International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 11 | Nov - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Blockchain Fraud Detection System

Yawar Hafiz Bin Taj
BE-Computer science, Chandigarh university. Department of Computer Science,Chandigarh University
21BCS11706@cuchd.in

Abhimanyu Kalia
BE-Computer science, Chandigarh university. Department of Computer Science,Chandigarh University
21BCS11714@cuchd.in

Satwik Shukla
BE-Computer science, Chandigarh university. Department of Computer Science,Chandigarh University
21BCS11701@cuchd.in

Anu priya
BE-Computer science, Chandigarh university. Department of Computer Science,Chandigarh University
e17025@cumail.in

***Abstract*—Blockchain fraud detection overcomes difficulties regarding electronic contract exploits, double-spending, and phishing crimes, among additional vulnerabilities in blockchain systems. The combined application of deliberation processes, machine learning, and real-time monitoring boosts protection and detects fraudulent activity in decentralized networks. This system provides an effective barrier against fraud in supply chain, electronic asset executives, and finance by ensuring data authenticity and openness while limiting the involvement of people.**

Keywords— Blockchain , fraud, detection, real-time, attacks, machine learning.

I. INTRODUCTION

Blockchain technology, while serves as a decentralized, open reliable platform, has entirely altered how information and interactions are administered. Blockchain systems are remain susceptible to a scam, involving double-spending, Sybil attacks, and smart contract exploitation, without any built-in safety precautions. Because the Blockchain systems are spread out and unchanging, it is difficult for them to identify criminal activity and traditional ways of fraud detection are not as successful. In reaction, machine learning (ML) has evolved into an effective tool to catch blockchain system fraud. Machine learning computations are capable of finding inconsistencies and unusual behaviour in real-time through looking at transaction structures, behaviour among users, and network activity. Blockchain technology and machine learning come forces to form an effective strategy that boosts fraud detection via mechanisation and analytical prediction while also preserving data integrity. In answer, blockchain fraud detection using machine learning (ML) has grown into an effective instrument Real-time anomalies and suspicious activity can be quickly recognised by machine learning models through the analysis of transaction patterns, behaviour of users, and activity on the network. A solid approach that guarantees data integrity and improves the detection of fraud with automation and analytical forecasting develops when blockchain technology and machine learning get merged.

II. RELATED WORK

A. Anomaly Detection in Blockchain Networks

Chen et al. (2020) Presented a framework for anomaly detection, using machine learning in identifying improper blockchain transactions. The approach was on peculiar patterns of activity on the cryptocurrency markets. The authors applied auto-encoders and clustering, two unsupervised learns closer to identify anomalies and fraudulent activities. Their technology could detect transactions that might be questionable but not reported by conventional methods.

B. Smart Contract Fraud Detection

Li et al. (2019) Developed an algorithm using machine learning to identify vulnerabilities in smart contracts using Ethereum. The system classifies agreements based on the likelihood of those agreements having weaknesses through supervised learning using neural networks, SVM decision tree models. They showed that, by using machine learning, fraudulent or other malicious contracts may be reliably detected.

C. Machine Learning in Cryptocurrency Fraud Detection

Jiang et al. (2021)- The task explored the possibility of using machine learning techniques to detect fraudulent transactions in cryptocurrencies through the utilization of supervised approaches such as random forest and gradient boosting. In this paper, the model was able to identify legitimate and fraudulent transactions by focusing on the pump-and-dump scheme within cryptocurrency trading platforms.

D. Consensus Mechanisms and Machine Learning

Sharma and Liu (2020)- Developed a novel way of incorporating Proof of Stake (PoS) consensus treatments into the system with the help of machine learning. The devices tracked patterns of voting together with node performance to identify persons who made attempts to break the consensus. Effective detection of malicious activity set a new standard for network security at large.

E. Blockchain Fraud Detection with Deep Learning

Wu et al. (2020)- Examined time-series blockchain transaction information using deep learning models including recurrent neural networks (RNN) and neural networks with convolution (CNN). The framework exhibited real-time fraud detection abilities correctly recognizing established and fresh scam inclinations.

F. Comparative Studies

Pham et al. (2021)-To detect anomalies in transactions carried on the blockchain, impartial comparison of many statistical models-such as, unsupervised woods, neural

network models and even support vector machine-was performed. As they found out, the results showed that where high accuracy and recall have to be achieved for fraud detection ensemble methods like random woodlands and gradient enhancement excelled other independent systems.

III. Methodology

1. Double-Spending Attack

An individual may conduct a double-spending attack via constantly employing an identical cryptocurrency token, and taking advantage of the blockchain's latency in transaction confirmation. The security mechanism of the blockchain is being undermined by this type of attack.

In the beginning stages of Bitcoin, some of the most popular happenings included researchers who found that double-spending may go unnoticed in the absence of an established consensus process. Afterwards, double-spending assaults, in which adversaries used 51% attacks to seize custody of the majority of the blockchain's computing power, went ahead against a number of Bitcoin forks, especially Bitcoin Gold.

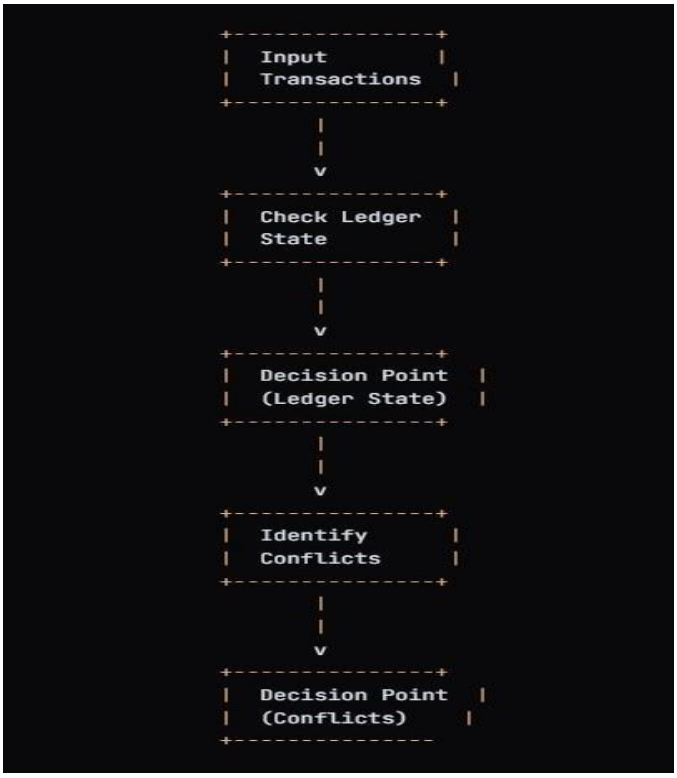

Fig .1 Double spending attack detection.

1.1 Detection Mechanism

In order to identify irregularities in transaction data, such as numerous contradictory transactions coming from a single place, machine learning models will be trained.

Detection Formula: Let:

- Ti be the set of transactions from a given user.
- Ci be the set of confirmed transactions at time t.

For a double-spending attack:

$$\sum_{T_i}(t < C_i) > 1$$

1.2. Model for Double-Spending Attack

Supervised Learning Models: To decide if a transaction appears erroneous Random Forests, supervised Decision Trees, and Gradient Boosting are utilized.

Evaluation Metrics: The model's performance is evaluated with the following metrics: the F1-s Confusion Matrix, accuracy, precision, and Remember.

**Machine-learning algorithms identify attempts to use the same data in multiple spends and watch unverified transactions in concert of the Proof of Work (PoW) confirmation technique to avoid double-spending.*

2. Sybil Attack

Establishing multiple imaginary identities with the goal to obtain overwhelming influence over a network is known as a Sybil assault. Sybil attacks, because they relate to blockchain technology, aim at disrupting consensus mechanisms through the proliferation of nodes in order to overrun reliable ones and tamper with the verification of transactions. This has been particularly significant for consensus mechanisms employing Proof of Stake (PoS) and Proof of Work (PoW).

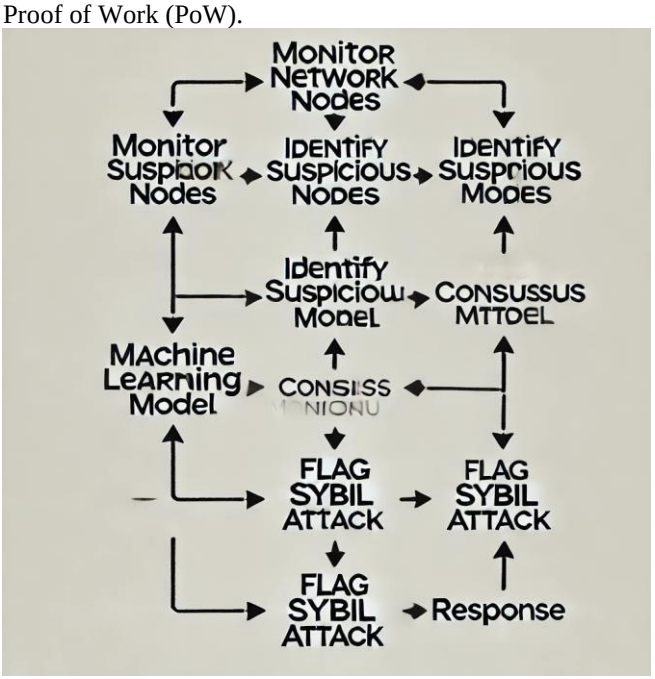

Fig.2 Sybil attack detection.

2.2. Detection Mechanism

In networks where evil nodes have been built to vote against legitimate nodes in agreement, Sybil assaults often take place. Machine learning may identify common voting behaviors or collusion between nodes by dividing IP addresses and analyzing voting behavior among nodes.

Detection Formula: Let:

- Ni represent the number of nodes a user controls.

- Vi represent the voting power each node has in the system.
- A Sybil attack is detected if:

$$\sum_{V_i \times N_i} > \theta$$

2.3. Model for Sybil Attack

Unsupervised Learning Models: By monitoring node actions, clustering methods like K-means and DBSCAN can be used to identify nodes who are colluding.

Metrics for evaluation include the Adapted Rand Index (ARI) to assess clustering results, Silhouette rating, and Cluster Integrity.

IV. CONCLUSION

As a result of the data and methods for blockchain fraud detection analysis, it is clear that even while blockchain technology offers decentralized security, it is still susceptible to attacks like double-spending and Sybil attacks. By allowing for the real-time study and identification of anomalous patterns in transaction and node behavior, machine learning integration greatly improves fraud detection capabilities. While unsupervised clustering methods work well for minimizing Sybil attacks, supervised models are useful for detecting instances of double-spending. This strategy is a strong answer for changing fraud strategies in blockchain networks since it decreases false positives and negatives while simultaneously increasing accuracy and scalability. The success of blockchain systems against emerging threats requires regular changes to these machine learning models as they expand.

REFERENCE

1. Zohar, A. "Bitcoin: An Innovative Alternative Digital Currency." 21st International Conference on Financial Cryptography and Data Security*, 2015.

2. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., & Felten, E. W. "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." 36th IEEE Symposium on Security and Privacy, 2015.

3. Eyal, I., & Sirer, E. G. "Majority is Not Enough: Bitcoin Mining is Vulnerable." 18th International Conference on Financial Cryptography and Data Security, 2014.

4. Conti, M., Kumar, C., Lal, C., & Ruj, S. "A Survey on Security and Privacy Issues of Bitcoin." 25th International Conference on Internet of Things, Big Data, and Security (IoTBDS), 2018.

5. Yu, F. R., Zhang, Y., Yang, L., & Xiao, W."Blockchain-Based Consensus Algorithms and Protocols: A Survey." *IEEE International Conference on Communications (ICC)*, 2019.

6. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. "A Survey on the Security of Blockchain Systems." 29th IEEE International Conference on Communications (ICC), 2018.

7. Kiffer, L., Rajaraman, R., & Shelat, A. "A Better Method to Analyze Blockchain Consistency." 26th ACM Conference on Computer and Communications Security (CCS), 2017.

8. Monrat, A. A., Schelén, O., & Andersson, K. "A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities." IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2019.

9. Nguyen, G. T., & Kim, K. "A Survey about Consensus Algorithms Used in Blockchain." IEEE International Conference on Information Networking (ICOIN), 2018.

10. Rossi, A., & Zhou, Y. "The Challenges of Sybil Attacks in Blockchain-Based Applications." 26th International Conference on Network Protocols (ICNP), 2019.