Abnormal Node Classification and Security Detection for Cross-border SME E-commerce Using Blockchain Network Topology Algorithms

Yuyan Lyu[1,*], Dongmei Han[2]
[1]Business School, Guangzhou College of Technology and Business, Guangzhou 510000, China
[2]School of Business and Trade, Anhui Wenda University of Information Engineering, Hefei 23000, China
E-mail: colour_lyy@163.com, 26347751@qq.com
[*]Corresponding author

Keywords: blockchain, network topology, cross-border e-commerce, digital economy, transaction security

Received: June 18, 2025

In light of the pressing concerns regarding the inadequacy of transaction security, efficiency, and transparency within the financial system, this study endeavors to enhance the security of digital economy transactions for small and medium-sized enterprises engaged in cross-border e-commerce through the application of blockchain network topology algorithms. Specifically, the research introduces an innovative approach to classifying abnormal nodes, leveraging a dynamic update algorithm rooted in blockchain network topology. Additionally, it proposes a method for detecting security in digital economy transactions, also grounded in blockchain network topology algorithms. Under the conditions of a total of 60,000 records of real transactions in Bitcoin and Ethereum and a node scale of 100 to 1,000, the experiment uses a combination of cosine and Euclidean distance to calculate the transaction frequency, amount and time series characteristics of nodes and complete clustering. Subsequently, a sliding time window is used to dynamically update the node similarity threshold to identify anomalies. Compared with the three benchmark methods of density clustering, graph convolutional network and autoencoder, the proposed blockchain network topology algorithm has a root mean square error of 0.09, a mean absolute error of 0.09, an anomaly detection accuracy of 8.6%, and a transaction success rate of 1.1%, which is jointly determined by a 1.8-millisecond delay and a throughput of 13.2 transactions per second. All indicators are superior to the benchmark methods. The blockchain network topology algorithm can significantly improve transaction security and system stability, which is of great significance for promoting sustainable economic growth and social stability.

Povzetek:

1 Introduction

With the rapid evolution of the digital economy, small and medium-sized enterprises operating in the cross-border e-commerce (CBEC) sector are gaining ever-greater prominence in the landscape of global trade. Nevertheless, the escalating concerns surrounding transaction security within the financial system have emerged as a pivotal obstacle, significantly hindering the industry's growth and development [1]. The traditional financial system has problems such as cumbersome processes, easy errors, low efficiency, and insufficient security, which not only increase transaction costs, but also may lead to financial fraud and data leakage, seriously affecting the stable growth of the economy and the sustainable development of society [2-3]. The application of blockchain technology (BCT) can significantly reduce the risk of financial fraud transactions, accelerate trade financial settlement time, and improve compliance efficiency. In addition, the integration of blockchain with artificial intelligence (AI), the Internet of Things (IoT), and cloud computing (CC) has further enhanced real-time financial monitoring, trade authentication, and data security management capabilities, promoting the digitalization process of finance [4]. However, current research has predominantly centered on the theoretical exploration and initial implementation of BCT, leaving a conspicuous gap in thorough and comprehensive investigations into the effective identification and categorization of anomalous nodes within digital economic transactions, along with the development of efficient algorithms for detecting security risks in such transactions [5-6].

To address the issue of insufficient transparency in the financial system, Abdin et al. systematically explored the application trends, challenges, and impacts of BCT in the financial sector through case analysis. The results showed that the application of BCT significantly reduced financial fraud transactions by 42%, accelerated trade finance settlement time by 58%, and improved compliance efficiency by 49%. In addition, the integration of blockchain with AI, the IoT, and CC enhanced real-time financial monitoring, trade authentication, and data security management capabilities, promoting the digitalization process of finance [7]. Mishra et al.

proposed a solution using blockchain network technology to address the problems of cumbersome processes, easy errors, low efficiency, and insufficient security in traditional financial systems. The research results indicated that compared with traditional systems, BCT had the characteristics of lower cost, higher transparency, and better efficiency. Especially in the banking industry, BCT could significantly improve security, performance, and reduce the cost of various business processes, providing users with better quality services [8]. In response to the issue of storage sustainability in blockchain systems, Liu et al. optimized storage structures and data management methods to improve storage efficiency and encourage users to pay reasonable transaction fees to cover storage costs. The research results indicated that these mechanisms could effectively alleviate storage pressure, enhance the long-term feasibility of the system, and provide reference for small and medium-sized enterprises to ensure data storage security in CBEC business [9]. To address the issues of insufficient transparency and lack of public trust in the economic field, Cao et al. used a literature review method to examine the impact of BCT on improving economic transparency and cultivating public assurance. By analyzing multiple sources of information and text, the study found that BCT, with its high transparency, security, and data integrity, became an effective tool for achieving economic transparency and enhancing public trust. The results indicated that in an increasingly data dependent society, BCT was of great significance in promoting sustainable economic growth and social stability [10]. The application effects and limitations of BCT in the financial system are compared in Table 1.

Table 1: Comparison of the application effects and limitations of BCT in the financial system

References	Main findings	Limitations
Abdin et al. [7]	BCT significantly reduces financial fraud by 42%, accelerates transaction settlement by 58%, and enhances compliance efficiency by 49%	There is a lack of in-depth research on the detection and classification of abnormal nodes
Mishra et al. [8]	BCT reduces the costs of the traditional financial system and enhances transparency and efficiency	There is no detailed application involving the integration of blockchain with other technologies
Liu et al. [9]	Optimize the storage structure and data management methods to alleviate storage pressure	Anomaly detection and system stability have not been fully considered
Cao et al. [10]	BCT enhances economic transparency and public trust	There is a lack of in-depth analysis of the blockchain network topology

In summary, existing research has mostly focused on theoretical exploration and preliminary applications, and there remains a notable absence of rigorous investigation into how to effectively utilize blockchain network topology to identify and classify abnormal nodes, as well as how to design efficient transaction security detection algorithms. The core research question focuses on the dynamic topology update mechanism of blockchain networks. It examines whether this mechanism can effectively improve abnormal node detection accuracy and enhance transaction security for cross-border small and medium-sized e-commerce. To delve deeper into the application of blockchain network topology algorithms for abnormal node detection and transaction security enhancement, thereby improving both transaction safety and system stability, a method is proposed for classifying abnormal nodes based on a dynamic update algorithm derived from blockchain network topology. Additionally, an algorithm is designed for detecting security risks in digital economy transactions. By analyzing the hierarchical structure, node clustering, and dynamic update mechanism of blockchain networks, accurate identification and classification of abnormal nodes can be achieved, and network topology analysis and node behavior characteristics can be used to identify and defend against various attack behaviors. A method based on blockchain network topology dynamic update algorithm is innovatively proposed, which achieves accurate identification and classification of abnormal nodes in digital economy transactions by analyzing the hierarchical structure of the blockchain network, combining node clustering analysis and dynamic update mechanism. Additionally, an efficient digital economy transaction security detection algorithm was designed, which utilizes network topology analysis and node behavior characteristics to accurately detect and defend against various attack behaviors, significantly improving the security and system stability of digital economy transactions for small and medium-sized enterprises in CBEC. By introducing a dynamic update mechanism for the blockchain network topology, the research can more accurately capture the spatio-temporal variation characteristics of node behavior, thereby achieving significant improvements in key performance indicators such as anomaly detection accuracy, transaction processing delay, and system stability. This method, grounded in topological dynamics, offers a fresh perspective and solution for bolstering the security and robustness of blockchain networks. It effectively bridges the gap left by existing approaches in anomaly detection within dynamic network settings, showcasing its distinct advantages and significant application potential in current research.

2 Methods and materials

The study proposes an innovative method based on blockchain network topology dynamic update algorithm, aiming to identify and classify abnormal nodes in digital economic transactions, and designs an efficient digital economic transaction security detection algorithm. Through the hierarchical structure and node clustering analysis of blockchain networks, combined with dynamic update mechanisms, accurate identification and classification of abnormal nodes can be achieved. Meanwhile, network topology analysis and node behavior characteristics can be used to detect and defend against various attack behaviors, providing technical support for improving the security of digital economy transactions for CBEC small and medium-sized enterprises.

2.1 Classification of abnormal nodes in digital economy transactions based on topology dynamic update algorithm

The research selects the design principle based on the dynamic update algorithm of blockchain network topology to accurately identify and classify abnormal nodes in the e-commerce scenarios of cross-border small and medium-sized enterprises, ensuring transaction security and system stability. Clustering technology is chosen because it can effectively identify node groups with similar behavioral characteristics, laying the foundation for anomaly detection. Meanwhile, the research introduces dynamic update thresholds, enabling the algorithm to adapt in real time to changes in network topology and ensuring high detection accuracy under different network conditions. This enhances the accuracy of anomaly detection and the real-time performance and adaptability of the system, providing reliable and secure protection for digital economy transactions. Blockchain is divided into data layer, network layer, consensus layer, and application layer. The data layer is mainly responsible for the storage and management of blockchain data, including transaction data, block structure, etc. The network layer is responsible for communication and data transmission between nodes. The consensus layer ensures the verification and confirmation of transactions by nodes in the network through consensus mechanisms. The application layer provides various blockchain-based application services. In digital economy transactions, each layer may become a target of attack, so it is necessary to comprehensively consider the security of each layer [11-12]. The blockchain hierarchy is shown in Figure 1.

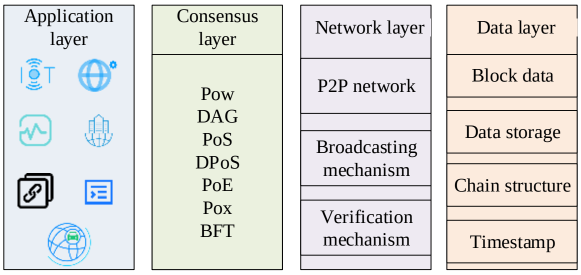


Figure 1: Blockchain hierarchy

In Figure 1, the data layer is accountable for storing the basic data of the blockchain, including block data, data storage, chain structure, and timestamps. The network layer includes peer-to-peer (P2P) networks, broadcasting mechanisms, and verification mechanisms to ensure the transmission and verification of data between nodes. The consensus layer involves various consensus algorithms, such as Proof of Work (PoW), Directed Acyclic Graph (DAG), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Energy (PoE), Proof of X (PoX), and Byzantine Fault Tolerance (BFT), employed to reach agreement within distributed networks. The application layer covers a variety of application scenarios such as the IoT, the Internet of Vehicles, the Industrial Internet, smart contracts, smart cities and health records, and shows the extensive application of BCT in different fields. The architecture of the blockchain node network topology system is shown in Figure 2. In this architecture, nodes communicate through the network layer, the data layer stores transaction information, the consensus layer ensures the legality of transactions, and the application layer provides transaction services. Through this hierarchical architecture, node behavior in the network can be effectively managed and monitored, providing a foundation for detecting abnormal nodes [13-14].

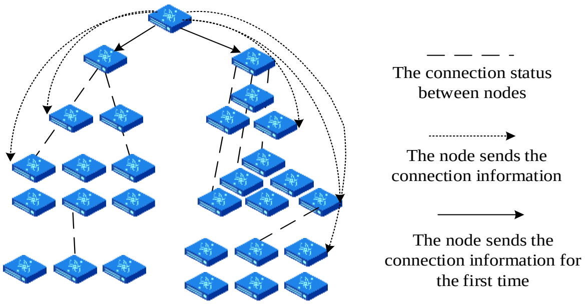

The connection status between nodes
The node sends the connection information
The node sends the connection information for the first time

Figure 2: Architecture of the blockchain node network topology system

In Figure 2, when a node joins the network for the first time or needs to establish a connection with another node, it sends connection information to the target node. Once the connection is established, the nodes will maintain this connection state and ensure the validity of the connection through continuous communication. The architecture displays multi-level connections between nodes, meaning that one node can be connected to multiple nodes to form a complex network structure. This multi-level connection enhances the robustness and decentralization of the network. Nodes not only communicate with directly connected nodes, but also propagate information through indirectly connected nodes, thereby achieving widespread dissemination of information in the network.

Subsequently, an algorithm is developed to group nodes in blockchain networks with the aim of categorizing them into diverse classes. This process promotes multi-threaded recognition of network structures. By using clustering algorithms, nodes with similar behavioral characteristics can be grouped together, which facilitates subsequent anomaly detection. Meanwhile, an algorithm is introduced to make real-time adjustments to the network structure. The algorithm's objective is to diminish usage of network resources required for identifying network structures and enhance the rate of network structure identification updates [15-16]. The classification process of abnormal nodes in digital economy transactions based on topology dynamic update algorithm is shown in Figure 3.

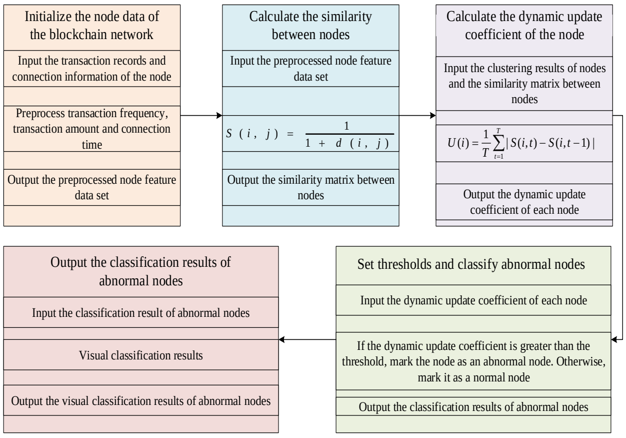

Initialize the node data of the blockchain network
Input the transaction records and connection information of the node
Preprocess transaction frequency, transaction amount and connection time
Output the preprocessed node feature data set
Calculate the similarity between nodes
Input the preprocessed node feature data set
$S(i,j)=\frac{1}{1+d(i,j)}$
Output the similarity matrix between nodes
Calculate the dynamic update coefficient of the node
Input the clustering results of nodes and the similarity matrix between nodes
$U(i)=\frac{1}{T}\sum_{t=1}^{T}|S(i,t)-S(i,t-1)|$
Output the dynamic update coefficient of each node
Set thresholds and classify abnormal nodes
Input the dynamic update coefficient of each node
If the dynamic update coefficient is greater than the threshold, mark the node as an abnormal node. Otherwise, mark it as a normal node
Output the classification results of abnormal nodes
Output the classification results of abnormal nodes
Input the classification result of abnormal nodes
Visual classification results
Output the visual classification results of abnormal nodes

Figure 3: Flow chart of abnormal node classification in digital economy transaction based on topology dynamic update algorithm.

In Figure 3, first, cluster analysis is performed on the nodes in the blockchain network. To accurately describe the similarity measurement, the study adopts a combined method of cosine similarity and Euclidean distance to calculate the similarity between nodes. Cosine similarity is used to measure the directional similarity of node feature vectors, while Euclidean distance is used to measure the absolute distance of feature vectors. Similarity can be calculated based on features such as transaction frequency, transaction amount, and connection time between nodes. Specifically, as shown in equation (1).

$$S(i,j)=\frac{1}{1+d(i,j)} \tag{1}$$

In equation (1), $S(i,j)$ represents the similarity between node i and node j, and $\frac{1}{1+d(i,j)}$ represents the Euclidean distance or other distance measure between node i and node j. By calculating the similarity between all nodes, nodes can be divided into different clusters. A dynamic update algorithm is designed based on clustering. The dynamic update coefficient of node is defined to measure the behavior change of node i within a continuous time window. Specifically, as shown in equation (2).

$$U(i)=\frac{1}{T}\sum_{t=1}^{T}|S(i,t)-S(i,t-1)| \tag{2}$$

In equation (2), $U(i)$ represents the dynamic update coefficient of the node, T represents the size of the time window, and $S(i,t)$ represents the similarity of node i over time t. By calculating the dynamic update coefficient of nodes, nodes with abnormal behavior can be identified. According to the dynamic update coefficient of nodes, they are divided into normal nodes and abnormal nodes. The study sets a threshold θ, when , node i is marked as an abnormal node. The research has refined the approach to identifying abnormal nodes by moving away from the simplistic method of setting a fixed threshold at zero. Instead, it has introduced a dynamic threshold mechanism grounded in statistical analysis, which carefully considers the normal range of fluctuations inherent in network behavior. The threshold of the dynamic update coefficient $U(i)$ is determined by analyzing the distribution of $U(i)$ in historical data, ensuring that node i is marked as abnormal only when $U(i)$ exceeds a certain confidence interval within the normal fluctuation range. This data-driven threshold setting method reduces false alarms caused by normal fluctuations and improves the accuracy and robustness of anomaly detection. The selection of thresholds in the research is based on the statistical analysis and experimental verification of the dynamic update coefficients of nodes. By analyzing a large amount of node behavior data, the distribution characteristics of the dynamic update coefficient are determined, and then the initial threshold is set based on these distribution characteristics. During the experimental stage, the anomaly detection performance under different thresholds is evaluated. Based on indicators such as detection accuracy and false alarm rate, the grid search method is used to optimize and adjust the thresholds. Eventually, the optimal threshold is determined to achieve precise identification and classification of abnormal nodes. In terms of abnormal node classification, the study adopts the K-means clustering algorithm. The clustering process calculates the similarity between nodes based on characteristics such as transaction frequency, transaction amount and connection time of nodes, and uses the Euclidean distance metric, as shown in equation (3).

$$similarity_{ij}=\exp(-distance_{ij}) \tag{3}$$

In equation (3), $distance_{ij}$ represents the Euclidean distance between node i and node j. Based on this similarity, the K-means algorithm divides nodes into different clusters, and the nodes within the clusters have similar behavioral characteristics. Subsequently, through the dynamic update algorithm, the dynamic update coefficient is calculated based on the behavioral changes of nodes within the continuous time window to identify abnormal nodes.

2.2 Digital economy transaction security detection based on blockchain network topology algorithm

The classification method of abnormal nodes in digital economy transactions based on topology dynamic update algorithm can effectively identify and classify abnormal nodes in transactions. On this basis, further research is conducted to design a digital economy transaction security detection method based on blockchain network topology algorithm, which utilizes network topology structure and node behavior characteristics to identify and defend against various attack behaviors, thereby enhancing the security of the entire transaction system. This algorithm utilizes network topology analysis and combines node behavior characteristics to achieve accurate detection of abnormal behavior [17-18]. Figure 4 shows how attackers can control multiple malicious nodes to send a large number of requests to the target node, causing the target node to exhaust its resources and unable to process legitimate transaction requests.

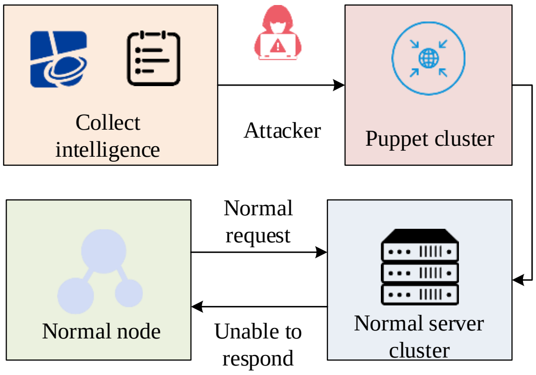


Figure 4: Schematic diagram of network denial-of-service attack.

In Figure 4, puppet cluster refers to a collection of nodes that are manipulated by attackers and used to launch a large number of malicious requests to exhaust the resources of the target node. The Normal server cluster represents the collection of normal nodes in the blockchain network that are responsible for processing legitimate transactions. The intelligence information section shows that the attacker first collects intelligence information and then uses this information to organize a puppet cluster to make malicious requests to the normal server cluster. These malicious requests cause the server to respond to malicious requests while ignoring requests from normal nodes, ultimately resulting in requests from normal nodes being unresponsive, and the normal server cluster being unable to provide services normally. The schematic diagram of the network topology structure is shown in Figure 5, depicting the connection relationships of nodes in the blockchain network. By analyzing these connection relationships, abnormal patterns in the network can be identified, such as abnormal transaction frequencies or unusual connection patterns.

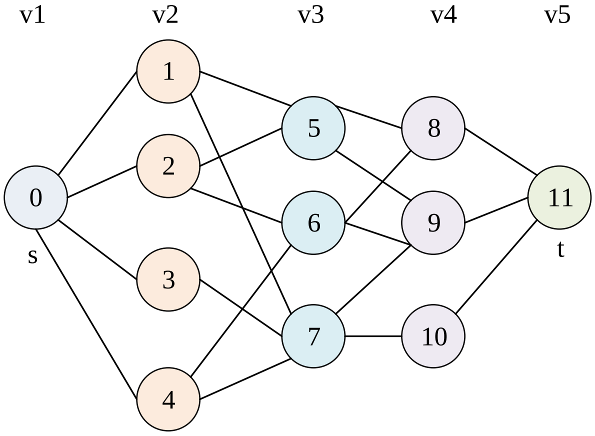


Figure 5: Schematic diagram of the network topology structure.

Figure 5 shows a network model consisting of nodes and edges. The starting node is marked as s, the ending node is marked as t, and there are several nodes numbered 0 to 10 in between. The connections between nodes represent their connectivity relationships, forming a complex network. Node 0 is directly connected to nodes 1 to 4, while nodes 5 and 6 are connected to multiple other nodes, further expanding the coverage of the network. Nodes 8 to 11 form another part of the network, connected to the starting and intermediate nodes through multiple paths. The flowchart of the digital economy transaction security detection algorithm based on blockchain network topology algorithm is shown in Figure 6.

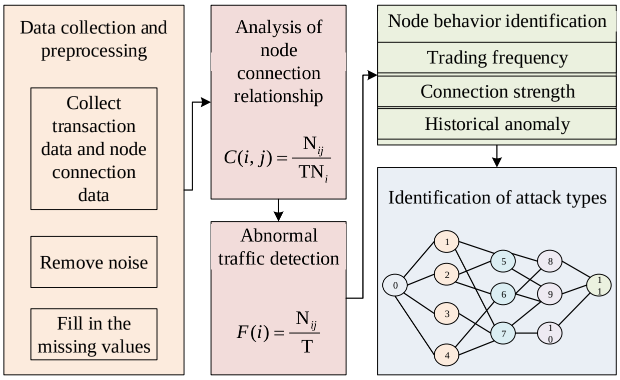

Data collection and preprocessing
Collect transaction data and node connection data
Remove noise
Fill in the missing values
Analysis of node connection relationship
$C(i,j)=\frac{N_{ij}}{TN_i}$
Abnormal traffic detection
$F(i)=\frac{N_{ij}}{T}$
Node behavior identification
Trading frequency
Connection strength
Historical anomaly
Identification of attack types

Figure 6: Flowchart of the digital economy transaction security detection algorithm based on blockchain network topology algorithm.

In Figure 6, the algorithm first collects transaction data and node connection data in the blockchain network, and preprocesses these data to remove noise and fill in missing values. Next, the algorithm analyzes the connection relationships between nodes and quantifies the transaction interactions between node i and node j by calculating the connection strength, as shown in equation (4).

$$C(i,j)=\frac{N_{ij}}{TN_i} \tag{4}$$

In equation (4), $C(i, j)$ is the ratio of the total number of transactions between node i to the number of transactions between node i and node j, N_{ij} represents the number of transactions between node i and node j, and TN_i represents the total number of transactions participated by node i. The transaction frequency is used to measure the trading activity of node i within a given time window T, as shown in equation (5).

$$F(i) = \frac{N_i}{T} \tag{5}$$

In equation (5), $F(i)$ represents the total number of transactions that node i participates in within the time window T, and N_i represents the total number of transactions of node i. The node behavior feature vector is a comprehensive description of node behavior, including transaction frequency, connection strength with another node, and historical anomaly records, as shown in equation (6). The historical anomaly record in the feature vector represents the number of times a node has been marked as an anomaly within a certain period of time in the past.

$$B(i) = [F(i), C(i, j), \text{Historical Anomaly Records}_i] \tag{6}$$

In equation (6), $B(i)$ represents the behavior feature vector of node i and $\text{Historical Anomaly Records}_i$ represents the historical abnormal behavior records related to node i. Historical abnormal behavior is quantified by tallying the frequency with which a computing node has been flagged as anomalous over a designated past time frame, and this count is then incorporated as a constituent element of the feature vector. This quantization method provides a clear numerical representation of the feature vectors, which helps capture the historical behavior patterns of nodes in the model and thereby enhances the accuracy of anomaly detection. Subsequently, a transaction frequency threshold is set to detect abnormal traffic. If the transaction frequency of node i exceeds the threshold within time window T, the node is marked as abnormal. In addition, random forests are used to classify node behavior based on node behavior feature vectors, including transaction frequency, connection strength, and historical anomaly records. The algorithm further identifies specific types of attacks, with denial-of-service attacks identified by detecting abnormal transaction frequencies, witch attacks and solar eclipse attacks identified by analyzing the connection strength and transaction flow between nodes, and network segmentation attacks identified by detecting the presence of isolated subgraphs in the network [19-20]. Finally, based on the detection results, corresponding security strategies will be deployed to isolate abnormal nodes, strengthen monitoring and defense of potential attack paths, effectively detect and defend against attack behaviors in CBEC small and medium-sized enterprise digital economy transactions, and ensure transaction security and stability. The pseudo-code of the algorithm is shown in Table 2.

Table 2: Pseudo-code of the Algorithm.

```
1. Initialize the set of abnormal nodes A as an empty set
2. For each time window t ∈ {1, 2, ..., T}:
  a. Calculate the similarity matrix S between nodes using a combination of cosine similarity and Euclidean distance:
     S[i][j] = α * cos(V[i], V[j]) + (1 - α) * exp(-distance(V[i], V[j]))
  b. Perform clustering on nodes using the K-means algorithm to obtain clustering result C
  c. For each node i:
     i. Calculate the dynamic update coefficient DUC[i] of node i based on its similarity changes within time window t:
        DUC[i] = (S[i][j] - S[i][j-1]) / T
     ii. If DUC[i] > θ, then mark node i as an abnormal node and add it to set A
3. Return the set of abnormal nodes A
```

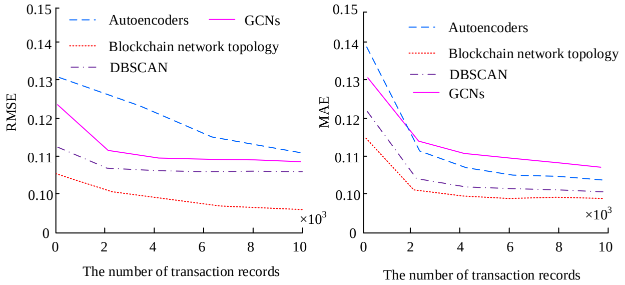
The research proposes an abnormal node classification method based on the dynamic update algorithm of blockchain network topology. This method first collects and preprocesses the transaction data of the Bitcoin and Ethereum networks, then extracts node features including transaction frequency, transaction amount, connection time and historical abnormal records, and standardizes these features to eliminate dimensional influence. Subsequently, the K-means clustering algorithm is applied to conduct cluster analysis based on the similarity of node feature vectors. The dynamic update coefficient of each node is calculated to reflect the change of its behavior over time. A threshold is set to identify abnormal nodes whose dynamic update coefficient exceeds this threshold. Finally, the performance of the algorithm is evaluated by analyzing the detection results. The parameters are adjusted based on the feedback from the validation set to optimize the model.

3 Results

The performance of the proposed blockchain network topology algorithm was evaluated through experiments, and its application effect in the digital economy transaction security of small and medium-sized enterprises in CBEC was analyzed. The experiment selected multiple blockchain network datasets and compared the performance of this algorithm with other advanced algorithms in terms of performance indicators. Meanwhile, the actual application effect of this algorithm in digital economy transaction security was analyzed from multiple dimensions such as transaction processing latency, network throughput, node discovery time, and anomaly detection accuracy.

3.1 Performance evaluation of blockchain network topology algorithms

To ensure the reproducibility and transparency of the research, the study provided detailed model parameters, training procedures and validation details. The model parameters included a time window size set at 12 hours, the parameters of the clustering algorithm optimized to 5 based on the elbow rule, and the threshold determined through grid search within the range of 0.05 to 0.15. In terms of the training program, the dataset was divided into a training set and a validation set in a 7:3 ratio. The model was trained based on the training set, and the optimal parameters were selected according to the performance of the validation set. To comprehensively evaluate the model's performance, the study comprehensively considered multiple dimensions of indicators such as precision, recall rate, F1 score, system stability, and resource utilization. Precision and recall respectively measured the accuracy and completeness of the model in predicting abnormal nodes, while the F1 score comprehensively considered both precision and recall, providing a balanced performance evaluation. In addition, system stability was measured by the percentage of uptime, while resource utilization assessed the model's occupation of computing resources in practical applications, ensuring that the model could efficiently detect anomalies while also operating stably in resource-constrained environments. The Bitcoin dataset contained transaction records from 2010 to 2020, totaling over 5 million transactions. The Ethereum dataset covers transaction data from 2015 to 2020, totaling approximately 3 million records. The sampling method adopted stratified random sampling, ensuring the representativeness and diversity of the data. The preprocessing steps included data cleaning, outlier removal, standardization processing, and feature extraction, etc., to improve data quality and the accuracy of the algorithm. To verify the effectiveness and superiority of the proposed blockchain network topology algorithm, a series of experiments were designed and compared with several other advanced algorithms. Comparative algorithms included Density-Based Spatial Clustering of Applications with Noise (DBSCAN), Graph Convolutional Networks (GCNs), and Autoencoders. The accuracy of anomaly detection reflected the algorithm's ability to identify abnormal nodes and was a key indicator for measuring the algorithm's performance. Transaction processing latency and transaction verification time were directly related to the system's response speed and user experience. Network throughput and concurrent processing capacity reflected the system's ability to handle transactions within a unit of time and were important bases for evaluating system scalability and handling large-scale transactions. The system stability and resource utilization rate demonstrated the reliability and resource utilization efficiency of the algorithm in actual operation. The root means square error (RMSE) and mean absolute error (MAE) of several algorithms are shown in Figure 7.

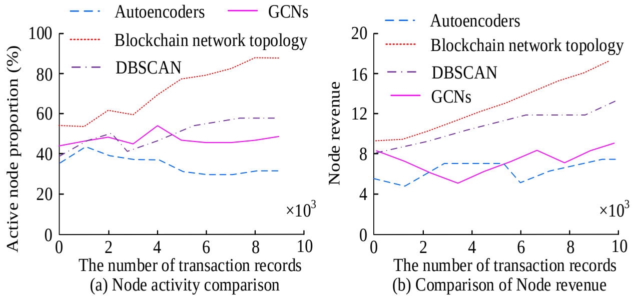


(a) RMSE

(b) MAE

Figure 7: RMSE and MAE of several algorithms.

In Figure 7 (a), the blockchain network topology algorithm exhibited the lowest RMSE at all data volumes, especially when the data volume was small. Finally, when the data volume reached 60000, the RMSE dropped to about 0.09. The RMSE of the DBSCAN algorithm did not vary significantly throughout the entire range of data volume, remaining at around 0.11. This indicated that blockchain network topology algorithms had better prediction accuracy and stability when processing data of different scales. In Figure 7 (b), the blockchain network topology algorithm exhibited the lowest MAE at all data volumes, especially when the data volume was small. Finally, when the data volume reached 60000, the MAE dropped to about 0.09. This further confirmed that blockchain network topology algorithms not only had better prediction accuracy when processing data of different scales but also performed well in error control, demonstrating their potential and advantages in practical applications. The node activity and node revenue of several algorithms are shown in Figure 8. Node Revenue referred to the economic benefits obtained by nodes during their participation in transactions. It was used to measure the economic contribution and revenue of nodes in the network, reflecting the activity and economic benefits of nodes in the blockchain network. High node returns usually meant more transactions were successfully processed, which was closely related to transaction security and system stability, because only in a safe and stable environment could nodes continuously earn returns.



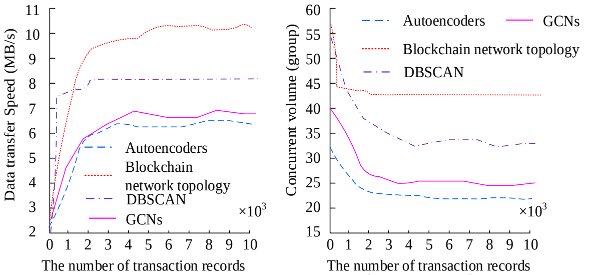
(a) Node activity comparison

(b) Comparison of Node revenue

Figure 8: Node activity and node revenue of several algorithms.

In Figure 8 (a), with the increase of data volume, the node activity ratio of the blockchain network topology algorithm significantly increased, from about 40% when the data volume was 0 to nearly 90% when the data volume was 10000. This indicated that it could effectively improve node activity when processing large-scale data.

The blockchain network topology algorithm had significant advantages in improving node activity. Especially when processing large-scale data, it could effectively stimulate node participation, thereby improving the efficiency and performance of the entire network. In Figure 8 (b), the node revenue of the blockchain network topology algorithm significantly increased with the increase of data volume, from about 8 units when the data volume was 0 to nearly 20 units when the data volume was 10000. Units referred tao the amount of revenue accumulated by a node through participating in transaction verification within a specific time window, which was measured by the product of the number of valid transactions processed by the node and the corresponding transaction fees. This indicated that it could bring higher revenue to nodes when processing large-scale data. The transmission rate and concurrency rate of several algorithms are shown in Figure 9.



(a) Transmission rate (b) Concurrent volume

Figure 9: Transmission rate and concurrency rate of several algorithms.

In Figure 9 (a), the blockchain network topology algorithm quickly reached the peak transmission rate of nearly 11 MB/s when the dataset size was about 1000, and remained relatively stable when the dataset size increased to 10000. The blockchain network topology algorithm had significant transmission rate advantages when processing small datasets; it could quickly achieve high transmission rates and still maintain high transmission efficiency when processing larger datasets. In Figure 9 (b), the concurrency of the blockchain network topology algorithm gradually decreased with the increase of dataset size, from about 55 groups when the dataset size was 0 to about 45 groups when the dataset size was 10000, indicating a decrease in its concurrency processing ability when dealing with large-scale datasets. Although blockchain network topology algorithms performed well in terms of transmission speed, further optimization might have been needed in terms of concurrent processing capabilities to meet the concurrent processing requirements of large-scale datasets.

3.2 Analysis of the security effectiveness of digital economy transactions for small and medium-sized enterprises in CBEC

To accurately simulate and detect specific attack behaviors, such as denial-of-service attacks (DoS) and eclipse attacks, corresponding attack models were studied and constructed, and targeted detection mechanisms were designed. In the context of DoS attacks, the detection mechanism operated by simulating scenarios where an attacker gained control over multiple malicious nodes, which then flooded the target node with a vast number of requests. This onslaught depleted the target node's resources, rendering it incapable of processing legitimate transaction requests. The mechanism subsequently identified attack behaviors by scrutinizing abnormal fluctuations in both the transaction frequency and connection strength of the nodes involved. For solar eclipse attacks, it simulated that the attacker used the controlled node to isolate the target node from the rest of the network, making the target node communicate only with the node controlled by the attacker. The detection mechanism identified such attacks by analyzing abnormal patterns in the connection relationships between nodes, such as the appearance of isolated subgraphs. To evaluate the performance of the proposed blockchain network topology algorithm more comprehensively, the study introduced multiple baseline methods for comparison, including not only DBSCAN, GCN, and Autoencoder, but also Isolation Forest and LSTM-based detectors.The comparison results are shown in Table 3.

Table 3: Performance comparison of different baseline methods and blockchain network topology algorithms.

Algorithms	DBSCAN	GCN	Autoencoder	Isolation Forest	LSTM-based Detector	Blockchain network topology algorithm
Anomaly detection accuracy (%)	79.0	83.0	78.0	80.5	82.0	86.0
Transaction Processing Delay (ms)	2.2	2.1	2.5	2.3	2.0	1.8
Transaction Verification Time (ms)	2.9	2.7	3.0	2.8	2.6	2.5
Network Throughput (TPS)	8.5	11.0	7.8	9.0	10.5	13.2
Concurrent	546	510	680	560	580	800

Processing Capability (TPS)						
Network scalability (nodes per second)	5	2	4	3	3	10
System stability (%)	94.1	95.0	93.0	94.5	95.5	97.0
Resource utilization rate (%)	89.0	91.0	86.0	88.0	90.0	93.0

From Table 3, the proposed blockchain network topology algorithm achieved 86.0% accuracy in anomaly detection, which was significantly higher than other baseline methods. This indicated that it had higher precision in identifying abnormal nodes. In terms of transaction processing latency and transaction verification time, this algorithm was only 1.8ms and 2.5ms respectively. Compared with other algorithms, it could complete transaction processing and verification more quickly. The network throughput of this algorithm was 13.2TPS, and its concurrent processing capacity was as high as 800TPS, far exceeding other baseline methods. This indicated that it could handle a large number of transactions more efficiently and had a stronger concurrent processing capacity. In addition, in terms of indicators such as network scalability, system stability, resource utilization rate, and transaction success rate, this algorithm also demonstrated excellent performance. The network scalability was 10 nodes per second, the system stability was as high as 97.0%, the resource utilization rate was 93.0%, and the transaction success rate was 91.1%. These data indicated that this algorithm ensured transaction security while maintaining the stable operation of the system and the efficient utilization of resources. The standard deviation of all data was within 1.2%, indicating that the algorithm had high stability and reliability in multiple experiments. The CPU usage and response time of the algorithm in actual CBEC small business digital economy transactions are shown in Figure 10.

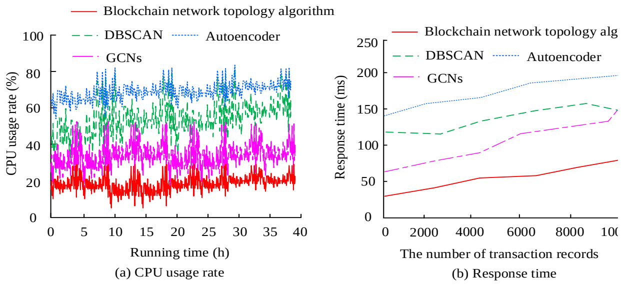


Figure 10: CPU occupancy and response time of the algorithm.

In Figure 10 (a), the blockchain network topology algorithm maintained the lowest CPU usage throughout the entire runtime, with a fluctuation range of approximately 10% to 30%, demonstrating high stability and efficiency. This indicated that blockchain network topology algorithms could more effectively utilize CPU resources and reduce the consumption of computing resources when processing the same tasks. In Figure 10 (b), as the amount of data increased, the response time of all algorithms also increased, but the response time growth of blockchain network topology algorithms was the smoothest, increasing from about 20 milliseconds to around 100 milliseconds. This indicated that blockchain network topology algorithms had better scalability and responsiveness when processing large-scale data, and could effectively handle a large number of concurrent requests while maintaining low latency.

3.3 The practical application results of blockchain network topology algorithms

To further verify the effectiveness of the proposed blockchain network topology algorithm, the experimental results were elaborated in detail through the Receiver Operating Characteristic Curve (ROC), confusion matrix and time series graph. The ROC curve of the blockchain network topology algorithm is shown in Figure 11.

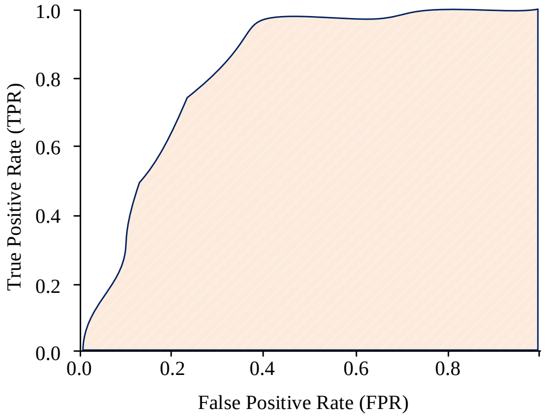


Figure 11: ROC curve of blockchain network topology algorithm.

In Figure 11, the Area under the Curve (AUC) of the blockchain network topology algorithm was 0.92, demonstrating its superior performance in anomaly detection. The actual classification confusion matrix of the blockchain network topology algorithm is shown in Figure 12.

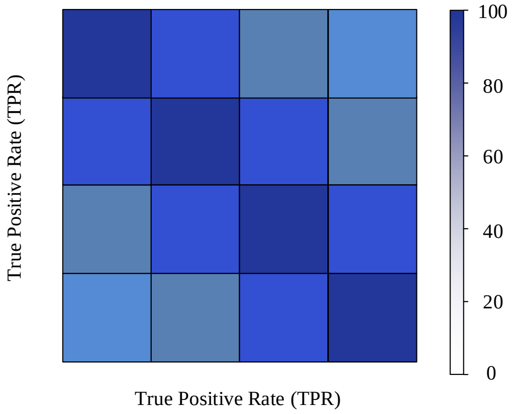


Figure 12: Actual classification confusion matrix of blockchain network topology algorithm.

In Figure 12, the TPR of the blockchain network topology algorithm on the test dataset reached 86.0%, further demonstrating its high precision and low false alarm rate. The curve of the actual transaction processing delay varying with time is shown in Figure 13.

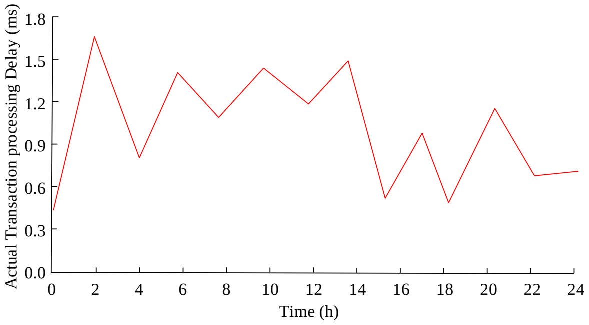


Figure 13: Curve of actual transaction processing delay over time.

In Figure 13, the proposed algorithm maintained a transaction processing delay of approximately 1.8 milliseconds within 24 consecutive hours of operation without significant fluctuations, demonstrating the high stability and reliability of the algorithm in practical applications.

4 Discussion

The algorithm proposed by the research achieved an anomaly detection accuracy of 86.0%, which was significantly higher than the 79.0% reported by DBSCAN, 83.0% by GCN, and 78.0% by Autoencoder. This improvement was mainly attributed to the fact that the algorithm proposed by the research utilized the multi-layer structure and node behavior characteristics of the blockchain network, and adjusted the similarity threshold in real time through a dynamic update mechanism, thereby more accurately identifying abnormal nodes. Although the research by Abdin Z et al. [7] made significant progress in reducing financial fraud, their methods were mainly based on macro transaction data and lack fine-grained analysis of node behavior. Although the research by Liu Y et al. [9] optimized the storage structure and improved the system stability, there is still room for improvement in the accuracy of anomaly detection. In terms of latency, the transaction processing latency of the algorithm proposed by the research was only 1.8 milliseconds, which was much lower than the latencies reported by other algorithms. This advantage was attributed to the dynamic update mechanism of the algorithm proposed by the research, which could quickly identify and handle abnormal nodes within a short period of time, thereby significantly reducing transaction processing time. Furthermore, the algorithm proposed by the research also performed well in terms of system stability, reaching 97.0%, which was higher than the system stabilities reported by other algorithms. This result indicated that the algorithm proposed by the research not only had an advantage in the accuracy of anomaly detection, but also performed well in system stability and real-time performance, and could better meet the needs of cross-border small and medium-sized enterprises for transaction security and system stability in e-commerce. Compared with the research of Mishra et al. [8], although Mishra et al. emphasized the potential of BCT in reducing the cost of the traditional financial system and improving transparency, they did not provide specific anomaly detection indicators. The research proposed that by implementing a dynamic update algorithm for the blockchain network topology, not only was the accuracy of anomaly detection enhanced, but significant improvements were also achieved in latency and system stability. This, in turn, provided a more secure and efficient transaction environment for cross-border e-commerce among small and medium-sized enterprises. Furthermore, although the research by Cao et al. [10] explored the application of BCT from the perspective of economic transparency, it lacked in-depth analysis in terms of anomaly detection and system stability. The research proposed that through detailed experimental verification, the advantages of the proposed algorithm in these key performance indicators were proved.

The hardware environment used in the research was a server equipped with an Intel Xeon E5-2690 v4 processor and 128GB DDR4 memory. The runtime performance test showed that when processing the e-commerce transaction data of cross-border small and medium-sized enterprises, the average CPU usage rate of the proposed blockchain network topology algorithm was 35% and the memory usage rate was 45%. The average processing time for a single transaction was 1.8 milliseconds. In the scalability test, this algorithm could add 10 new nodes per second in a single-server environment. When extended to a distributed cluster environment, the number of new nodes per second could reach 100. However, as the number of nodes further increased, the rate of new nodes slightly decreased due to the influence of network latency and data synchronization mechanisms. This indicated that in large-scale distributed scenarios, the scalability of the algorithm had certain limitations. It is necessary to further optimize the network communication and data synchronization strategies to enhance its applicability in ultra-large-scale networks. In the field of cross-border small and medium-sized enterprise e-commerce, privacy protection, regulatory compliance and deployment implementation are the key factors to ensure the effective application of BCT. In terms of privacy protection, cross-border transactions involve the flow of data from multiple countries. It is essential to ensure compliance with the privacy regulations of each country, prevent data leakage, and at the same time guarantee the anonymity and security of user information. In terms of regulatory compliance, financial regulatory requirements vary among different countries. The proposed blockchain network topology algorithm needs to adapt to and meet these norms to ensure legal and compliant operation. During the deployment and implementation process, it is necessary to consider the compatibility of the system with the existing e-commerce architecture, operation and maintenance costs, as well as technical feasibility, to ensure that the solution can be smoothly integrated into the existing business processes.

5 Conclusion

The research aimed to enhance the security of small and medium-sized enterprises in CBEC in digital economy transactions, and proposed an abnormal node classification method and digital economy transaction security detection algorithm based on blockchain network topology dynamic update algorithm. The research designed efficient network topology dynamic update algorithms and node clustering algorithms to achieve accurate identification and classification of abnormal nodes. Meanwhile, The research used network topology analysis combined with node behavior characteristics to detect and defend against various attack behaviors. The research results showed that the blockchain network topology algorithm only took 2.5 milliseconds for transaction verification time, had a node verification success rate of 8.9%, a transaction conflict rate of only 1.7%, 3 security vulnerabilities, an attack detection delay of 0.8 milliseconds, a recovery time of 0.7 seconds, and a failure rate of 7.2%. These data were all superior to the comparison algorithms, demonstrating the superiority of the algorithm in terms of security and stability. The blockchain network topology algorithm could effectively enhance the security and stability of digital economic transactions, providing a reliable security solution for small and medium-sized enterprises in CBEC. However, the concurrent processing capability of the algorithm decreased when dealing with large-scale datasets, and further optimization is needed to adapt to the concurrent processing requirements of larger datasets. To quantify the limitation of insufficient concurrency of the algorithm when dealing with large datasets, subsequent experiments should cover different data loads, including small-scale, medium-scale and large-scale datasets, and test the concurrent processing capacity, response time and resource consumption of the algorithm under each load respectively. Through comparative analysis, the changing trend of algorithm performance with the growth of data scale can be clearly identified, providing empirical basis for optimizing the algorithm and enhancing its applicability in the big data environment.

References

[1] Mishra L, Kaushik V. Application of blockchain in dealing with sustainability issues and challenges of financial sector. Journal of Sustainable Finance & Investment, 2023, 13(3): 1318-1333. DOI:10.1080/20430795.2021.1940805.

[2] Iskamto D, Juariyah L. Blockchain technology challenge in the future: Data security and efficiency. International Journal of Law, Policy, and Governance, 2023, 2(2): 65-76. DOI:10.54099/ijlpg.v2i2.708.

[3] Guntara R G, Nurfirmansyah M N. Blockchain implementation in e-commerce to improve the security online transactions. Journal of Scientific Research, Education, and Technology (JSRET), 2023, 2(1): 328-338. DOI:10.58526/jsret.v2i1.85.

[4] Syafira T, Jackson S, Tambunan A. Fintech integration with crowdfunding and blockchain in industry 4.0 era. Startupreneur Business Digital (SABDA Journal), 2024, 3(1): 10-18. DOI:10.33050/sabda.v3i1.433.

[5] Hussain M, Ahmed R, Cheema H M. Segmented radon Fourier transform for long-time coherent radars. IEEE Sensors Journal, 2023, 23(9): 9582-9594. DOI:10.1109/JSEN.2023.3260024.

[6] Djenouri Y, Yazidi A, Srivastava G. Blockchain: Applications, challenges, and opportunities in consumer electronics. IEEE Consumer Electronics Magazine, 2023, 13(2): 36-41. DOI:10.1109/MCE.2023.3247911.

[7] Abdin Z. Empowering the hydrogen economy: The tr ansformative potential of blockchain technology. Re newable & sustainable energy reviews, 2024, 200(Au g.):114572.1-114572.17. DOI:10.1016/j.cie.2024.11 0548.

[8] Mishra L, Kaushik V. Application of blockchain in dealing with sustainability issues and challenges of financial sector. Journal of Sustainable Finance & Investment, 2023, 13(3): 1318-1333. DOI:10.1080/20430795.2021.1940805.

[9] Liu Y, Fang Z, Cheung M H, Cai W, Huang J. Mechanism design for blockchain storage sustainability. IEEE Communications Magazine, 2023, 61(8): 102-107. DOI:10.1109/MCOM.001.2200809.

[10] Cao J. Evaluation of Cross-border E-commerce Economic and Trade Data Management Device Based on Blockchain Technology. Journal of Internet Technology, 2025, 26(1):137-145. DOI:10.70003/160792642025012601012.

[11] Christodoulou I, Rizomyliotis I, Konstantoulaki K, Nazarian A, Binh D. Transforming the remittance industry: harnessing the power of blockchain technology. Journal of Enterprise Information Management, 2024, 37(5): 1551-1577. DOI:10.1108/JEIM-03-2023-0112.

[12] Cai T, Chen W, Psannis K E, Goudos S K, Yu Y, Zheng Z, Wan S. Scalable on-chain and off-chain blockchain for sharing economy in large-scale wireless networks. IEEE Wireless Communications, 2022, 29(3): 32-38. DOI:10.1109/MWC.004.2100616.

[13] Adewale T T, Olorunyomi T D, Odonkor T N. Blockchain-enhanced financial transparency: A conceptual approach to reporting and compliance[J]. International Journal of Frontiers in Science and Technology Research, 2022, 2(1): 024-045. DOI:10.53294/ijfstr.2022.2.1.0027.

[14] Xu M, Ren X, Niyato D, Kang J, Qiu C, Xiong Z, Leung V C. When quantum information technologies meet blockchain in web 3.0. IEEE Network, 2023, 38(2): 255-263. DOI:10.1109/MNET.134.2200578.

[15] Khatwani R, Mishra M, Bedarkar M, Nair K, Mistry J. Impact of blockchain on financial technology innovation in the banking, financial services and insurance (BFSI) sector. Journal of Statistics Applications and Probability, 2023, 12(1): 181-189. DOI:10.18576/jsap/120117.

[16] Demirel E, Karagöz Zeren S, Hakan K. Smart contracts in tourism industry: a model with blockchain integration for post pandemic economy. Current Issues in Tourism, 2022, 25(12): 1895-1909. DOI:10.1080/13683500.2021.1960280.

[17] Silva E C, Mira da Silva M. Research contributions and challenges in DLT-based cryptocurrency regulation: a systematic mapping study. Journal of Banking and Financial Technology, 2022, 6(1): 63-82. DOI:10.1007/s42786-021-00037-2.

[18] Bhosle K, Musande V. Evaluation of Deep Learning CNN Model for Recognition of Devanagari Digit. Artificial Intelligence and Applications, 2023, 1(2): 114-118. DOI:10.47852/bonviewAIA3202441.

[19] Xiao Y, Xu L, Zhang C, Zhu L, Zhang Y. Blockchain-empowered privacy-preserving digital object trading in the metaverse. IEEE MultiMedia, 2023, 30(2): 81-90. DOI:10.1109/MMUL.2023.3246528.

[20] Alshar'e M, Abuhmaidan K, Ahmed F Y H, Abualkishik A, Al-Bahri M, Yousif J H. Assessing blockchain's role in healthcare security: a comprehensive review. Informatica, 2024, 48(22). DOI:10.31449/inf.v48i22.6155.