ENHANCING BLOCKCHAIN SECURITY: A COMPREHENSIVE STUDY ON FRAUD DETECTION AND PREVENTION

*Rintu Augustine** [1], *A. Krishnaveni* [2]

ABSTRACT

Blockchain technology has revolutionized digital transactions by integrating transparent, secure, and decentralized financial systems. It is also threatened by critical vulnerabilities from defects such as Sybil attacks, selfish mining, and double-spending attacks. Researchers have explored various methods to minimize such threats, including hybrid consensus protocols, machine learning algorithms, Graph Neural Networks (GNNs), and mathematical modeling-based fraud prediction and prevention. To achieve maximum blockchain security, Meybodi introduces machine learning algorithms (SDTLA and WVBM), while Kang et al. propose a GNN-based model to precisely predict double-spending attacks. To address double-spending attacks, Akbar et al. propose a hybrid Proof-of- Work (PoW) and Proof-of-Stake (PoS), whereas Yuen et al. focus on Bitcoin Generator Scam (BGS) detection, addressing over-smoothing issues in GNNs. Other strategies for blockchain security improvement are Block Access Restriction (BAR) techniques, ECDSA-based prevention mechanisms, and Graph SAGE and Graph Attention Networks (GAT). A safer and stronger decentralized financial system is guaranteed by this research's discussion of such methods, research gaps identification, and investigation of enhancements to enhance blockchain networks' capabilities in fraud detection, scalability, and flexibility.

Keywords: Blockchain Security, Double-Spending Attack, Graph Neural Networks, Fraud Detection, Crypto currency

Department of Computer Applications[1],
Adi Shankara Institute of Engineering and Technology, Kalady, Kerala, India[1] rintu.cs@adishankara.ac.in[1]
Department of Computer Science[2],
Karpagam Academy of Higher Education, Coimbatore, India[2]
krishnaveni.arumugam@kahedu.edu.in

* Corresponding Author

I. INTRODUCTION

Blockchain technology has revolutionized digital transactions by providing transparent, secure, and decentralized financial systems. However, vulnerabilities such as Sybil attacks, selfish mining, and double-spending attacks compromise its integrity. If an attacker successfully spends the same bitcoin multiple times prior to confirmation, it is referred to as double-spending and undermines network confidence. Scholars have explored various methods to transcend these hurdles, including machine learning algorithms, hybrid consensus algorithms, Graph Neural Networks (GNNs), and mathematical modeling for enhanced fraud detection and prevention. Meybodi proposes machine learning-based methods (SDTLA and WVBM) to enhance security in blockchain, while Kang et al. propose a GNN-based model that can effectively predict double-spending attacks. While Yuen et al. focus on detecting BGS and try to solve the problem of over-smoothing in GNNs, Akbar et al. propose a hybrid PoW and PoS mechanism to prevent double-spending attacks. GraphSAGE and Graph Attention Networks (GAT), ECDSA-prevention strategies, and Block Access Restriction (BAR) approaches are other ways of improving blockchain security. In this research article, various strategies are evaluated, areas for further research are identified, and potential for enhancing the accuracy, scalability, and flexibility of fraud detection in blockchain systems is discussed.

II. LITERATURE REVIEW

Kang et al. [1] offer a GNN-based model to identify Bitcoin double-spending attacks through predicting double-spending attempts on unspent transaction outputs (UTXOs). Within a 14,000-node peer-to-peer (P2P) network, the model monitors the mempool's availability of transactions for a minimum of 150 observer nodes, with over 95% accuracy. The model allows for fast payments while identifying double-spending attempts and verifies transaction propagation. Kang et al. [1] employ the Barabasi-Albert

model to generate virtual Bitcoin networks, which they utilize to train the GNN rather than relying on the topology of a real Bitcoin network. From training 14,000-node virtual networks, the GNN classifies graphs by whether or not a node has a particular feature, such as connectedness, label, or In a peer-to-peer (P2P) network of 14,000 nodes, the model witnesses the mempool's transaction availability for at least 150 observer nodes with over 95% accuracy. The model allows for fast payments and double-spending attempts detection as well as transaction propagation checking. Kang et al.employ the Barabasi-Albert model to generate virtual Bitcoin networks, which are employed for training the GNN rather than leveraging the topology of a real Bitcoin network. Kang et al. introduce a GNN-based model to identify Bitcoin double-spending attacks by predicting double spend attempts on unspent transaction outputs (UTXOs). In a 14,000-node peer-to-peer (P2P) network, the model observes the mempool's transaction availability for at least 150 observer nodes, achieving over 95% accuracy. Fast payments are permitted by the model, which also detects double- spending attempts and checks for transaction propagation. Kang et al. employ the Barabasi-Albert model in generating virtual Bitcoin networks, upon which they train the GNN rather than employing an actual Bitcoin network's topology. Kang et al. introduce a model using a GNN for identifying Bitcoin double-spending attacks by predicting attempts to double spend unspent transaction outputs (UTXOs). Within a 14,000-node peer-to-peer (P2P) network, the model monitors the mempool's transaction availability for a minimum of 150 observer nodes with more than 95% accuracy. The model allows fast payments and double-spending attempt detection, in addition to transaction propagation checks. Kang et al. employ the Barabasi-Albert model to generate virtual Bitcoin networks, which they subsequently employ as training for the GNN rather than employing an existing Bitcoin network topology. Kang et al. introduce a GNN-based model to identify Bitcoin double-spending attacks by predicting attempts to double spend unspent transaction outputs (UTXOs) [1].

Meybodi [3] focuses on releasing two machine learning-based models, SDTLA and WVBM, which utilize learning automata to minimize the threats of selfish mining and double-spending. These models better enhance security and performance in blockchain networks, even when they do not explicitly utilize GNN algorithms, by adjusting parameters to minimize the risk of double-spending. To effectively resist selfish mining attacks on blockchain networks, Meybodi[3] presents two learning automata-based methods: SDTLA (Selfish Mining Defense with Learning Automata) and WVBM (Weighted Value-Based Model). The SDTLA method increases the profitability requirement for selfish mining by up to 47%.The Z Parameter of the SDTLA and WVBM methods is tunable to reduce double-spending attack risks, rendering blockchain networks safer and more efficient.

Machine learning-based fraud serves to effectively enhance security and performance in blockchain networks, even if they do not make an explicit use of GNN algorithms, through parameter tuning to reduce double-spending probabilities. WVBM (Weighted Value-Based Model) and SDTLA (Selfish Mining Defense based on Learning Automata) are two machine learning-based methods Meybodi[3] introduces to effectively counter selfish mining attacks in blockchain networks. The SDTLA method increases the profitability level of selfish mining by up to 47%.

Use of GNNs to detect Bitcoin Generator Scams (BGS) is the main subject of Yuen et al. [5], and they also address concerns, such as over-smoothing in GNNs. Though not specifically addressing double spending attacks, Yuen et al. [5] suggest using Random Walk Positional Encoding (RWPE) and propose the General, Powerful, Scalable (GPS) Graph Transformer to enhance the detection of BGS. Detection of Bitcoin transactions related to Bitcoin Generator Scams (BGS) using traditional machine learning (ML) approaches and graph neural networks (GNNs) is investigated by Yuen et al. [3]. It emphasizes GNNs' issues, notably the over-smoothing issue, and presents Random Walk Positional Encoding (RWPE) as a method to effectively represent long-range interactions. Yuen et al. [5] evaluate the performance of various graph sampling methods, specifically rather than being explicitly directed against

double spending attacks, Yuen et al. [5] recommend applying Random Walk Positional Encoding (RWPE) and introduce the General, Powerful, Scalable (GPS) Graph Transformer to strengthen BGS detection. Yuen et al. [5] investigate the application of both classical machine learning (ML) techniques and graph neural networks (GNNs) towards the identification of Bitcoin transactions linked to Bitcoin Generator Scams (BGS). It puts into perspective the issues that GNNs encounter, namely, the over-smoothing problem, and presents Random Walk Positional Encoding (RWPE) as an approach to effective long-range interaction capturing.

In order to prevent double spending, Akbar et al. [6] implemented a hybrid approach that combines the Proof-of-Work (PoW) and Proof-of-Stake (PoS) paradigms. By requiring full network control and preventing double mining, it aims to enhance security by reducing the probability of successful double-spending attacks. By merging the two consensus mechanisms by forking, the hybrid approach suggested by Akbar et al. [6] integrates Proof-of-Work (PoW) and Proof-of-Stake (PoS) processes to enhance security against double-spending attacks. The research makes it more difficult for attackers to gain full control of the network, which reduces the possibility of double mining and remedies weaknesses in existing consensus techniques, particularly the 51% attack. Hybrid consensus methods have been recognized as effective strategies, such as integrating PoW and PoS. It attempts to enhance security by avoiding double mining and demanding full network control, which reduces the chances that double-spending attacks would be successful. Akbar et al. [6] propose a hybrid solution integrating Proof-of-Work (PoW) and Proof-of-Stake (PoS) processes to enhance security against double-spending attacks by blending the two methods of consensus together through forking. The study reduces the risk of double mining and also corrects the weaknesses in existing consensus algorithms, particularly the 51% attack, by making it difficult for the attackers to take full control of the network. Akbar et al. [6] proposed a hybrid approach that fused the Proof-of-Work (PoW) and Proof-of-Stake (PoS) schemes to prevent double spending. It attempts to enhance security by inhibiting double mining and requiring absolute control over the network, which reduces the likelihood that double-spending attacks would succeed. Akbar et al, 2021 introduced a hybrid approach combining Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms to prevent double-spending. This method aims to strengthen security by preventing double mining and ensuring full control over the network, thereby lowering the chances of successful double-spending attacks.

Although they focus on GraphSAGE and Graph Attention Network (GAT) for classifying behavior in Bitcoin and Ethereum networks, Jeyakumar et al[8] provide no recommendations on mitigating double spending attacks. Rather, it attempts to identify malicious transactions by investigating relationships between smart contracts and wallets using Graph Neural Networks (GNN). The method focuses on identifying malicious participants through the examination of the smart contract and wallet relationships, visualizing the topological blockchain network from graph data.

Jeyakumar et al[8] utilizes a combination of heterogeneous Graph Neural Network (GNN) models, specifically GraphSAGE and Graph Attention Network (GAT), to investigate the behavior of Bitcoin and Ethereum networks through a generalized graph structure. According to Farrugia et al. [9], rather than using GraphSAGE and GAT, the method aims to detect malicious transactions by mapping the relationships between smart contracts and wallets using Graph Neural Networks (GNN).The method focuses on identifying malicious parties through examining the relationships between smart contracts and wallets, utilizing graph information for depicting the topological structure of the blockchain network. Pérez-Solà et al. [10] propose a double-spending prevention method for zero-confirmation transactions that leverages the Bitcoin programming language and exploits vulnerabilities in the ECDSA signature system. This approach allows for penalizing attackers by revealing their secret keys if a double-spending attempt occurs, effectively preventing such attacks in fast-payment situations.

In [10], Pérez-Solà et al. 2017 [10] introduced a double-spending prevention system for Bitcoin zero-confirmation

payments by creating special spendable transaction outputs spendable with one signature. But if two different signatures for the same output become known, the private key used to sign the transaction is revealed, and anyone who observes can make a third transaction spending the same output. The method causes network users to become observers that can detect double-spending attempts. This system enables punishers to expose attackers' secret keys if a double-spending attempt occurs, thereby deterring such attacks in fast-payment scenarios. Pérez-Solà et al. [10] propose a double-spending prevention mechanism for Bitcoin zero-confirmation payments by creating special spendable transaction outputs that require only a single signature to be spent.

Xing & Chen[11] emphasizes Block Access Restricted (BAR) mechanism, which governs block requests and identifies malicious activities, thus maintaining miners' rights and maintaining equity in the blockchain network. Xing & Chen[7] pinpoint the importance in addressing security vulnerabilities, particularly in the context of post-quantum computing. To protect the rights of miners and ensure fairness in the blockchain network, Xing & Chen[11] propose a Block Access Restriction (BAR) system that controls legitimate block requests and detects malicious behavior while transactions are being recorded in a specific block. Apart from explaining how this method can prevent Double Spending Attacks (DSA) even when a hacker attempts to bypass it, it offers step-by-step guidelines for deploying the BAR switch within blockchain networks.

In their latest model of attack, Zhang & Lee [12] integrate double-spending with a Sybil attack and study how the attacker can use delays in block propagation to improve the likelihood of winning the race. Rather than keeping an emphasis on mitigation techniques such as GNNs, this research focuses on the economic implications of a unified model of attack and the mathematical probability of a successful attack. Zhang & Lee[8] describe how an attacker can implement a double-spend attack in conjunction with a Sybil attack on the Bitcoin network to control block propagation latency and boost their probability of success at the mining race. For this combination scheme, Zhang & Lee [8] develop a mathematical framework to calculate the probability of success. Then they perform an economic analysis. Different from mitigation measures such as GNNs, this research looks at the economic impact of a joint attack model and the mathematical probability of a successful attack. Zhang & Lee[8] describe how a double-spend attack coupled with a Sybil attack on the Bitcoin network can be used by an attacker to manipulate block propagation latency and gain an advantage in the mining race.

III.ANALYSIS OF BLOCKCHAIN SECURITY SOLUTIONS

Existing Solutions	Methodology	Attacks Handled	Success Rate	Practical Implementation
Kang et al. [1]	Graph Neural Network (GNN) with Barabasi-Albert model	Double-spending attacks	Over 95%	Predicts attempts at double spending using virtual Bitcoin networks and observer nodes.
Meybodi[2]	Machine learning-based models (SDTLA and WVBM)	Selfish mining, double-spending attacks	Up to 47% (for selfish mining)	Adjusts parameters in blockchain networks to reduce risks of selfish mining and double-spending.
Yuen et al. [3]	GPS Graph Transformer and RWPE	Bitcoin Generator Scams (BGS)	Not specified	Identifies BGS using graph neural networks and improved sampling strategies like RFS.
Akbar et al. [4]	Hybrid PoW and PoS mechanisms	Double-spending attacks, 51% attack	High	Integrates PoW and PoS consensus protocols to reduce vulnerabilities like double mining.
Jeyakumar et al.[5]	GraphSAGE and Graph Attention Network (GAT)	Malicious transactions	Not specified	Detects malicious parties by exploring smart contracts and wallets relationships.

Pérez-Solà et al.[6]	ECDSA-based double-spending prevention system	Double-spending attacks	High	Exposes secret keys of attackers during zero-confirmation transactions to deter double-spending.
Xing & Chen[7]	Block Access Restriction (BAR) mechanism	Double-spending attacks	High	Regulates block reque sts and identifies malicious activity to maintain equity among miners.
Zhang & Lee[8]	Mathematical modeling	Double-spending with Sybil attack	Calculated probabilistically	Explores economic feasibility of combination attacks, focusing on block propagation delays.

The above table identifies a few existing methodologies for mitigating attacks against blockchain, along with details of the type of threats they address, their success rates, and actual implementations. Kang et al. utilize a Graph Neural Network (GNN) based on the Barabasi-Albert model to predict double-spending attempts in virtual Bitcoin networks with a success rate of more than 95%. To avoid selfish mining and double-spending, Meybodi introduces machine learning-based algorithms (SDTLA and WVBM), which achieve 47% success rate for selfish mining. With graph neural networks and advanced sampling algorithms, Yuen et al. utilize GPS Graph Transformer and RWPE to detect Bitcoin Generator Scams (BGS). Akbar et al. integrate hybrid Proof-of-Work (PoW) and Proof-of- Stake (PoS) methods to effectively prevent 51% and double-spending attacks. Jeyakumar et al. utilize GraphSAGE and Graph Attention Network (GAT) to detect malicious software. Kang et al. apply a Graph Neural Network (GNN) based on the Barabasi-Albert model to predict double-spending attempts in virtual Bitcoin networks, achieving a success rate exceeding 95%. To combat selfish mining and double-spending, Meybodi employs machine learning algorithms (SDTLA and WVBM), with a 47% success rate against selfish mining. Yuen et al. use graph neural networks combined with advanced sampling techniques, applying GPS Graph Transformer and RWPE to identify Bitcoin Generator Scams (BGS). Akbar et al. integrate hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) schemes to effectively defend against 51% and double-spending attacks. The table summarizes several existing approaches to mitigating blockchain-based attacks, detailing the types of threats addressed, success rates, and practical implementations.

IV. RESEARCH GAP AND FUTURE SCOPE

Their lack of ability to cover dynamic transaction patterns and node significance is the principal research shortcoming in Graph Convolutional Networks (GCNs) for detecting blockchain fraud. Through the use of set weights to summarize neighborhood information, standard GCNs can overlook small variations in fraudulent behavior. A major limitation is that, there is no adaptive edge weighting available, which could enhance the sensitivity of fraud discovery by adding transaction frequency or money amounts. GCNs are also difficult to scale in large blockchain networks since node representations become indistinguishable with the over-smoothing effect of deeper layers. By bridging this gap, more accurate fraud detection algorithms that can handle complex blockchain transactions will be generated.

V. CONCLUSION

To summarize, several methods have been researched to mitigate attacks related to blockchain technology, namely Bitcoin Generator Scams (BGS), selfish mining, and double-spending. Although Graph Neural Networks (GNNs) are highly accurate in detecting fraudulent transactions, scalability challenges, identification of dynamic transaction patterns, and over-smoothing remain. Other approaches are provided by machine learning-based models like SDTLA and WVBM, but they have to be optimized further for higher rates of success. While hybrid consensus methods, such as a

combination of Proof-of-Work (PoW) and Proof-of-Stake (PoS), hold the potential to enhance security, they have to be tested empirically in real-world blockchain environments. Additionally, while economic feasibility analysis and mathematical modeling identify vulnerabilities within blockchain networks, they do not present tangible remedies. Increasing GCN-based fraud detection using temporal understanding, adaptive edge weighting, and hybrid learning methods is the prime area of research requirement. While Graph Neural Networks (GNNs) have demonstrated high accuracy in detecting fraudulent transactions, challenges such as scalability, detecting dynamic transaction patterns, and over-smoothing persist. Alternative approaches are provided by machine learning models like SDTLA and WVBM, though they require further fine-tuning to achieve higher success rates. While hybrid consensus methods like the merge of Proof-of-Work (PoW) and Proof-of-Stake (PoS) guarantee security enhancements, they need empirical validation in real-world blockchain environments.

REFERENCES

[1] Kang, C., Woo, J., & Hong, J. W. K. (2023). Bitcoin Double-Spending Attack Detection using Graph Neural Network. IEEE ICBC 2023.

[2] Hassan, M. U., Rehmani, M. H., & Chen, J. (2023). Anomaly Detection in Blockchain Networks: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 25(1), 289-318.

[3] Ghoreishi, S. A., & Meybodi, M. R. (2023). New intelligent defense systems to reduce the risks of Selfish Mining and Double-Spending attacks using Learning Automata.

[4] Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach. Engineering, Technology & Applied Science Research, 14(1), 12822-12830

[5] Yuen, Z., Branco, P., Chew, A., Jourdan, G., Lim, F. Y. C., & Wynter, L. (2023). Are GNNs the Right Tool to Mine the Blockchain? The Case of the Bitcoin Generator Scam. IBM Research.

[6] Akbar, N. A., Muneer, A., ElHakim, N., & Fati, S. M. (2021). Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. Future Internet, 13(11), 285.

[7] Bains, P. (2022). Blockchain Consensus Mechanisms: A Primer for Supervisors. International Monetary Fund.

[8] Jeyakumar, S. T., Yugarajah, A. C. E., Hou, Z., & Muthukkumarasamy, V. (2024). Detecting Malicious Blockchain Transactions Using Graph Neural Networks. Springer.

[9] Farrugia, S., Ellul, J., & Azzopardi, G. (2020). Detection of Illicit Accounts Over the Ethereum Blockchain. Expert Systems with Applications, 150, 113318.

[10] Pérez-Solà, C., Delgado-Segura, S., Navarro-Arribas, G., & Herrera-Joancomartí, J. (2017). Double-spending Prevention for Bitcoin zero-confirmation transactions.

[11] Lin, X., Zhang, Y., Huang, C., Xing, B., Chen, L., Hu, D., & Chen, Y. (2023). An Access Control System Based on Blockchain with Zero-Knowledge Rollups in High-Traffic IoT Environments. Sensors, 23(3443).

[12] Zhang, S., & Lee, J.-H. (2019). Double-spending with a Sybil Attack in the Bitcoin Decentralized Network. IEEE Transactions on Industrial Informatics.