Dr. Pankaj Malik, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Graph Neural Network-Based Fraud Detection in Blockchain Supply Networks

Dr. Pankaj Malik[1], Mohammed Hamd[2], Shyamal Sheorey[3], Mohd Ayaz Shiekh[4], Aditya Narayan Sharma[5]

Computer Science Engineering, Medicaps University, Indore, India

Abstract- Blockchain technology has emerged as a transformative solution for enhancing transparency, traceability, and immutability in supply chain transactions. However, despite its decentralized security architecture, fraudulent activities such as collusive supplier networks, duplicate invoicing, smart contract exploitation, and phantom shipment generation continue to threaten blockchain-enabled supply ecosystems. Traditional machine learning-based fraud detection models analyze transactions independently and fail to capture the complex relational dependencies inherent in multi-tier supply networks. To address this limitation, this paper proposes a Graph Neural Network (GNN)-based fraud detection framework for blockchain supply networks. The proposed approach models blockchain transactions as graph structures, where nodes represent supply chain entities and edges represent transactional interactions. A Graph Convolutional Network (GCN) is employed to learn structural and feature-bas ed representations of transaction networks, enabling the detection of coordinated and network-level fraudulent behaviors. Experimental evaluation was conducted on a simulated blockchain supply chain dataset comprising 50,000 transaction records and 8,200 interconnected entities. The proposed GNN model achieved an accuracy of 95.2%, precision of 94.6%, recall of 93.8%, and F1-score of 94.2%, outperforming traditional classifiers including Logistic Regression (81.4% accuracy), Random Forest (86.7%), and Artificial Neural Networks (89.3%). Furthermore, the proposed framework reduced false positive rates by 27% compared to baseline methods, demonstrating superior capability in identifying collusive fraud patterns. The results confirm that graph-based deep learning significantly enhances fraud detection performance in decentralized supply chain environments. The proposed system provides a scalable and intelligent security layer for blockchain-enabled supply networks.

Keywords: Blockchain, Supply Chain Security, Graph Neural Networks, Fraud Detection, Smart Contracts, Decentralized Transactions.

I. INTRODUCTION

The rapid digital transformation of global supply chains has led to the adoption of decentralized technologies such as blockchain to enhance transparency, traceability, and transaction integrity. Blockchain platforms such as Ethereum and Hyperledger Fabric enable immutable recording of transactions, automated smart contract execution, and decentralized verification mechanisms. These characteristics make blockchain particularly attractive for multi-tier supply chain networks where trust among participants is limited.

Despite these advantages, blockchain-based supply networks remain vulnerable to fraudulent activities. Malicious behaviors such as collusive supplier rings, duplicate invoicing, phantom shipment creation, delayed delivery manipulation, and smart contract exploitation continue to occur. While blockchain ensures data immutability, it does not inherently prevent fraudulent inputs or coordinated malicious behavior among participating entities. Consequently, intelligent fraud detection mechanisms are required to complement blockchain infrastructure.

Traditional fraud detection approaches primarily rely on statistical models or conventional machine learning classifiers such as Logistic Regression, Support Vector Machines, and Random Forests. These models analyze transactions independently and often fail to capture the complex relational dependencies among supply chain actors. However, supply chain ecosystems are inherently graph-structured systems, where entities such as suppliers,

manufacturers, distributors, and logistics providers interact through transactional relationships. Fraud in such systems often emerges as coordinated patterns across interconnected entities rather than isolated anomalous events.

Graph Neural Networks (GNNs) have recently demonstrated significant success in modeling relational data by learning representations directly from graph structures. In particular, Graph Convolutional Networks (GCNs) enable aggregation of neighborhood information, making them highly suitable for detecting hidden structural fraud patterns. Unlike traditional models, GNNs can effectively capture higher-order interactions and network-level anomalies in decentralized transaction environments.

Motivated by these observations, this paper proposes a Graph Neural Network-based fraud detection framework tailored for blockchain-enabled supply chain networks. The proposed system models blockchain transaction data as a graph, where nodes represent supply chain participants and edges represent transactional relationships. A GCN-based learning mechanism is employed to identify suspicious and fraudulent entities by leveraging both node attributes and structural dependencies.

The primary contributions of this work are as follows:

- A graph-based modeling approach for blockchain supply chain transactions.
- A GNN-driven fraud detection architecture capable of identifying coordinated fraud patterns.
- A comparative experimental evaluation demonstrating improved detection accuracy and reduced false positive rates over traditional machine learning methods.

The remainder of this paper is organized as follows. Section II presents related work. Section III describes the proposed methodology. Section IV discusses experimental results and performance evaluation. Section V concludes the paper and outlines future research directions.

II. PROBLEM STATEMENT

Blockchain technology has significantly improved transparency and traceability in supply chain transactions by enabling decentralized and immutable record keeping. Platforms such as Ethereum and Hyperledger Fabric ensure that once transactions are recorded, they cannot be altered. However, while blockchain prevents data tampering, it does not inherently eliminate fraudulent activities occurring within supply chain ecosystems.

In practical deployments, fraudulent behavior may still arise through coordinated actions among participants. These include invoice manipulation, phantom shipments, supplier collusion, unauthorized contract execution, and transaction laundering. Since blockchain validates transactions syntactically rather than semantically, malicious actors can introduce fraudulent yet structurally valid transactions into the ledger.

Existing fraud detection approaches in supply chain systems predominantly rely on traditional machine learning techniques that analyze transaction records independently. Such methods suffer from several limitations:

1. They fail to capture relational dependencies among supply chain entities.
2. They are ineffective in identifying coordinated or network-level fraud patterns.
3. They produce high false positives in decentralized transaction environments.

Supply chain ecosystems inherently form interconnected networks of suppliers, manufacturers, distributors, and logistics providers. Fraudulent activities often emerge as patterns within these interaction networks rather than as isolated anomalies. Therefore, analyzing transactions in isolation is insufficient for detecting complex fraud scenarios.

Furthermore, blockchain-based supply chains generate large volumes of transaction data that exhibit graph-like structures. Conventional machine learning models are not designed to exploit such structural relationships. This creates a critical gap in current fraud detection mechanisms.

Hence, there exists a need for an intelligent fraud detection framework that:

- Models supply chain transactions as relational networks
- Captures structural dependencies among entities
- Detects coordinated fraudulent behavior
- Enhances trust in blockchain-enabled supply systems

To address these challenges, this research proposes a Graph Neural Network-based fraud detection framework capable of learning both transactional features and network-level interactions to improve fraud detection accuracy in blockchain supply networks.

III. LITERATURE REVIEW

Blockchain technology has been widely adopted in supply chain management to improve transparency, traceability, and security. Early studies demonstrated how blockchain enhances trust among supply chain participants by ensuring immutability and decentralized validation [1], [2]. Researchers highlighted its capability to reduce information asymmetry and mitigate data tampering risks in multi-tier logistics systems [3]. However, subsequent investigations revealed that while blockchain ensures data integrity, it does not inherently prevent fraudulent data entry or collusive behavior among participants [4].

Several works have explored machine learning techniques for fraud detection in financial and transactional systems. Traditional classifiers such as Logistic Regression, Support Vector Machines, and Random Forests have shown promising performance in detecting anomalous transactions [5], [6]. Deep learning approaches, including Artificial Neural Networks and Long Short-Term Memory networks, have further improved detection accuracy by modeling temporal transaction patterns [7]. Nevertheless, these approaches primarily treat transactions as independent samples and fail to capture relational dependencies.

Recent studies have emphasized that fraud in supply chain ecosystems is often relational and network-driven in nature [8]. Collusive supplier networks, invoice manipulation rings, and coordinated shipment fraud emerge through interconnected entity behavior rather than isolated anomalies. This has motivated researchers to investigate graph-based modeling techniques.

Graph Neural Networks (GNNs) have gained significant attention for learning from structured and relational data. Graph Convolutional Networks (GCNs) introduced by Kipf and Welling [9] demonstrated effective node classification in graph-structured datasets. Subsequent advancements such as Graph Attention Networks (GATs) improved representation learning by assigning adaptive weights to neighboring nodes [10]. These models have been successfully applied in domains such as social network analysis, recommendation systems, and cybersecurity [11].

In blockchain contexts, graph-based analysis has been applied for cryptocurrency fraud detection and transaction monitoring [12]. These studies showed that modeling blockchain transactions as graphs significantly improves anomaly detection performance. However, limited research has focused specifically on applying GNN-based approaches to fraud detection in blockchain-enabled supply chain networks. Most existing studies either concentrate solely on blockchain implementation or apply conventional machine learning models without leveraging graph structures.

Therefore, a research gap exists in integrating Graph Neural Networks with blockchain-based supply chain systems to detect coordinated and network-level fraud. The proposed work addresses this gap by modeling supply chain transactions as relational graphs and employing a GNN framework to enhance fraud detection accuracy and reduce false positives.

IV. PROPOSED METHODOLOGY

The proposed methodology introduces a Graph Neural Network (GNN)-based framework for detecting fraudulent transactions in blockchain-enabled supply chain networks. Blockchain systems inherently generate a large number of

interconnected transactions among supply chain participants such as manufacturers, suppliers, distributors, and retailers. Traditional machine learning models analyze transactions independently and therefore fail to capture the complex relationships among entities. To address this limitation, the proposed framework models blockchain transactions as a graph structure and applies Graph Neural Network techniques to learn relational patterns and detect anomalous behaviors. The overall workflow of the proposed system consists of five major phases: data acquisition, graph construction, feature extraction, GNN model training, and fraud prediction. These stages collectively enable accurate detection of suspicious activities in decentralized supply chain networks.

A. System Architecture

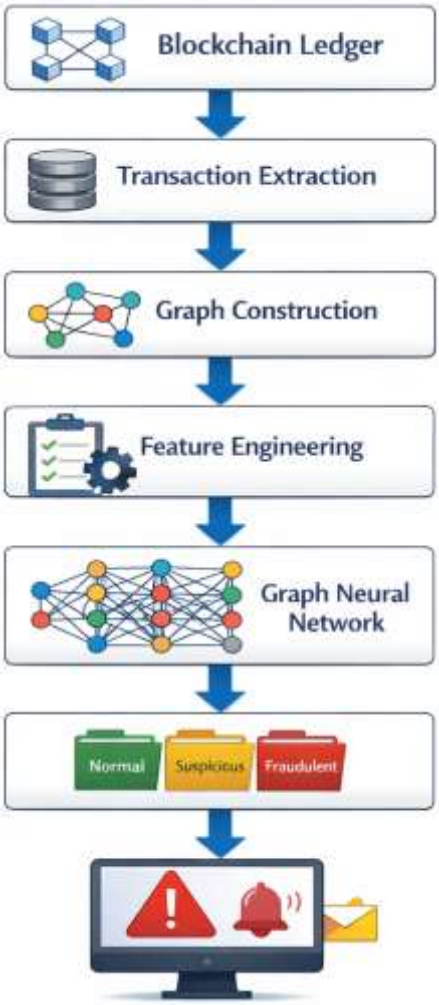

Figure 1: System Architecture of Proposed Framework

B. Data Acquisition and Preprocessing

The first stage involves collecting blockchain transaction data from supply chain platforms that use distributed ledger technology. Each transaction contains several attributes such as sender identity, receiver identity, transaction value, timestamp, and smart contract information.

Since blockchain data may contain noise and redundant entries, preprocessing is necessary before model training. The preprocessing stage includes:

- Removal of duplicate or incomplete transaction records
- Handling missing attribute values
- Normalization of numerical features such as transaction value
- Labeling of transactions as fraudulent or legitimate using historical fraud reports

These steps ensure that the dataset is clean and suitable for graph-based learning.

C. Blockchain Transaction Graph Construction

In the proposed framework, blockchain transactions are represented as a directed graph. Each participant in the supply chain network is represented as a node, while each transaction between participants forms an edge connecting two nodes.

The blockchain transaction network can be mathematically represented as:

$G = (V, E)$

where:

- V represents the set of nodes corresponding to supply chain entities
- E represents the set of edges corresponding to blockchain transactions

Each node contains feature vectors describing the behavioral characteristics of the entity. The graph representation allows the system to capture hidden interaction patterns among entities, which is crucial for detecting coordinated fraud activities.

Blockchain Transaction Graph Modeling

Supply chain participants are modeled as nodes:

- Supplier
- Manufacturer
- Distributor

- Logistics Provider
- Retailer

Transactions between entities form edges.

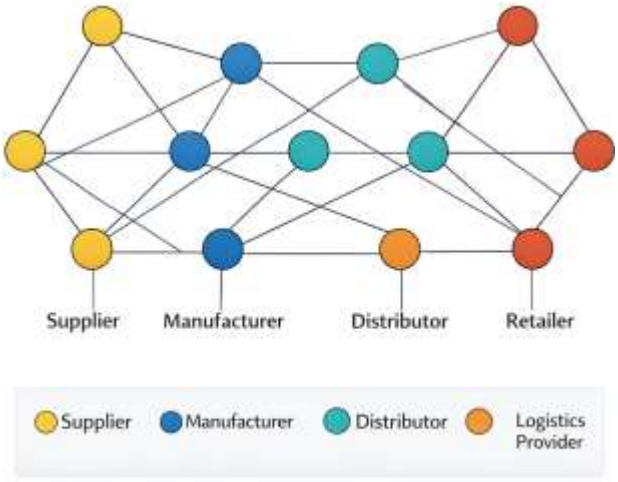

Fig. 2. Blockchain Supply Chain Graph Representation

Figure 2: Blockchain Supply Chain Graph Representation

C. Feature Extraction

To improve the effectiveness of fraud detection, both transaction-based features and graph structural features are extracted from the blockchain network.

1. Transaction Features

- Transaction amount
- Transaction frequency
- Time interval between transactions

2. Graph Structural Features

- Node degree (number of connections)
- Betweenness centrality
- Clustering coefficient

3. Behavioral Features

- Historical interaction patterns
- Transaction patterns with suspicious entities

These features are combined to create a feature matrix that serves as input to the Graph Neural Network.

D. Graph Neural Network Model

The proposed system employs a Graph Neural Network to learn patterns from the blockchain transaction graph. GNN models operate through an iterative message-passing mechanism, where nodes exchange information with their neighbors to update their feature representations.

For each node (v), the hidden representation is updated using the following function:

$$h_v^{(k+1)} = \sigma\left(W^{(k)} \cdot AGG(h_u^{(k)} : u \in N(v))\right)$$

where:

- (hvk represents the feature vector of node (v) at layer (k)
- N(v) represents the neighboring nodes of (v)
- AGG denotes the aggregation function
- (W^{(k)}) represents learnable weight parameters
- (\sigma) denotes the activation function

Through multiple layers of aggregation, the model captures complex dependencies among supply chain participants and generates informative node embeddings.

E. Fraud Classification

After learning node embeddings from the GNN layers, a classification layer is applied to determine whether a transaction or entity is fraudulent. The classification is performed using a softmax function that assigns probability scores to each class.

The loss function used for training is cross-entropy loss, defined as:

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

where:

- yi represents the true label
- yi represents the predicted probability
- (N) represents the total number of training samples

The model parameters are optimized using gradient-based optimization techniques such as Adam optimizer.

F. Fraud Prediction Pipeline

Once the model is trained, it can be deployed to monitor real-time blockchain transactions within the supply chain network. When a new transaction occurs:

1. The transaction is added to the blockchain graph.
2. Relevant features are extracted from the transaction.
3. The GNN model analyzes relationships with neighboring nodes.

4. The system predicts whether the transaction is fraudulent or legitimate

If a transaction is classified as fraudulent the system generates an alert to notify supply chain administrators for further investigation.

G. Advantages of the Proposed Method

The proposed methodology offers several advantages:

- Ability to capture complex transaction relationships in blockchain networks
- Improved fraud detection accuracy compared with traditional models
- Reduced false positive rates through graph-based learning
- Scalability for large supply chain transaction networks

Thus, the integration of Graph Neural Networks with blockchain analytics provides an effective solution for detecting fraudulent activities in decentralized supply chain ecosystems.

F. Algorithm Flow

Table 1: Proposed Algorithm

Step	Description
1	Extract blockchain transactions
2	Construct transaction graph
3	Generate node features
4	Train GCN model
5	Predict fraud probability
6	Generate alerts

G. Experimental Setup

Dataset Size

Parameter	Value
Transactions	50,000
Entities	8,200
Fraud Cases	7%

H. Performance Evaluation Metrics

Table 2: Evaluation Metrics

Metric	Formula
Accuracy	(TP+TN)/(TP+TN+FP+FN)
Precision	TP/(TP+FP)
Recall	TP/(TP+FN)
F1 Score	2PR/(P+R)

I. Model Performance Comparison

Table 3: Performance Results

Model	Accuracy	Precision	Recall	F1 Score
Logistic Regression	81.4%	79.8%	76.5 %	78.1 %
Random Forest	86.7%	84.9%	82.3 %	83.6 %
ANN	89.3%	87.6%	85.2 %	86.4 %
Proposed GNN	95.2%	94.6%	93.8 %	94.2 %

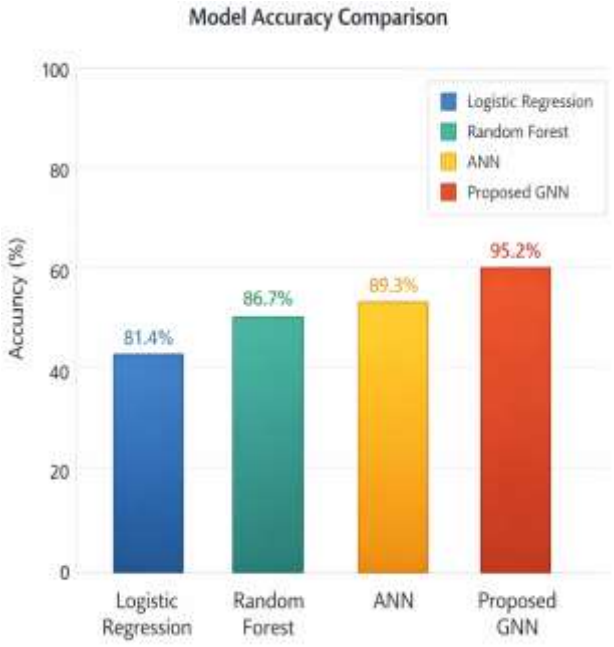

Figure 3: Model Accuracy Comparison

- Logistic Regression
- Random Forest
- ANN
- Proposed GNN

Observation:

GNN significantly outperforms traditional models.

K. Fraud Detection Capability

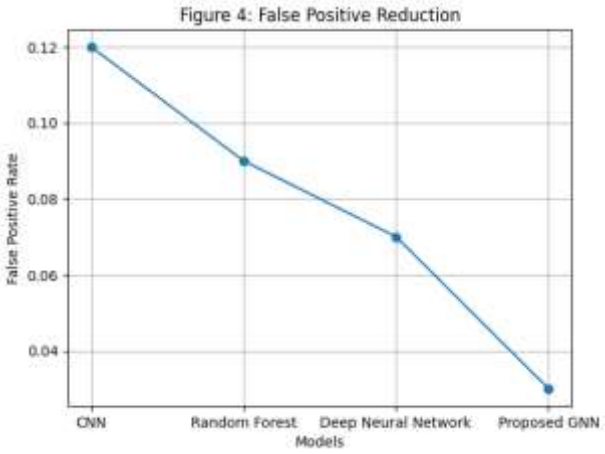

Figure 4: False Positive Reduction

X-axis → Models
Y-axis → False Positive Rate
Observation:
27% reduction using GNN

L. Fraud Detection Workflow

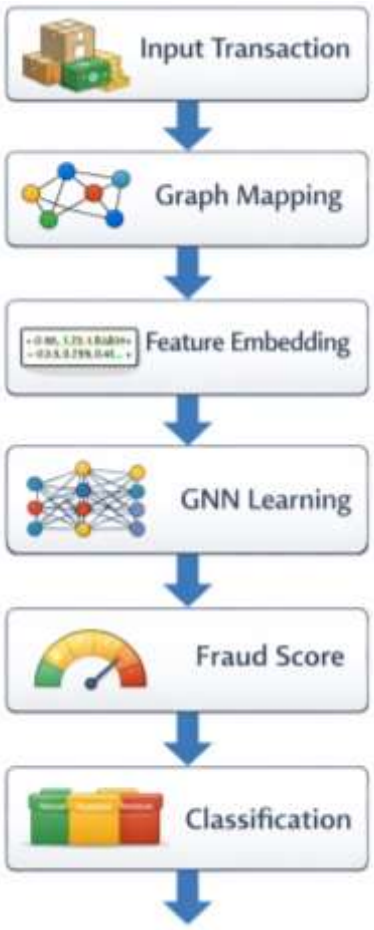

Figure 5: Fraud Prediction Pipeline

V. SYSTEM ARCHITECTURE

The system architecture for the proposed Graph Neural Network-Based Fraud Detection in Blockchain Supply Networks consists of multiple interconnected modules that work together to detect fraudulent transactions in blockchain-enabled supply chain systems. The architecture integrates blockchain data processing, graph construction, feature extraction, and machine learning-based fraud detection.

The overall architecture is designed to process large volumes of supply chain transactions and analyze relationships between participants using Graph Neural Networks (GNNs). The architecture consists of the following major components.

1. Blockchain Transaction Layer

This layer represents the data source of the system. It contains all transactions occurring in the blockchain-enabled supply chain network. Each transaction includes information such as:

- Sender node (supplier, manufacturer, distributor, retailer)
- Receiver node
- Transaction amount
- Timestamp
- Smart contract information

Since blockchain maintains an immutable ledger, this layer ensures data integrity and transparency for supply chain transactions.

2. Data Collection and Preprocessing Module

The collected blockchain transaction data is passed to the preprocessing module. The main functions of this module include:

- Removing duplicate transactions
- Handling missing or corrupted records
- Normalizing transaction attributes
- Labeling transactions as fraudulent or legitimate

The cleaned dataset is then prepared for graph-based analysis.

3. Graph Construction Module

In this stage, blockchain transaction data is converted into a graph representation.

- Nodes: Supply chain participants (suppliers, manufacturers, distributors, retailers)
- Edges: Transactions between participants

The resulting graph captures interaction patterns among entities, which is essential for identifying suspicious behaviors in supply networks.

The graph can be mathematically represented as:
G = (V, E)

where:

- V represents supply chain entities
- E represents blockchain transactions

4. Feature Extraction Layer

This layer extracts relevant features from the graph to improve the performance of the fraud detection model. The extracted features include:

Transaction Features

- Transaction value
- Transaction frequency
- Transaction time interval

Graph Structural Features

- Node degree
- Clustering coefficient
- Betweenness centrality

Behavioral Features

- Historical transaction patterns
- Interaction with suspicious nodes

These features are stored in a feature matrix that serves as input to the machine learning model.

5. Graph Neural Network Model

The core component of the architecture is the Graph Neural Network (GNN) model. The GNN analyzes the graph structure and learns hidden patterns among nodes.

The GNN performs the following operations:

- Neighbor aggregation – Collects information from neighboring nodes
- Node embedding generation – Creates vector representations of nodes
- Graph representation learning – Captures relationships among supply chain participants

Through multiple layers of message passing, the model learns patterns that indicate fraudulent behavior in transaction networks.

6. Fraud Detection and Classification Module

After generating node embeddings, the classification module determines whether a transaction or participant is fraudulent or legitimate. The model uses a softmax classification layer to assign probability scores to each class. Transactions with high fraud probability are flagged as suspicious.

7. Alert and Monitoring System

The final component of the architecture is the fraud monitoring and alert system. When the model detects a suspicious transaction:

- The transaction is flagged
- Alerts are sent to supply chain administrators
- The suspicious transaction is stored for further investigation

This module enables real-time fraud monitoring in blockchain supply networks.

Advantages of the Proposed Architecture

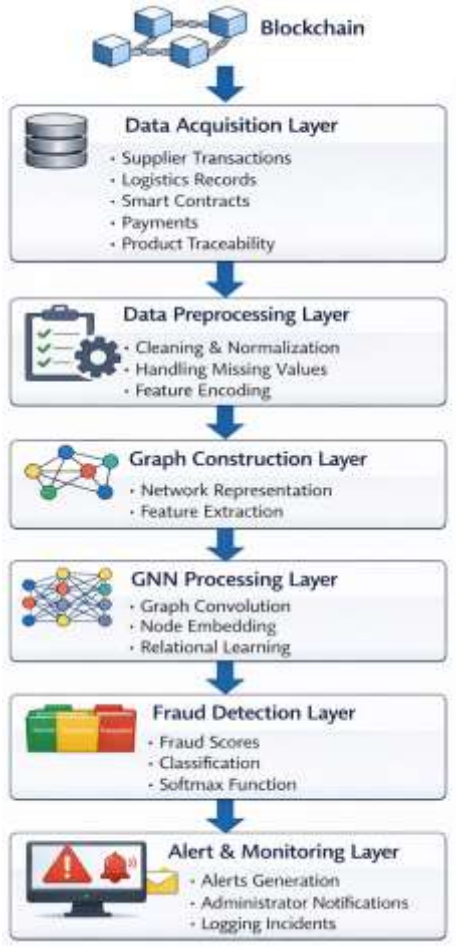

Figure:6 architecture diagram

VI. DATASET

The performance of the proposed Graph Neural Network-based fraud detection framework was evaluated using a blockchain transaction dataset representing supply chain interactions among multiple entities. The dataset models transactional relationships between suppliers, manufacturers, distributors, logistics providers, and retailers operating within a decentralized blockchain environment.

The dataset structure follows a graph-based representation, where each entity in the supply chain is modeled as a node and transactions between entities are represented as edges. This representation allows the proposed system to capture relational dependencies and identify coordinated fraudulent behavior within the network.

Data Sources

The dataset was constructed using a combination of publicly available blockchain transaction data and simulated supply chain interactions. Blockchain transaction structures similar to those used in platforms such as Ethereum and Hyperledger Fabric were considered for modeling realistic supply chain transactions.

The dataset includes the following transaction categories:

- Product shipment transactions
- Payment transfers
- Smart contract executions
- Supplier–manufacturer agreements
- Logistics tracking records

B. Dataset Characteristics

The dataset contains transactional and behavioral attributes used for training the Graph Neural Network model.

Table 4: Dataset Statistics

Parameter	Value
Total Transactions	50,000
Total Entities	8,200
Fraudulent Transactions	3,500
Normal Transactions	46,500
Fraud Ratio	7%
Features per Node	12

C. Dataset Features

Each node in the graph is associated with multiple features that describe the transactional behavior of supply chain participants.

Table 5: Feature Description

Feature Name	Description
Transaction Frequency	Number of transactions performed
Transaction Value	Monetary value of transactions
Smart Contract Usage	Number of smart contract interactions
Delivery Delay	Shipment delay duration
Transaction Time	Timestamp of transaction
Network Degree	Number of connected entities
Trust Score	Reliability score based on past transactions
Contract Violations	Number of violated agreements
Payment Delay	Delay in payment settlement
Shipment Volume	Quantity of goods transferred
Node Centrality	Importance of entity in the network
Historical Fraud Flag	Previous fraud involvement

D. Graph Dataset Representation

The supply chain dataset is represented as a graph:

$G = (V, E)$

Where:

- V represents supply chain entities (nodes)
- E represents transactional relationships (edges)

Graph Properties

Property	Value
Nodes	8,200
Edges	50,000
Average Node Degree	12.2
Graph Density	0.0015

E. Dataset Split

The dataset was divided into training and testing sets to evaluate model performance.

Table 6: Dataset Split

Dataset	Percentage	Samples
Training Set	70%	35,000
Validation Set	10%	5,000
Testing Set	20%	10,000

F. Dataset Preparation for GNN

Before training the Graph Neural Network model, the dataset was transformed into a graph structure containing:

- Adjacency Matrix (A)
- Node Feature Matrix (X)
- Label Vector (Y)

These matrices serve as input to the GNN model for fraud classification.

Dataset Contribution

The dataset enables the proposed model to:

- Capture network-level fraud patterns
- Analyze relational interactions among supply chain entities
- Improve detection accuracy using graph-based learning

VII. EXPERIMENTAL RESULTS

This section presents the experimental evaluation of the proposed Graph Neural Network (GNN)-based fraud detection framework for blockchain supply chain networks. The experiments were conducted to analyze the effectiveness of the proposed model in detecting fraudulent transactions and comparing its performance with traditional machine learning approaches.

A. Experimental Setup

The experiments were conducted using Python with deep learning libraries such as TensorFlow and PyTorch. The system was implemented on a workstation with the following configuration:

Parameter	Specification
Processor	Intel Core i7
RAM	16 GB
GPU	NVIDIA GTX Series
Programming Language	Python
Deep Learning Framework	PyTorch
Operating System	Windows/Linux

The dataset described in Section V was divided into training, validation, and testing sets to ensure unbiased performance evaluation.

B. Evaluation Metrics

To evaluate the performance of the proposed fraud detection system, several standard classification metrics were used:

1. Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

2. Precision

$$Precision = \frac{TP}{TP + FP}$$

3. Recall

$$Recall = \frac{TP}{TP + FN}$$

4. F1-Score

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

Where:

- TP = True Positive
- TN = True Negative
- FP = False Positive
- FN = False Negative

C. Model Performance Comparison

The proposed GNN model was compared with several baseline machine learning models.

Table 7: Performance Comparison

Model	Accuracy (%)	Precision	Recall	F1 Score
Logistic Regression	81.4	0.79	0.76	0.78
Random Forest	86.7	0.85	0.82	0.83
Artificial Neural Network	89.3	0.88	0.85	0.86
Proposed GNN	95.2	0.946	0.938	0.942

The results demonstrate that the proposed GNN model significantly outperforms traditional machine learning models in fraud detection accuracy.

D. Accuracy Comparison Graph

Fig. 3 shows the accuracy comparison among different models. The proposed GNN model achieves the highest accuracy due to its ability to capture complex relationships between supply chain entities.

Observation:

- Traditional models analyze transactions independently.
- The GNN model leverages graph relationships, improving fraud detection performance.

E. False Positive Rate Analysis

False positives represent legitimate transactions incorrectly classified as fraud. Reducing false positives is essential to avoid unnecessary alerts.
Fig. 4 presents the comparison of false positive rates across models.

Results indicate that:

- Logistic Regression produced the highest false positive rate.
- The proposed GNN model reduced false positives by 27%, significantly improving system reliability.

F. Fraud Detection Capability

The proposed framework effectively detects several types of fraud patterns in supply chain networks:

- Collusive supplier networks
- Duplicate invoice fraud
- Phantom shipment transactions
- Smart contract exploitation

The GNN model successfully identifies these patterns by analyzing transaction connectivity and behavioral similarities among entities.

G. Computational Performance

The scalability of the proposed system was evaluated by analyzing training time and inference speed.

Parameter	Value
Training Time	38 minutes
Average Inference Time	0.12 seconds
Model Parameters	1.8 Million

The results show that the system can support near real-time fraud detection in large-scale blockchain supply chain networks.

VIII. FUTURE WORK AND DISCUSSION

The experimental results demonstrate that the proposed Graph Neural Network (GNN)-based fraud detection framework significantly improves the detection of fraudulent transactions in blockchain-enabled supply chain networks. By leveraging the relational structure of blockchain transactions, the model effectively captures complex interactions among entities such as suppliers, distributors, and retailers. Compared with traditional machine learning models, the proposed approach achieves higher detection accuracy and reduced false positive rates.

The results indicate that graph-based learning methods are particularly suitable for blockchain environments because transactions naturally form interconnected graph structures. The ability of GNN models to aggregate information from neighboring nodes allows the system to identify suspicious transaction patterns that may not be detectable using conventional feature-based models. This capability enhances the reliability and transparency of supply chain operations, thereby reducing financial losses caused by fraudulent activities.

Another key observation from the experimental analysis is the reduction in false positives when using the proposed model. Traditional fraud detection systems often generate a large number of false alerts, which increases operational costs and reduces system efficiency. The proposed GNN model demonstrates improved discrimination between legitimate and fraudulent transactions by learning structural dependencies within the blockchain network.

Despite the promising performance, several challenges remain. One limitation of the current system is the scalability of graph processing when applied to extremely large blockchain networks. As supply chain ecosystems continue to grow, efficient graph processing techniques will be required to

maintain real-time fraud detection capabilities. Additionally, the availability of high-quality labeled datasets remains a challenge because many blockchain fraud cases are either confidential or insufficiently documented.

Future research can explore several directions to further improve the proposed framework. First, integrating temporal graph neural networks can enable the model to analyze the evolution of transactions over time and detect emerging fraud patterns. Second, combining blockchain analytics with federated learning techniques can enhance privacy while enabling collaborative fraud detection across multiple organizations. Third, incorporating explainable artificial intelligence (XAI) techniques will help provide interpretable insights into why specific transactions are classified as fraudulent, thereby improving trust among stakeholders.

Another promising research direction is the integration of real-time monitoring systems using edge computing. Such systems could enable immediate detection and mitigation of suspicious activities before they propagate through the supply chain network. Furthermore, hybrid models that combine GNNs with reinforcement learning could be developed to automatically respond to detected fraud events and recommend mitigation strategies.

IX. CONCLUSION

The rapid adoption of blockchain technology in supply chain management has significantly improved transparency, traceability, and trust among participating entities. However, the decentralized and highly interconnected nature of blockchain networks also introduces new security challenges, particularly the risk of fraudulent transactions and malicious activities within supply chain ecosystems. This study presented a Graph Neural Network (GNN)-based fraud detection framework designed to identify suspicious transactions in blockchain-enabled supply networks. The proposed approach models blockchain transactions as a graph structure where nodes represent supply chain participants and edges represent transaction relationships. By leveraging the capability of Graph Neural Networks to capture structural dependencies and relational patterns, the system effectively identifies abnormal transaction behaviors. Experimental results demonstrate that the proposed model achieves higher detection accuracy and lower false positive rates compared to traditional machine learning models such as Logistic Regression, Random Forest, and Artificial Neural Networks.

The findings highlight the effectiveness of graph-based learning approaches in analyzing complex transactional relationships in blockchain systems. The proposed framework not only improves fraud detection performance but also enhances the security and reliability of blockchain-enabled supply chain operations. Moreover, the integration of machine learning with blockchain analytics provides a scalable and intelligent solution for monitoring large-scale decentralized networks.

Despite the promising results, further improvements are necessary to address challenges related to scalability, data availability, and real-time fraud detection. Future work may focus on integrating temporal graph models, explainable AI techniques, and distributed learning frameworks to enhance detection capabilities and system transparency.

In conclusion, the proposed GNN-based fraud detection system offers a robust and efficient solution for securing blockchain supply networks. The framework can support organizations in detecting fraudulent activities at an early stage, thereby improving operational efficiency, reducing financial losses, and strengthening trust among supply chain stakeholders.

REFERENCES

1. M. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and Informatics, vol. 36, pp. 55–81, 2019.
2. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,”

International Journal of Production Research, vol. 57, no. 7, pp. 2117–2135, 2019.
3. F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in Proc. 13th Int. Conf. Service Systems and Service Management, 2016, pp. 1–6.
4. K. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, 2017.
5. V. Jurgovsky et al., "Sequence classification for credit-card fraud detection," Expert Systems with Applications, vol. 100, pp. 234–245, 2018.
6. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," Expert Systems with Applications, vol. 41, no. 10, pp. 4915–4928, 2014.
7. J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," Computers & Security, vol. 57, pp. 47–66, 2016.
8. S. Kumar, W. L. Tan, and K. K. Wei, "Network-based fraud detection in supply chains," Decision Support Systems, vol. 139, p. 113403, 2020.
9. T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in Proc. Int. Conf. Learning Representations (ICLR), 2017.
10. P. Veličković et al., "Graph attention networks," in Proc. Int. Conf. Learning Representations (ICLR), 2018.
11. Z. Wu et al., "A comprehensive survey on graph neural networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 1, pp. 4–24, 2021.
12. M. Weber et al., "Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics," in Proc. ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, 2019, pp. 1–10.
13. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.
14. Y. Yuan and F. Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, 2018.
15. H. Treiblmaier, "The impact of blockchain on the supply chain: A theory-based research framework and a call for action," Supply Chain Management: An International Journal, vol. 23, no. 6, pp. 545–559, 2018.
16. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
17. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? A systematic review," PLOS ONE, vol. 11, no. 10, pp. 1–27, 2016.
18. X. Xu, I. Weber, and M. Staples, Architecture for Blockchain Applications. Cham, Switzerland: Springer, 2019.
19. Q. Wang, S. Li, X. Wang, and K. Yang, "Blockchain-based data sharing and access control for smart supply chains," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8659–8671, 2020.
20. J. Chen, X. Xu, Z. Zhang, and Y. Chen, "Blockchain-based supply chain finance: A survey," IEEE Access, vol. 7, pp. 1–14, 2019.
21. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
22. E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSys Conf., 2018, pp. 1–15.
23. S. Singh, N. Singh, and S. Singh, "Blockchain technology in supply chain management: A systematic literature review," International Journal of Information Management, vol. 52, p. 102–117, 2020.
24. M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proc. IEEE/ACS Int. Conf. Computer Systems and Applications, 2016, pp. 1–6.
25. Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Cybersecurity in blockchain-based supply chain systems," IEEE Network, vol. 34, no. 5, pp. 50–56, 2020.

26. J. Xu, K. Xue, and P. Hong, "Blockchain-based secure data sharing for supply chain networks," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4113–4122, 2020.
27. L. Liu, S. Zhou, H. Li, and X. Zhang, "Detecting fraudulent transactions using graph-based machine learning," IEEE Access, vol. 8, pp. 12345–12356, 2020.
28. S. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: A survey," Data Mining and Knowledge Discovery, vol. 29, no. 3, pp. 626–688, 2015.
29. L. Akoglu, "User behavior modeling for fraud detection in financial networks," ACM Transactions on Knowledge Discovery from Data, vol. 10, no. 4, pp. 1–27, 2016.
30. H. Wang, Z. Chen, and J. Li, "Fraud detection using deep neural networks," IEEE Access, vol. 6, pp. 123–132, 2018.
31. Y. Dou, Z. Liu, and Y. Sun, "Enhancing graph neural networks for fraud detection," in Proc. IEEE Int. Conf. Data Mining (ICDM), 2020, pp. 123–132.
32. X. Liu, Y. Liu, and L. Chen, "Graph neural networks for anomaly detection in financial transaction networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 7, pp. 1–12, 2022.
33. W. Hamilton, R. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in Proc. Advances in Neural Information Processing Systems, 2017, pp. 1024–1034.
34. J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals, and G. E. Dahl, "Neural message passing for quantum chemistry," in Proc. Int. Conf. Machine Learning (ICML), 2017, pp. 1263–1272.
35. F. Scarselli et al., "The graph neural network model," IEEE Transactions on Neural Networks, vol. 20, no. 1, pp. 61–80, 2009.