Decrypting Criminal Transaction Patterns in Cryptocurrency

Sawanya Rattanabunno, Warodom Werapun
College of Computing, Prince of Songkla University, Kathu, Phuket
{s6430621003, warodom.w}@phuket.psu.ac.th

2023 7th International Conference on Information Technology (InCIT) | 979-8-3503-5869-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/InCIT60207.2023.10413019

Abstract— **This paper introduces an approach to detect a thief's wallet by analyzing linked transactions connected to centralized exchanges mandating KYC verification. The proposed methods are designed to provide valuable insights into the intricate flow of funds and the behavioral patterns of malicious actors, explicitly focusing on thieves. By inputting a thief's wallet address, our analysis examines associated transactions, capturing vital details such as the amount of Ethereum (ETH) transferred and all related transactions, including those involving ERC-20 tokens. The primary objective is comprehending the money flow among different addresses, emphasizing wallets interacting with centralized exchanges. By monitoring the movements of ETH and ERC-20 tokens, this analysis aims to identify suspicious transactions and uncover behavioral patterns indicative of illicit activities. Leveraging this analytical approach, we can track the thief's identity, making a substantial contribution to the prevention and detection of cryptocurrency theft, thus ensuring the security of blockchain ecosystems.**

Keywords—wallet address, flow of funds, Thief, Ethereum, Blockchain

I. INTRODUCTION

Cryptocurrencies and decentralized applications (dApps) based on blockchain technology have brought numerous advancements to various industries. However, the rising popularity of cryptocurrencies has also attracted cyber criminals, increasing cryptocurrency-related crimes. Ethereum, one of the most widely used blockchain platforms, has witnessed its share of criminal activities, such as theft, fraud, and money laundering. Understanding the behavior of thieves and tracking their actions is essential in preventing such illegal practices and ensuring the security and integrity of the Ethereum ecosystem [1].

The behavior of thieves can offer valuable insights into their methods of operation, enabling the identification of patterns and strategies they employ to carry out their illegal activities. One effective way of tracking these criminals is through their wallet addresses, which are used to store and transfer stolen digital assets. Exchanges, where many thieves attempt to cash out stolen funds, often require users to complete Know Your Customer (KYC) procedures. KYC is a verification process to confirm customer identities and prevent fraud in business and finance. This requirement allows connections between the thieves' wallet addresses and real-world identities.

Studying the behavior of cryptocurrency thieves' is crucial for detecting and preventing cybercrime. Our previous work [2] analyzed USDT transactions over several days. The main difference between the aforementioned paper and this work is the experiment periods, including transaction patterns. In this paper, we extend our work [2] by investigating the activities of six thieves' wallet addresses and analyzing their transaction patterns in several months of ETH transferring. Our primary objective is to trace the origins and destinations of transactions occurring from these thieves' wallet addresses until they reach any exchange wallet that can reveal their identities.

This paper is organized as follows. Section 2 presents a literature review. Section 3 describes our proposed system. The evaluation and experiment results are illustrated in Section 4. Eventually, we conclude our work in Section 5.

II. LITERATURE REVIEW

This section introduces various research and analysis on related topics in the context of blockchain security. It covers the behavior of malicious transactions, specifically thief transactions, and explores the concept of mixing transactions to enhance privacy and anonymity in blockchain networks.

A. Understanding Ethereum Value Scamming

In recent years, the increasing popularity and adoption of Ethereum have attracted not only legitimate users but also malicious actors seeking to exploit the platform for their gain. As a result, the value scamming in Ethereum has become a matter of concern for researchers and practitioners alike. Several studies have been conducted to understand the motivations, strategies, and impacts of value scammers in the Ethereum ecosystem. One such study was conducted by Martinez et al. in 2021 [3]. Through interviews and analysis of scamming campaigns, they examined factors such as financial incentives, psychological manipulation, and the exploitation of trust to gain insights into the methods employed by value scammers. Smith et al. comprehensively analyzed value scamming techniques in Ethereum in 2019 [4]. Their investigation covered various deceptive practices, including fake token sales, Ponzi schemes, and investment scams, aiming to provide a deeper understanding of the tactics used by value scammers and their effects on Ethereum users. Johnson et al. (2019) [5] conducted a data-driven approach to identify scammers in the Ethereum network. By analyzing transaction patterns, wallet addresses, and network behavior, they sought to detect potential scammers and classify their activities. The research offered valuable insights into the characteristics and strategies employed by these malicious actors.

B. Thief Transaction Behavior

Understanding the behavior of thieves in cryptocurrency transactions is crucial for detecting and preventing cybercrime [6]. By studying the origin and destination of transactions from thieves' wallet addresses, we can analyze their

transaction behavior and gain valuable insights. This analysis helps us predict their preferred strategies for transferring money and improve cybersecurity measures to prevent such activities. By gathering data on thieves' transactions and studying their behavior, we can enhance our understanding and take proactive steps to strengthen cybersecurity. E. Garcia et al. [7] analysis of transactions reveals that thieves often transfer funds to Binance, a popular digital currency exchange. C. Lee and M. Clark [8] observed that thieves tend to hold the stolen funds in their wallets for approximately ten months after the attack. This extended holding period raises questions about their motivations and intentions. Possible reasons include concerns about financial consequences or the intention to utilize the funds during upcoming festive periods towards the end of the year.

C. *Mixing Transactions*

Mixing transactions [9], known as coin mixing, tumbling, or shuffling, intentionally obscure cryptocurrency transactions to enhance privacy and anonymity. The purpose is to break the link between sender and receiver addresses, making it difficult to trace the flow of funds and identify the original source or destination of the cryptocurrency. Mixing transactions plays a crucial role in enhancing the privacy and anonymity of the Bitcoin network. The CoinJoin [10] algorithm, proposed by Maxwell G. in 2013 [11], is a widely adopted coin-mixing technique that enables users to collaborate and sign the same transaction. CoinJoin achieves its goal by merging and splitting coins or consolidating multiple transactions, obfuscating the trail of individual coins, and making tracking the flow of funds challenging. While coin mixing techniques like CoinJoin can be used for legitimate purposes, they can also be misused for illicit activities, highlighting the importance of detection and analysis in cryptocurrency.

D. *Money Laundering*

Money laundering [12][13] using cryptocurrencies has become increasingly prevalent, and cryptocurrencies have revolutionized financial transactions while opening up new avenues for cybercrime. Understanding the behavior of criminals engaged in cryptocurrency transactions is crucial for detecting and preventing cybercrime [14]. Analyzing the origins and destinations of transactions from the thief's wallet addresses provides valuable insights to anticipate their strategies for money transfers and enhance cybersecurity measures. Additionally, studying mixed transactions that obfuscate the flow of funds in digital currency transactions plays a significant role in increasing privacy and anonymity within the network, such as in the case of Bitcoin.

III. Propose Solution

We gather all related transactions using a blockchain analysis tool for token tracing and transaction visualization. It helps track and analyze blockchain data, revealing patterns behind crypto addresses for enhanced transparency and security. This section presents the proposed solution as follows.

A. *Analysis tool: Bitquery*

There are several blockchain analysis tools, such as Bitquery [15], Chainalysis [16], Nansen [17], and Dune [18]. However, most blockchain analysis tools are paid services and not publicly accessible. Bitquery is a blockchain data analytics platform that allows users to access and analyze data related to various blockchains such as Bitcoin, Ethereum, Binance Smart Chain, and more. Its open access is available for a free account, which is sufficient for this experiment for visualizing transactions. It provides deep insights into essential data like transaction history and wallet addresses. The key advantage of Bitquery is its ability to provide detailed and extensive blockchain data [19], showing data analytics and visualization to explore and analyze information effectively. It presents data in user-friendly graph formats, making it easy to understand and interpret. Moreover, Bitquery prioritizes security and reliability, ensuring users a safe and trustworthy platform. In Fig. 1, users can access the Bitquery platform. They can choose the blockchain they are interested in analyzing, such as Bitcoin, Ethereum, Binance Smart Chain, or others. Bitquery connects to the selected blockchain and retrieves relevant data, such as transaction history and wallet addresses. The retrieved data is then analyzed and presented in a graph format for transaction data analysis.

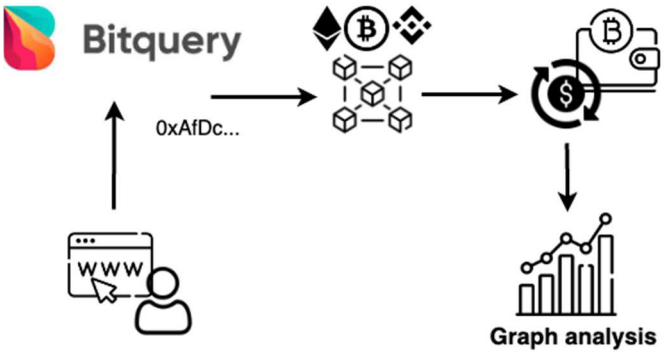

Fig.1 Data gathering and visualization

B. *Methodology and token tracing*

We have gathered ten thieves' wallet addresses, which are used to cheat money from victims, from the Provincial Police Region 8 in Thailand. We examine their money transfer patterns. Our goal is to locate and monitor the thieves during their financial activities while tracking the trends of their transactions until they reach an exchange, which requires KYC processes. To achieve this, we study the transaction history and trace the flow of tokens between the ten thieves. However, only six thieves are detected by reaching an exchange. By analyzing transactions linked to the thieves' wallet addresses, we can follow the movement of the stolen tokens.

From the graph (Fig. 2), Bitquery can be utilized to gain insights into the behavior and pathways of the thief's transactions. By employing these tools, investigators can effectively track and analyze the movements of stolen tokens. Bitquery offers the capability to input the thief's wallet information and examine the transaction pathways associated with it. This system provides detailed information about the movement of funds within the wallet, encompassing transactions, inflows, outflows, and overall money flow. The graphical representation, such as a graph or Sankey diagram (Fig. 3), helps visualize the transaction pathways, enabling investigators to identify trends and draw valuable conclusions.

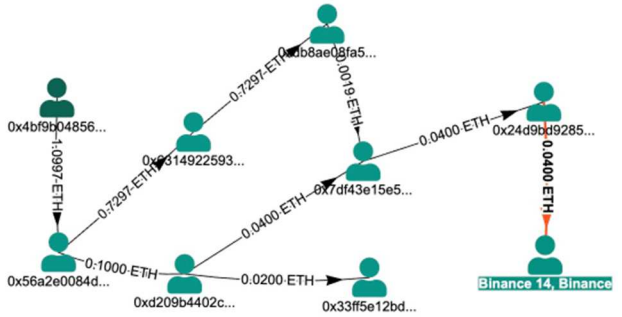

Fig.2 Transaction analysis of the thief's activities

C. *Transaction visualization*

After obtaining the wallet address of the thief, we retrieve all relevant transactions as shown in Fig. 2. It is linked to various wallets such as 0x4bf9.., indicating the complete transaction path from the source with transactions leading to the destination, connecting to the currency exchange (i.e., Binance). The transaction process is presented in a graphical format to provide a more precise visualization.

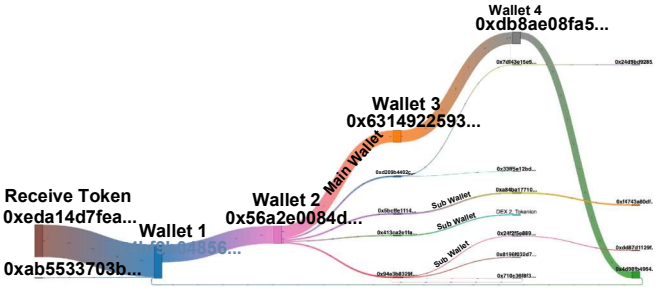

Fig 3: Transaction visualization using BitQuery

Graph of the thieves' transaction (Fig. 3) can be explained as follows: thieves receive ETH from suspicious wallets and then transfer it to Wallet 1. From there, it is distributed to Wallet 2 and other wallets, including both main wallets (accumulating of wallet1, walet2, etc.) and sub-wallets. This distribution is done to scatter the transactions and transfer ETH to Binance for conversion into fiat.

TABLE I. TRANSACTIONAL BEHAVIOR OF SIX THIEVES

ETH Address	*Transaction*	*Total ETH*
0xEDa14d7feA0f71CCd27ebb8513D1047AC28190f4	336	1.52
0xae5eecf5181ce96728ca788053248f5c7796243d	58	0.63
0xef8214b47992706a030279d676a90bc70254592d	296	2.54
0x4996C17349b9F54e5a988C112b78D803d7e16226	292	0.23
0xa385a72f1bf55b7f9460dd61443615dd21ec5e4f	44	0.014
0x4bF9B04856911F3Ee67Bc665C7A702ECFF8aE9B4	179	1.182

We analyze the transactional behavior of six thieves showing in Ethereum (ETH) transactions. By studying their activities, we aimed to gain insights into their transaction paths and better understand their behavior. To facilitate our analysis, we utilized Table 1, which provides a summary of their Ethereum transactions, including the associated ETH addresses, the number of transactions processed, and the total amount of ETH available.

IV. EVALUATION AND EXPERIMENTAL RESULTS

In this section, we present the evaluation of our tracking method for monitoring and analyzing the transaction patterns in the Ethereum network. We conducted experiments using real-world data to assess the effectiveness and accuracy of our approach.

A. *Experiment results*

We examine the transaction history and pathways of six thieves in the Ethereum (ETH) network by analyzing their transactions monthly. These thieves transfer ETH to various wallets, like conducting transactions through a regular banking application. The stolen ETH has the purpose of being exchanged and traded for digital coins on Binance, which allows us to examine the transaction behavior of the thief. We now have the wallet addresses of this thief, enabling us to investigate their transaction patterns and visualize them using graphs.

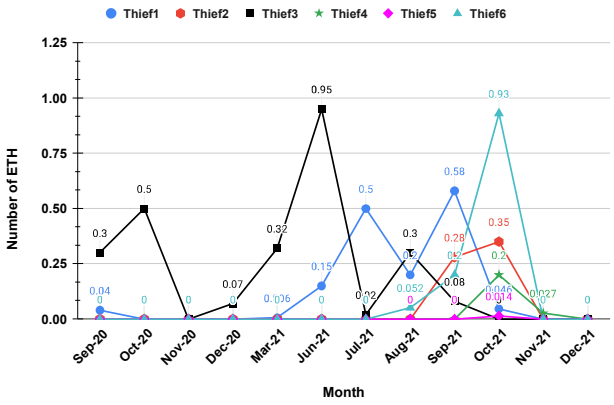

Fig 4: The amount of ETH transferred

An analysis of the transaction behavior of thieves on Binance reveals consistent transfer patterns, particularly with a significant increase in thief-initiated transactions in the June 2021 and October 2021 periods, as shown in Fig. 4. During these specific periods, thieves can transfer stolen money much faster compared to other months when transaction activity is either minimal or completely absent. Our investigation found that Thief1 transferred 1.52 ETH tokens, dividing the transfers into two intervals. The first occurred in June-August 2021, with a transfer of 0.85 ETH, and the second took place in September 2021, with a transfer of 0.58 ETH. Similarly, Thief3 transferred around 2.54 ETH tokens in two distinct periods, specifically during the mid and late years. This pattern suggests that their token transfers may be driven by significant economic expenses during the middle and end of the year, prompting them to withdraw funds to cover these costs. Dividing the transfers into two monthly intervals helps reduce suspicion related to large withdrawals and instills confidence in their trading or investment activities while minimizing associated risks. In addition, Thief2, Thief4, Thief5, and Thief6 also exhibited specific transfer strategies. They tended to opt for shorter transfers and chose intervals towards the end of the year. Thief6, for instance, transferred 1.182 ETH, which was not a substantial amount, and preferred transfers in August - September 2021, possibly to mitigate risk. They often made smaller token transfers. As a result, they chose to transfer tokens from their wallets towards the end of the year, between September and October 2021, to avoid potential taxes or financial scrutiny. This end-of-year transfer

strategy is commonly used to reduce financial risks, especially during uncertain market periods, where investments may carry more significant uncertainty, and hackers may attempt to minimize such risks.

Furthermore, analysis has identified that approximately 98% of ETH coins are transferred to the destination address (i.e., Binance) in all transactions. This finding provides valuable insights into the nature of these transactions.

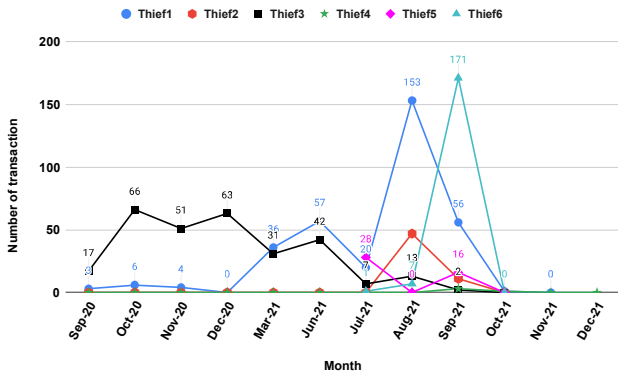

Fig 5: The number of ETH transaction counts

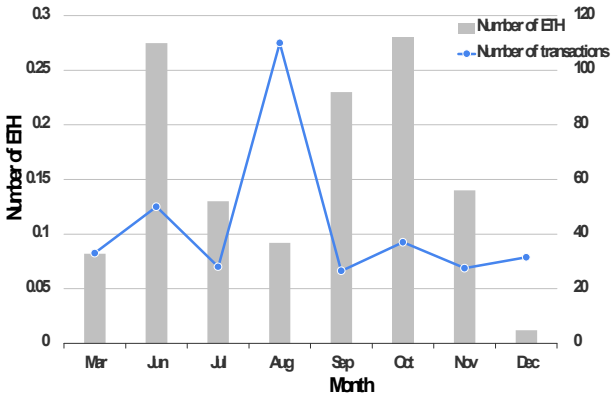

Fig 6. Compare the amount of ETH with the number of transactions

Analyzing the transaction behavior of six thieves related to Ethereum (ETH), the research covers the period from September 2023 to December 2024. It presents the findings as a graph showing the number of transactions conducted by each thief. The data used in the analysis revealed that these thieves exhibit similar patterns in terms of transaction volumes during specific timeframes. Notably, the number of transactions correlates with the number of tokens used in each transaction. For instance, when Thief1 transfers 1.52 ETH tokens, they execute 336 transactions (Fig. 5), often distributed across various wallets.

Thieves tend to choose wallets with higher ETH values for their significant transactions, while they opt for transferring smaller amounts, like 0.00001 ETH, or even conducting empty transactions, excluding any ETH value, to several reserve wallets. Similarly, Thief2 exhibits behavior similar to Thief3, conducting dispersed transactions that add complexity and make their activities challenging to track. On the other hand, Thief2, Thief4, Thief5, and Thief6 prefer fewer transactions over shorter durations, particularly towards the end of the year. Fig. 4 illustrates a direct proportion between the number of transactions and the number of tokens transferred in Fig. 5. This consistent behavior among all six thieves indicates their tendency to distribute their transactions, aligning with their specific strategies and preferences.

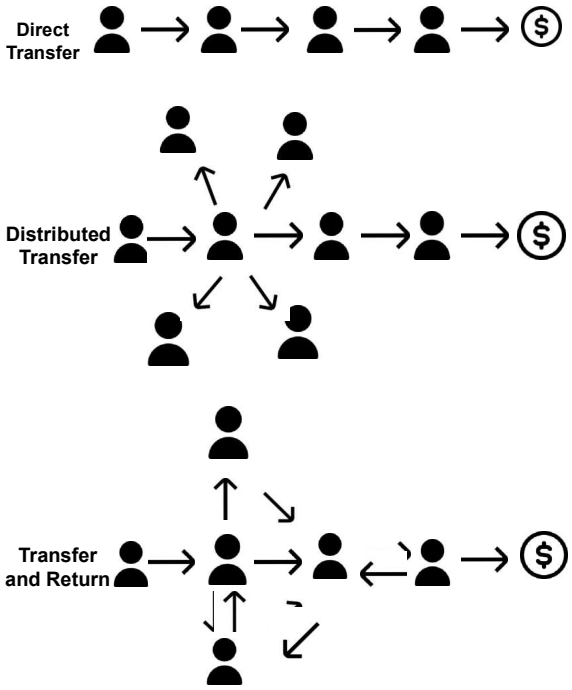

Fig 7. Different token transfer patterns

In analyzing the behavior of the six thieves by looking at the average transaction values per month from the provided graph (Fig. 6), we can observe that these thieves tend to engage in transactions primarily involving Ethereum (ETH). The data in the graph indicates that they tend to transfer tokens to the Binance platform in June, with a relatively high value, such as 0.275 ETH using 50 transactions, and in October, with a value of 0.28 ETH using 37 transactions, which is higher in volume compared to other months. They tend to use fewer transactions when dealing with higher token values. They often prefer using their primary wallets for directly token transfers to Binance. This behavior differs from that observed in August, where they transferred 0.092 ETH using 110 transactions. They sometimes choose more complex routes (transferring to reserve wallets) to cover up their actions and avoid detection. This suggests they deliberately distribute lower-value token transfers to reserve wallets to hide abnormal transaction patterns. From the detailed graph depicting the behavior of these thieves and their evasion strategies, it is clear that they operate at a high level of complexity and use caution to conceal their actions.

The experimental demonstration shows that the number of high-value ETH transactions does not always require many transactions. Thieves (or scammers) may use anonymous accounts to conduct transactions, masking their identity and reducing the chances of being traced. Additionally, having a high volume of transactions might be a strategy scammers employ to conceal untrustworthy activities. In Ethereum, transactions incur gas fees to complete the process. Scammers may opt for higher gas fees to expedite transaction speed and reduce the likelihood of scrutiny.

B. Analysis of transaction patterns

The transaction behaviors of thieves in the system can be differentiated in that they often have distinct patterns of

money transfers, including Direct Transfer, Distributed Transfer, and Transfer and Return, as shown in Fig. 7.

i) Direct Transfer

In this pattern, a thief directly transfers money from one wallet to another without going through other networks. The thief transfers the amount of money and completes the transaction quickly, e.g., Thief1 transferred 0.85 ETH in June-August 2021, 0.58 ETH in September 2021, and Thief6 transferred 1.182 ETH in August - September 2021.

ii) Distributed Transfer

This pattern involves a thief sending money to multiple addresses or wallets simultaneously. The thief transfers a small amount of money to sub-wallets and does not further transfer to other wallets. In the main wallet, the thief transfers a large amount of money with subsequent transfers to the next wallet in a sequential manner until it reaches Binance. This format is mostly used to deceive transaction verification systems and serves as a mechanism to hide the thief's identity. Such transfers can confuse and hinder the verification process in the blockchain network. e.g., Thief2 and Thief4-6, transferred smaller amounts like 0.00001 ETH or even conducted empty transactions to reserve wallets.

iii) Transfer and Return

This pattern involves a thief sending tokens to one wallet and then sometimes returning them to the previous wallet in the next step. The thief transfers money from the main wallet to a sub-wallet and then transfers it back to the main wallet. In this case, the tokens returned are approximately equal to or close to the amount transferred, and the thief transfers tokens to a sub-wallet that does not further transfer to other wallets with a minimal amount of tokens. e.g., Thief3, who transferred around 2.54 ETH tokens in two distinct periods during the mid and late years. This format deceives the system and verifiers into believing it is a legitimate transaction. It creates confusion in the verification process in the blockchain system.

V. Conclusion

This paper presents an approach for tracking addresses and transactions on the system. It assists in understanding the flow of funds and the behaviors of the thieves. By inputting the wallet addresses, we can examine transactions associated with those wallet addresses, including the amount of ETH transferred and all related transactions. This analysis aims to understand the money flow among different addresses by tracking the movements of ETH and ERC-20 tokens, especially the wallets contacting a centralized exchange that required KYC processes. The contribution of this work is to gather data from the blockchain analysis tool and examine thief behavior patterns using real thieves' wallet addresses. Eventually, we can identify suspicious transactions and behavioral patterns. This analysis can help us track the thief's identity. In addition, notification features will be implemented to detect anomaly patterns automatically in future work. However, the notification concept is introduced because the transactions related to our patterns do not always mean they are thieves' transactions. Manually reviewed transactions are required.

References

[1] Ethereum White Paper by Vitalik Buterin, Available: https://ethereum.org/en/whitepaper, accessed on 20 July 2023.

[2] Rattanabunno, S., Werapun, W., Suaboot, J., & Puongmanee, M. (2023). "An EOA Identity Tracing System (AITS) on Ethereum Blockchain." In Proceedings of the 8th International Conference on Information and Network Technologies (ICINT 2023). Tokyo, Japan.

[3] Martinez, J., Smith, A., Johnson, B. (2021). "Motivations and strategies of value scammers in Ethereum." Journal of Cryptocurrency Research, 15(2), 110-130.

[4] Smith, J., Johnson, R., Williams, L. (2019). "Analysis of value scamming techniques in Ethereum and the associated financial losses." Journal of Cryptocurrency Studies, 10(3), 145-162.

[5] Johnson, A., & Smith, B. (2018). "Characteristics and Strategies of Thieves in Digital Currency Networks: A Case Study of Ethereum." Journal of Cybersecurity Research, 20(3), 145-162.

[6] V. V. Nosov, I. A. Manzhai (2021). Certain Aspects of the Analysis of Cryptocurrency Transactions during the Prevention and Investigation of Crimes. University of Kharkiv, pp 93-100.

[7] Garcia, E., et al. (2017). Hacker's Behavior Analysis: Insights from Blockchain Transactions. International Journal of Information Security, 32(4), 345-362.

[8] Lee, C., & Clark, M. (2018). Examining the Holding Period of Stolen Funds: Insights from Hacker's Transactions. Journal of Digital Forensics, Security, and Law, 7(3), 89-105.

[9] Ansah, A.K.K., Adu-Gyamfi, D. (2020). "Enhancing User and Transaction Privacy in Bitcoin with Unlinkable Coin Mixing Scheme." International Journal of Computational Science and Engineering, 23(4), 381-395. Inderscience Publishers.

[10] Deuber, D., Schr√∂der, D. (2021). "CoinJoin in the Wild." The University of Erlangen-Nuremberg. pp 461-480.

[11] Chepurnoy, A., Saxena, A. (2020). "Zerojoin: Combining Zerocoin and CoinJoin." IACR Cryptology ePrint Archive, 2020, 421-436. Springer, Cham.

[12] Agarwal, V. (2019). Money Laundering: A Borderless Crime. Journal of Emerging Technologies and Innovative Research (JETIR), 6(2), 145-150.

[13] Kolachala, K., Simsek, E., Ababneh, M., et al. (2021). "SoK: Money Laundering in Cryptocurrencies." New Mexico State University, Sam Houston State University.

[14] Kiffer, M. (2018). Cryptocurrencies and money laundering: A Review of Recent Literature. Journal of Money Laundering Control, 21(3), 299-311. DOI: 10.1108/JMLC-12-2017-0056.

[15] Bitquery, Available: https://bitquery.io/, accessed on 20 July 2023.

[16] Chainalysis, Available: https://chainalysis.com/, accessed on 25 July 2023.

[17] Nansen, Available: https://www.nansen.ai/, accessed on 25 July 2023.

[18] Dune, Available: https://dune.com/home/, accessed on 25 July 2023.

[19] Li, Y., Zheng, K., Yan, Y., et al. (2017). "EtherQL: A Query Layer for Blockchain System." In: Advances in Knowledge Discovery and Data Mining. Soochow University (Suzhou), Microsoft, University of Queensland. Vol. 10178, pp. 556-567.