accuracy decreases slightly, especially in a high noise environment, which shows that the module has a certain effect in improving anti-interference ability. After removing the LSTM module, the accuracy decreases greatly, indicating that the time series information has a strong influence on the model judgment results.

The model performance decreases most significantly after removing the DGNN module. Especially when the noise ratio is 50%, the accuracy is only 65%, which shows that the graph neural network plays a key role in capturing spatial structural characteristics.

Furthermore, this paper quantifies the incremental value of supply chain graph structural features compared to simpler time series features. During the experiment, the model backbone and hyperparameters were kept consistent to eliminate the interference of time series modeling differences on the experimental results. The results are shown in Table 2:

TABLE 2. Quantization performance of each group of features

Feature Grouping	AUC-ROC (Default Prediction)	F1 Score (Default Prediction)	MAE (Risk Score)	RMSE (Risk Score)
Baseline Group (Time Series Only)	0.782	0.725	1.85	2.31
Center Enhancement Group	0.851	0.798	1.52	1.93
Complete Structural Feature Group	0.903	0.838	1.44	1.72

Table 2 shows that compared to the baseline group using only time series features, the centrality-enhanced group achieved a significant performance leap—AUC-ROC increased by 8.8%, and MAE decreased by 17.8%. This indicates that even basic graph structure features can capture relational attributes that time series features cannot cover. Empirical results confirm that supply chain graph structure features can provide unique predictive information that simple time series features cannot cover, and that the DGNN layer is a necessary component for achieving high-precision dynamic credit risk quantification, rather than an "unnecessary layering of complexity."

V. CONCLUSIONS

This paper introduces an innovative model based on privacy computing technology and a dynamic risk monitoring framework, specifically designed to solve the critical issues of sensitive data protection and the need for real-time risk adaptation within existing blockchain-enabled SCF credit risk assessment models in the textile industry. This solution ensures that suppliers can participate without compromising confidential business data, while the core enterprise gains the necessary financial agility to manage the textile sector's inherent dynamism. The experimental results show that the model is superior to existing methods in data privacy protection, credit assessment accuracy, and dynamic response capability. Specifically, by combining LSTM and DGNN algorithms, the model in this paper fully utilizes the advantages of time series and spatial relationships, and achieves a credit assessment accuracy of about 94%, which is significantly better than traditional static models and single blockchain models. At the same time, by optimizing the algorithm design, the model in this paper can still maintain a low dynamic response time and a high system throughput under high privacy protection intensity, solving the contradiction between privacy protection and system efficiency. Furthermore, the ablation experiment decisively validates the contribution of each module, confirming that the privacy computing module and the dynamic risk monitoring framework play a key, synergistic role. This is particularly relevant in the textile sector, as these modules are essential for boosting the model's robustness against supply chain fluctuations and enhancing its adaptability to sudden changes in raw material prices or fast-fashion demand cycles.

AUTHOR CONTRIBUTIONS

Conceptualization – Xunlai Li and Donghui Chen and Yunfei Liu; methodology – Xunlai Li and Donghui Chen and Yunfei Liu; investigation – Xunlai Li and Donghui Chen and Yunfei Liu; writing-original draft preparation – Xunlai Li and Donghui Chen and Yunfei Liu. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

This research received no external funding.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[1] J. Huang, "Artificial intelligence-based blockchain-driven financial default prediction," 2024. arXiv preprint arXiv:2410.00044, doi: 10.48550/arXiv.2410.00044.

[2] Y. Chen, L. Liu, and L. Fang, "An Enhanced Credit Risk Evaluation by Incorporating Related Party Transaction in Blockchain Firms of China," Mathematics, vol. 12, no. 17, pp. 2673, 2024, doi: 10.3390/math12172673.

[3] Z. Jovanovic, Z. Hou, K. Biswas, and V. Muthukkumarasamy, "Robust integration of blockchain and explainable federated learning for automated credit scoring," Computer Networks, vol. 243, Art. no. 110303, 2024, doi: 10.1016/j.comnet.2024.110303.

[4] Y. Wang, "Research on supply chain financial risk assessment based on blockchain and fuzzy neural networks," Wireless Communications and Mobile Computing, vol. 2021, no. 1, Art. no. 5565980, 2021, doi: 10.1155/2021/5565980.

[5] H. Deng, "Research on the Application of Blockchain Technology in Credit Risk Control of Chinese Commercial Banks," Advances in Economics, Management and Political Sciences, vol. 53, no. 1, pp. 319-324, 2023, doi: 10.54254/2754-1169/53/20230862.

[6] G. Lian, "Research on credit algorithm of international trade enterprises based on blockchain," Mathematical Problems in Engineering 2022; 2022(1):4768868, doi: 10.1155/2022/4768868.

[7] Q. Guo, S. Lei, Q. Ye, and Z. Fang, "MRC-LSTM: A hybrid approach of multi-scale residual CNN and LSTM to predict bitcoin price," 2021 International Joint Conference on Neural Networks (IJCNN). IEEE, 2021, doi: 10.1109/IJCNN52387.2021.9534453.

[8] N. Patel, N. Vasani, N. K. Jadav, R. Gupta, S. Tanwar, and Z. Polkowski, "F-LSTM: Federated learning-based LSTM framework for cryptocurrency price prediction," Electronic Research Archive 31.10 (2023), doi: 10.3934/era.2023330.

[9] J. Liu and K. Chen, "Enterprise financial risk prevention and control and data analysis method based on blockchain technology," Mobile Information Systems 2022.1 (2022):9452342, doi: 10.1155/2022/9452342.

[10] Z. Wang, W. Wu, C. Zeng, J. Yao, Y. Yang, and H. Xu, "Graph neural networks enhanced smart contract vulnerability detection of educational blockchain," 2023. arXiv preprint arXiv:2303.04477, doi: 10.48550/arXiv.2303.04477.
[11] H. Kanezashi, T. Suzumura, X. Liu, and T. Hirofuchi, "Ethereum fraud detection with heterogeneous graph neural networks," 2022. arXiv preprint arXiv:2203.12363, doi: 10.48550/arXiv.2203.12363.
[12] D. Zhang, J. Chen, and X. Lu, "Blockchain phishing scam detection via multi-channel graph classification," Blockchain and Trustworthy Systems: Third International Conference, BlockSys 2021, Guangzhou, China, August 5–6, Art. no. Revised Selected Papers 3. Springer Singapore, 2021, 2021, doi: 10.1007/978-981-16-7993-3_19.
[13] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. Fitzek, and N. Aaraj, ""Survey on fully homomorphic encryption, theory, and applications." Proceedings of the IEEE," 2022; 110(10):1572-1609, doi: 10.1109/JPROC.2022.3205665.
[14] D. Nugent, "Privacy-preserving credit card fraud detection using homomorphic encryption," 2022. arXiv preprint arXiv:2211.06675, doi: 10.48550/arXiv.2211.06675.
[15] R. Raj, Y. Kurt Peker, and Z. D. Mutlu, "Blockchain and Homomorphic Encryption for Data Security and Statistical Privacy," Electronics, vol. 13, no. 15, pp. 3050, 2024, doi: 10.3390/electronics13153050.
[16] R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, and B. Krishnamachari, "A Survey on the Applications of Zero-Knowledge Proofs," 2024. arXiv preprint arXiv:2408.00243, doi: 10.48550/arXiv.2408.00243.
[17] J. G. Dhokrat and N. Pulgam, "A Framework for Privacy-Preserving Multiparty Computation with Homomorphic Encryption and Zero-Knowledge Proofs," Informatica 2024; 48(21), doi: 10.31449/inf.v48i21.6562.
[18] R. Soltani, M. Zaman, R. Joshi, and S. Sampalli, "Distributed ledger technologies and their applications: A review," Applied Sciences, vol. 12, no. 15, pp. 7898, 2022, doi: 10.3390/app12157898.
[19] M. D. Khan, D. Schaefer, and J. Milisavljevic-Syed, "A review of distributed ledger technologies in the machine economy: challenges and opportunities in industry and research."Procedia CIRP," 2022; 107:1168-1173, doi: 10.1016/j.procir.2022.05.126.
[20] M. C. Ballandies, M. M. Dapp, and E. Pournaras, "Decrypting distributed ledger design—taxonomy, classification and blockchain community evaluation," Cluster computing, vol. 25, no. 3, pp. 1817-1838, 2022, doi: 10.1007/s10586-021-03256-w.
[21] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," Information, vol. 14, no. 2, pp. 117, 2023, doi: 10.3390/info14020117.
[22] Qian, P, Liu, Z, Q. He, B. Huang, D. Tian, and X. Wang, "Smart contract vulnerability detection technique: A survey," 2022. arXiv preprint arXiv:2209.05872, doi: 10.48550/arXiv.2209.05872.
[23] N. Ivanov, C. Li, Q. Yan, Z. Sun, Z. Cao, and X. Luo, "Security threat mitigation for smart contracts: A comprehensive survey," ACM Computing Surveys, vol. 55, no. 14s, pp. 1-37, 2023, doi: 10.1145/3593293.
[24] K. Xu, Y. Cheng, S. Long, J. Guo, J. Xiao, and M. Sun, "Advancing financial risk prediction through optimized LSTM model performance and comparative analysis," 2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE). IEEE, 2024, doi: 10.1109/ICSECE61636.2024.10729338.
[25] W. Ormaniec, M. Pitera, S. Safarveisi, and T. Schmidt, "Estimating value at risk: LSTM vs," GARCH, Art. no. . arXiv preprint arXiv:2207.10539, 2022, doi: 10.48550/arXiv.2207.10539.
[26] J. Yao, J. Wang, B. Wang, B. Liu, and M. Jiang, "A Hybrid CNN-LSTM Model for Enhancing Bond Default Risk Prediction," Journal of Computer Technology and Software, pp. 3(6), 2024, doi: 10.5281/zenodo.13910344.
[27] Q. Zhang, C. Zhang, and X. Zhao, "Credit Risk Classification Prediction Based on Optimised Adaboost Algorithm with Long Short-Term Memory Neural Network (LSTM)," Advances in Economics, Management and Political Sciences, vol. 87, no. 1, pp. 152-158, 2024, doi: 10.54254/2754-1169/87/20240979.
[28] Z. Xia, "Early Warning of Credit Risk of Internet Financial Enterprises Based on CNN-LSTM Model," Procedia Computer Science, vol. 243, pp. 506-513, 2024, doi: 10.1016/j.procs.2024.09.062.
[29] M. Citterio, M. D'Errico, and G. Visentin, "Conditional Forecasting of Margin Calls using Dynamic Graph Neural Networks.2024," arXiv preprint arXiv:2410.23275, doi: 10.48550/arXiv.2410.23275.
[30] S. Xiang, D. Cheng, C. Shang, Y. Zhang, and Y. Liang, "Temporal and heterogeneous graph neural network for financial time series prediction," Proceedings of the 31st ACM international conference on information & knowledge management; 17-21 October 2022; Atlanta, GA, USA; 2022, doi: 10.1145/3511808.3557089.
[31] B. P. Jeyaraman, B. T. Dai, and Y. Fang, "Temporal Relational Graph Convolutional Network Approach to Financial Performance Prediction," Machine Learning and Knowledge Extraction, vol. 6, no. 4, pp. 2303-2320, 2024, doi: 10.3390/make6040113.
[32] D. Wang, Z. Zhang, J. Zhou, P. Cui, J. Fang, Q. Jia, et al., "Temporal-aware graph neural network for credit risk prediction," Proceedings of the 2021 SIAM International Conference on Data Mining (SDM). 29 April-1 May 2021; Online; 2021. Society for Industrial and Applied Mathematics, 2021, doi: 10.1137/1.9781611976700.79.
[33] A. Uddin, X. Tao, and D. Yu, "Attention based dynamic graph neural network for asset pricing," Global finance journal, vol. 58, Art. no. 100900, 2023, doi: 10.1016/j.gfj.2023.100900.
[34] S. S. Moghadam, A. Aghsami, and M. Rabbani, "A hybrid NSGA-II algorithm for the closed-loop supply chain network design in e-commerce," RAIRO-Operations Research, vol. 55, no. 3, pp. 1643-1674, 2021, doi: 10.1051/ro/2021068.
[35] A. Acerce and B. Denizhan, "Application of the Non-Dominated Sorting Genetic Algorithm II (NSGA-II) in a Two-Echelon Cold Supply Chain," Systems, vol. 13, no. 3, pp. 206, 2025, doi: 10.3390/systems13030206.
[36] M. Li, H. Ma, S. Lv, L. Wang, and S. Deng, "Enhanced NSGA-II-based feature selection method for highdimensional classification," Information Sciences, vol. 663, Art. no. 120269, 2024, doi: 10.1016/j.ins.2024.120269.
[37] H. Cui, F. Cao, and R. Liu, "A multi-objective partitioning algorithm for large-scale graph based on NSGA-II," Expert Systems with Applications, vol. 263, Art. no. 125756, 2025, doi: 10.1016/j.eswa.2024.125756.