ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.03
October-2023
Pages: 979-985

A NEW BITCOIN TRANSACTION NETWORK ANALYTIC METHOD FOR FUTURE BLOCK-CHAIN FORENSIC INVESTIGATION

***MR.PRABHAKAR GUDISE**
*Assistant Professor, Dept. Of CSE**, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, TELANGANA**, India
V. KEERTHI[1], O. CHANDANA[2], P. REVATHI[3], P. ANJALI[4]
B. Tech Pursuing, Department of CSE**, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN,** TELANGANA, India.

ABSTRACT:

Abstract In recent years, the application of virtual currency has become a part of people's life. The decentralization and anonymity of Bitcoin have made it a favorite tool for many criminals. Therefore, how to trace illegal activities in Bitcoin transactions has become one of the most important research areas. This paper systematically collects 25 research results in this field since 2018, and divides them into three areas, i.e., supervised learning, unsupervised learning, and topological analysis. The supervised learning method based on machine learning is the current mainstream in this research field. However, we believe that the model can achieve more accurate results after combining unsupervised learning and topological analysis features. Moreover, topology analysis can help to observe the entire or specific part of the bitcoin trading network from a macro perspective so as to discover the hidden illegal activities. In addition, data visualization techniques can provide structural insights to understand the bitcoin trading network.

KEY TERMS : Bitcoin, Flow Analysis, Review

1 INTRODUCTION：

Since its inception, the popularity of cryptocurrencies has risen, and now its application is ubiquitous. Bitcoin, as a founder, has a larger number of related application fields and users, but there are also criminals who are interested in using it for illegal purposes, such as illegal transactions on the dark web, money laundering, etc. There are still many regions that have not yet formulated clear regulatory norms for Bitcoin, so criminals can easily engage in money laundry regarding its decentralization, anonymity, and fast

transactions. In traditional crimes, illegal money flow tracing technology focuses on the time, amount, and locations where customers deposit or withdraw money from the bank to identify their abnormal behavior. Once the abnormal behavior has been detected, the bank can lock the account and provide the account owner's information to law enforcement agencies (LEAs) for further investigation. However, in Bitcoin transactions, it is difficult to directly identify the true owner of the account address. Therefore, the application of traditional cash flow tracking technology faces great challenges. How to trace the illegal money flow generated by Bitcoin money laundry has become a critical issue for LEAs. Although Bitcoin greatly hinders the investigation of tracking the money flow, its public ledger can also provide transparent transaction records, and by analyzing these transaction records, law enforcement agencies also have the opportunity to track down unlawful crimes. Bitcoin transaction records contain many features, such as transaction time, input wallet address, output wallet address, etc. How to select important features for subsequent analysis is an important topic. In related studies, possible features, such as cash deposits in different bank branches within a short time frame, transfers to accounts on which there are no other transactions or bank drafts cashed in for foreign currency, are adopted to detect money laundry; however, as far as our knowledge, rare research provide a comprehensive review of money laundry investigation strategy for cryptocurrency. In this paper, we proceed with a systematic review of this field and provide an architecture to demonstrate state-of-the-art algorithms for detecting cryptocurrency laundry

2.LITERATURE REVIEW :

1.1.TITLE: A Novel Methodology for HYIP Operators' Bitcoin Addresses Identification

Bitcoin is one of the most popular decentralized cryptocurrencies to date. However, it has been widely reported that it can be used for investment scams, which are referred to as high yield investment programs (HYIP). Although from the security forensic point of view it is very important to identify the HYIP operators' Bitcoin addresses, so far in the open technical literature no systematic method which reliably collects and identifies such Bitcoin addresses has been proposed. In this paper, a novel methodology is introduced, which efficiently collects a large number of the HYIP operators' Bitcoin addresses and identifies them based upon a novel analysis of their transactions history. In particular, a scraping-based method is first proposed which is able to collect more than 2,000 HYIP operators' Bitcoin addresses from the Internet thus providing a large number of the HYIPs' samples. Second, a supervised machine learning technique, which classifies, whether or not, specific Bitcoin addresses belong to the HYIP operators, is introduced and its performance is evaluated.

1.2.TITLE: competence of graph convolutional networks for anti-money laundering in bitcoin blockchain

Graph networks are extensively used as an essential framework to analyse the

interconnections between transactions and capture illicit behaviour in Bitcoin blockchain. Due to the complexity of Bitcoin transaction graph, the prediction of illicit transactions has become a challenging problem to unveil illicit services over the network. Graph Convolutional Network, a graph neural network based spectral approach, has recently emerged and gained much attention regarding graph-structured data. Previous research has highlighted the degraded performance of the latter approach to predict illicit transactions using, a Bitcoin transaction graph, so-called Elliptic data derived from Bitcoin blockchain. Motivated by the previous work, we seek to explore graph convolutions in a novel way.

For this purpose, we present a novel approach that is modelled using the existing Graph Convolutional Network intertwined with linear layers. Concisely, we concatenate node embeddings obtained from graph convolutional layers with a single hidden layer derived from the linear transformation of the node feature matrix and followed by Multi-layer Perceptron. Our approach is evaluated using Elliptic data, wherein efficient accuracy is yielded. The proposed approach outperforms the original work of same data set.

3.EXISTING SYSTEM:

In traditional crimes, illegal money flow tracing technology focuses on the time, amount, and locations where customers deposit or withdraw money from the bank to identify their abnormal behavior. Once the abnormal behavior has been detected, the bank can lock the account and provide the account owner's information to law enforcement agencies (LEAs) for further investigation. There are still many regions that have not yet formulated clear regulatory norms for Bitcoin, so criminals can easily engage in money laundry regarding its decentralization, anonymity, and fast transactions.

4.PROPOSED SYSTEM:

This paper systematically collects 25 research results in this field since 2018, and divides them into three areas, i.e., supervised learning, unsupervised learning, and topological analysis. The supervised learning method based on machine learning is the current mainstream in this research field.

However, we believe that the model can achieve more accurate results after combining unsupervised learning and topological analysis features. Moreover, topology analysis can help to observe the entire or specific part of the Bitcoin trading network from a macro perspective so as to discover the hidden illegal activities. In addition, data visualization techniques can provide structural insights to understand the Bitcoin trading network.

5.SYSTEM ARCHITECTURE:

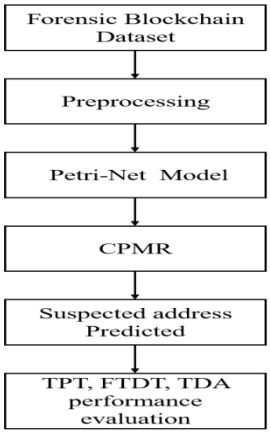
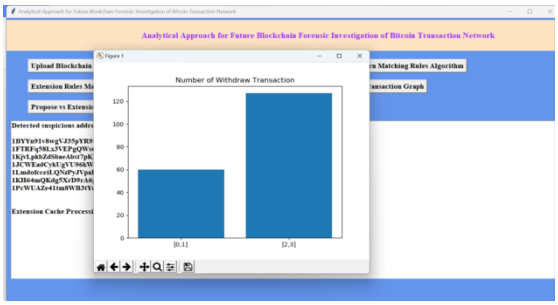


Fig:System Architecture

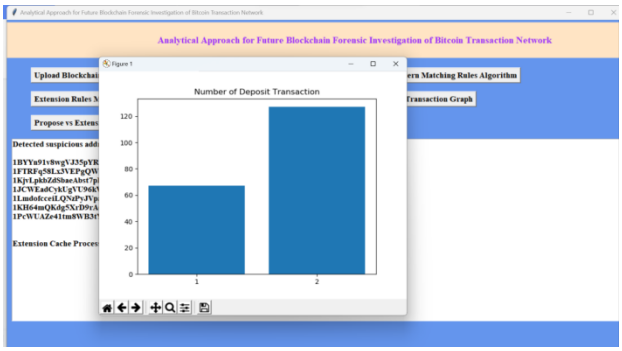
6. RESULT:

In above screen showing list of all suspected account details with invalid addresses. Now click on 'Withdraw Transaction Graph' button to view all withdraw transaction from different accounts

In above screen with extension Cache it took 0.0044 seconds to processes all transaction and now click on 'Propose vs Extension Graph' button to get below execution time graph



In above screen x-axis represents total withdraw from account 0 to 1 and vice versa and y-axis represents number of gather addresses for that withdrawal. Now click on 'Deposit Transaction Graph' button to get below graph.



In above screen x-axis represents number of account ID and y-axis represents number of deposit transaction made by that account

7. CONCLUSION: Cryptocurrency has the characteristics of decentralization,

transparency, and immutability. The number of users and related applications of cryptocurrency will only become more popular. However, this trend also encourages criminals to conduct illegal transactions on the dark web or money laundering. However, the nature of the cryptocurrency public ledger opens another door for LEAs to identify illicit activity in the Bitcoin trading network. In this paper, we applied an objective and systematic method to obtain 25 works of literature related to the identification of illegal activities in the Bitcoin trading network. The articles are divided into three categories, i.e., supervised learning, unsupervised learning, and topology. Supervised learning and unsupervised learning are techniques based on machine learning, and topology-based are techniques based on graph theory. By summarizing the algorithms in 3 aspects of the application, future researchers can more easily understand the current research stream in this field. Although the references which adopt the topology-based algorithm are fewer than the other two categories, we believe that the use of graph theory in Bitcoin flow analysis will be an important research direction.

8.REFERENCES:

[l] 1. Toyoda, K., P. Takis Mathiopoulos, and T. Ohtsuki, A Novel Methodology for HYIP Operators' Bitcoin Addresses Identification. IEEE Access, 2019. 7: p. 74835-74848.

2. Chang, T.H. and D. Svetinovic, Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020. 50: p. 9-20.

3. Nan, L. and D. Tao. Bitcoin mixing detection using deep autoencoder. in Proceedings - 2018 IEEE 3rd International Conference on Data Science in Cyberspace, DSC 2018. 2018. IEEE.

4. Shao, W., et al. Identifying bitcoin users using deep neural network. in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2018.

5. Wu, J., et al., Detecting Mixing Services via Mining Bitcoin Transaction Network With Hybrid Motifs. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021. 52(4): p. 2237-2249.

6. Kanemura, K., K. Toyoda, and T. Ohtsuki. Identification of Darknet Markets' Bitcoin Addresses by Voting Per-Address Classification Results. in ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency. 2019.

7. La Morgia, M., et al. Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations. in Proceedings - International Conference on Computer Communications and Networks, ICCCN. 2020.

8. Liang, J., et al. Targeted addresses identification for bitcoin with network

representation learning. in 2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019. 2019.

9. Alarab, I., S. Prakoonwit, and M.I. Nacer. Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. in ACM International Conference Proceeding Series. 2020.

10. Nerurkar, P., et al., Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020). Journal of Network and Computer Applications, 2021. 177.

AUTHOR

Mr.Prabhakar Gudise Assistant Professor Department of CSE MallaReddy Engineering College for Women, Hyderabad,prabhakarm.tech@gmail.com.