UDC 004.4 + 004.9
DOI: 10.20535/SRIT.2308-8893.2023.4.03

BLOCKCHAIN TRANSACTION ANALYSIS: A COMPREHENSIVE REVIEW OF APPLICATIONS, TASKS AND METHODS

Ya. DOROGYY, V. KOLISNICHENKO

Abstract. Blockchain transaction analysis is a powerful tool to gain insights into the actions and conduct of participants within blockchain networks. This article aims to extensively examine the applications, tasks, and methods associated with blockchain transaction analysis. We look at various uses of transaction analysis, ranging from its instrumental role in blockchain development to its pivotal significance in the field of criminal investigations. By leveraging common techniques and technologies employed in conducting such an analysis, we unlock hidden insights and uncover information that is not visible at first look. This article offers a wide-ranging perspective on the profound significance of blockchain transaction analysis while shedding light on its key role within the cryptocurrency industry and its wide-ranging applications beyond.

Keywords: blockchain transactions, transaction analysis, transaction tracing, flow analysis, blockchain forensics.

INTRODUCTION

Blockchain technology has revolutionized the way financial transactions are conducted and recorded, creating a public decentralized network that eliminates the need for intermediaries and enables secure and transparent transactions. With the growing popularity of cryptocurrencies and blockchain-based systems, the need for effective blockchain transaction analysis has become increasingly important. Blockchain transaction analysis refers to the process of examining and interpreting blockchain data to gain insights into the flow of transactions, identify patterns, and detect anomalies.

This paper provides a review of the applications of analysis in various domains, the methods and techniques used to analyze blockchain data. The paper is organized as follows. First, we provide an overview of blockchain technology and its key concepts including the types of data available on the blockchain. Then, we delve into the applications of blockchain transaction analysis, including cryptocurrency investigations. We provide real-world examples of how blockchain transaction analysis has been used in different domains and discuss the benefits and limitations of the approaches.

Next, we discuss blockchain transaction analysis, the challenges of analyzing blockchain data, and the methods and techniques used to perform blockchain transaction analysis.

Finally, we conclude the paper with a discussion of the future of blockchain transaction analysis, including the challenges and opportunities that lie ahead. We argue that blockchain transaction analysis has the potential to transform many industries by providing greater transparency, security, and efficiency. However, the field is still in its early stages, and much research is needed to develop more effective methods and tools for analyzing blockchain data.

Overall, this paper aims to provide a comprehensive overview of blockchain transaction analysis, covering both the methods and applications of the field. By doing so, we hope to contribute to the growing field of research on blockchain technology and its potential impact on various industries.

BLOCKCHAIN TRANSACTIONS

Blockchain transaction, in simple terms, can be defined as a record of the transfer of digital assets or the storage of information on a blockchain network that is permanently recorded on a distributed ledger.

One of the most notable features of blockchains is that everything stored is visible to everyone, meaning anyone can see who makes transactions to whom. While it may sound easy at first, it appears much more complex.

Mechanisms of asymmetric cryptography are used to define the sender or receiver of a transaction – addresses are formed from public keys, and private keys are used to sign transactions (to prove that the actual owner of the funds created the transaction).

Another concept blockchain networks are using is hierarchical deterministic (HD) wallets. In HD wallets a master seed is used to generate an unlimited number of public-private key pairs, allowing for the creation of multiple addresses and sub-wallets that can be easily managed from a single mnemonic phrase or seed. This enables users to receive and send funds with new addresses each time, therefore increasing the privacy of the end-user.

In terms of record-keeping, there are two common models: unspent transaction output (UTXO) model and account model. In the UTXO model (Fig. 1), each transaction creates a list of outputs that will be spent in future transactions (used as inputs). The outputs are assigned to the addresses that should be able to use (spend) them. The total balance of the address is the sum of all unspent outputs to this address at the current moment.

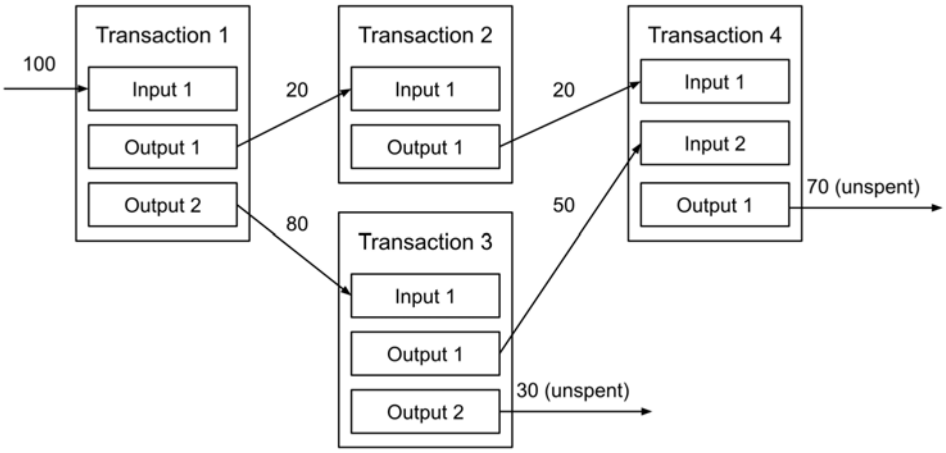

Fig. 1. Simplified UTXO model

The account model, on the other hand, is much simpler to understand. A blockchain maintains balance for each account and keeps a record of all transactions that have affected that balance.

In order to have the ability of multi-user ownership of funds, or more generally, to set up conditions and rules for spending funds (rules of ownership), blockchain networks were built with additional complexity. In fact, Bitcoin transactions do not have sender or receiver fields. Instead, Bitcoin uses lock (scriptPubKey) and unlock (scriptSig) scripts to create a concept of a puzzle, solvable by meeting specified conditions (e.g., to spend a transaction the one should specify a signature in the unlock script, whose public key is set in the lock script).

Bitcoin scripts are extremely limited and do not allow creating complex logic. To face this, Ethereum network uses a concept of smart contract [1], which enables creating complex programs using JavaScript-like language called Solidity, storing them on the blockchain and executing thorough Ethereum Virtual Machine.

Scripting and programming features give extensive possibilities to build applications with various levels of complexity providing end-users with secure decentralized financial (DeFi) services and developers with tools for further optimization (e.g., layer 2 networks) and development [2].

If we talk about what information is stored in the blockchain, then it is usually logical information. By logical information here we mean information related to blocks, transactions, accounts, etc. In other words, data to support the business logic of a blockchain.

There is much information that is not part of blockchain and, usually, it is more technical and does not influence the business logic directly. Let us consider a simplified process of including transactions into the blockchain (which is similar among different networks). A user creates a transaction and signs it, providing proof of address ownership and transaction integrity. After a transaction is signed, the user broadcasts it by using one's own node or through the JSON-RPC interface of a chosen public node. Traveling through a bunch of nodes, the transaction finally reaches miners who include it to the block and mine it. After the block is mined, it gets broadcast to the rest of the nodes. When the rest of the nodes accept it, it is considered as a part of the blockchain. No networking information (IP of the sender and nodes that broadcasted the transaction, etc.) in this process is included into the blockchain, however, intermediate hosts may store it in their own databases.

Taking into consideration all the mentioned specifics, it is not easy to analyze transactions and data stored in the blockchain – who owns the funds, how much, who was the actual sender, what logic the transaction performs, etc. In the next chapter we will go into why such analysis is important and where it is applied.

APPLICATION OF ANALYSIS

Blockchain transaction analysis is a powerful tool that allows us to better understand the behavior of users and events on blockchain networks. As blockchain and decentralized finance (DeFi) technologies continue to grow, there are an increasing number of use cases for transaction analysis. This chapter will explore the key applications of blockchain transaction analysis, including cryptocurrency investigations, risk management, tax compliance, and many others. By leveraging the insights gained through transaction analysis, stakeholders can seize the big picture and make informed decisions.

While some categories may overlap, we think the following distinguishment reflects the unique specifics in the best way.

Crime Investigation

Cryptocurrencies possess unique properties such as decentralization, independence from banks, security, ubiquity, and anonymity. As is the case with other types of assets, these distinct characteristics determine the specific applications of cryptocurrencies. However, these same properties have also made cryptocurrencies an appealing tool for illicit activities such as money laundering, fraud, scam, and sanctions evasion, among others [3; 4].

The Africrypt incident is one of the biggest that has happened with the involvement of cryptocurrencies. Two founders of Africrypt alleged that their firm was hacked resulting in the theft of all its assets. After the statement, the founders vanished. Approximately $3.6 billion in Bitcoin has disappeared in total [5]. As of now, not much added information has been found regarding this case. Law enforcement authorities are reportedly continuing their search for the founders [6]. This incident, among many others [7; 8], is similar to traditional finance scams, where founders (whose names are often known) collect money and disappear.

While blockchain technologies provide a certain level of privacy it cannot be considered as fully anonymous [9], and in many cases a careful analysis may answer the question “where the money goes” [10]. Let us examine some prominent cases where transaction analysis was helpful for the investigation.

Cryptocurrencies are often used as a means of payment in cyber extortion and ransomware attacks. Hackers who carry out these attacks demand payment in cryptocurrency in exchange for returning control of the victim’s computer system or stolen data. One of such cases is NetWalker malware, which is built as Ransomware as a Service (RaaS) model [11], where affiliates rent malware from operators to launch attacks. One of the affiliates was arrested, and a blockchain transaction analysis solution was used to help to track down addresses associated with the affiliate [12].

Hacking of the DeFi projects is quite widespread [13; 14]. Compared to other domains, in the blockchain domain a hacker directly operates the valuable assets such as coins or tokens. It is worth mentioning that the biggest amounts of assets are concentrated in cross-chain bridges and centralized crypto exchanges (CEX) which make them attractive targets [15]. Transaction analysis is usually applied to get an understanding of the attack and to track the ones who were involved.

An attack analysis is an essential measure to be taken after the incident has occurred. This process involves identifying how the system was compromised, assessing the extent of the damage caused, determining strategies for minimizing the damage, and addressing any vulnerabilities that were exploited. To identify how the blockchain system was hacked, attackers’ transactions together with involved smart contracts are analyzed. Such analysis is often performed by the owning company, investigating company or blockchain community [16; 17] with various levels of details.

Hackers who steal funds from blockchains often seek to launder the stolen cryptocurrencies to conceal their identities and make it difficult for law enforcement agencies to trace the illicit funds [18]. They can do this by using mixers, tumblers, or other obfuscation techniques to obscure the trail of transactions and make it hard to trace the stolen funds. Additionally, hackers can use decentralized exchanges to convert stolen cryptocurrencies to other assets, such as privacy coins or stablecoins, to further obfuscate the trail of transactions. These assets can then be moved through multiple wallets to further distance the funds from the original theft. The final step may involve converting the stolen cryptocurrencies to fiat currency through a regulated exchange or other means to cash out the illicit funds.

One of the successful investigations of laundering is the Bitfinex case. According to Elliptic [19], after the hack stolen funds were slowly being laundered using different techniques. AlphaBay is one of the services that was used as a mixer to hide the trails. However, later it was seized by law enforcement, and this likely allowed them to get trails to the hackers.

Another, less successful investigation case, is a hack of Zaif exchange in September 2018. Crystal Blockchain Analytics engineering team performed an analysis of bitcoin movements [20] and could find addresses involved in the hack. Although the owners of the addresses are unknown, the addresses are being monitored in case of further transactions.

One notable type of blockchain assets that got much attention is Non-Fungible Token (NFT). NFTs are assets that represent ownership of unique items such as music, videos, art or other on a blockchain network. They are not dividable and interchangeable with one another. Each NFT is unique and cannot be replicated. Although it can be implicated in criminal activities similar to other digital assets, one distinctive aspect worth mentioning is copyright infringement. Blockchain technology can guarantee the uniqueness of the token but cannot guarantee the uniqueness of the represented asset, which can be copied. Transaction analysis can be used to assist with NFT copyrighting. By analyzing the NFT transactions it may be possible to verify its authenticity and identify the original creator or owner of the work. This information could also be used as evidence to support copyright claims. One notable project that tries to detect copyright infringement by scanning blockchains and marketplaces is DeviantArt [21]. They use different techniques including machine learning to spot the copy.

We can observe that blockchain transaction analysis is used as a valuable tool in crime investigations, enabling law enforcement agencies to track the flow of funds in the blockchain network and identify any suspicious activity associated with illegal activities such as money laundering, dark web transactions, cybercrime, and fraud. Transaction analysis also helps trace the flow of funds associated with cyberattacks, ransomware payments, and other malicious activities. It provides insights into transaction behavior and patterns that can be used to identify potential criminal activity and take appropriate action.

Compliance and Regulation

Cryptocurrency regulations are laws or rules established by governments or regulatory bodies to govern the use, trading, and custody of cryptocurrencies. These regulations aim to protect investors, prevent illicit activities such as money laundering and terrorist financing, and promote the stability and integrity of the financial system. Cryptocurrency regulations can cover a wide range of topics, depending on the jurisdiction and the specific concerns of regulators [22]. While these regulations are mostly related to cryptocurrencies rather than technology itself, some countries may try to enforce regulations on the tech side too (e.g., on mining) [23].

Transaction analysis is a useful tool for enforcing cryptocurrency regulations and ensuring compliance with regulatory requirements [24; 25]. Regulators can use transaction analysis to monitor and detect potential money laundering activities, enforce KYC (know your customer) and tax compliance, prevent fraud, and protect consumers in the cryptocurrency market [26].

By analyzing transaction patterns and identifying any unusual or suspicious activity, regulators can take appropriate action to prevent money laundering and other financial crimes. They can also use transaction analysis to monitor compliance with know-your-customer requirements and tax laws and regulations. Additionally, transaction analysis can help prevent cryptocurrency fraud by identifying any fraudulent activity and taking appropriate action.

While in the previous section transaction analysis is applied after an event happened (for the investigation), in case of regulations, transaction analysis is mostly used continuously (for the detection and prevention).

Trade and investment

In traditional finance, financial transactions are mostly opaque, and investors often rely on intermediaries [27] to provide information about the assets they are investing in. Investors and traders use methods such as technical analysis to analyze financial markets and securities based on statistical trends and patterns in historical price and volume data. Trading in blockchain offers new opportunities and challenges with its unique characteristics of transparency, security, and decentralization [28].

Having access to transaction data changes the rules of the game. However, without a proper processing of massive amounts of raw data transparency does not give you advantages. Therefore, it is important to produce new methods and tools that can provide insights into the behavior of market participants and the underlying fundamentals of digital assets. Moreover, these methods and tools should be the same or better than in your potential opponents, as they also have access to the same raw data.

Here transaction analysis can be helpful in several ways. It can provide volume and velocity of transactions for a particular cryptocurrency [29]. Blockchain transaction analysis can give information on the distribution of digital assets among market participants and provide valuable insights into their behavior. This information can help traders and investors identify potential price levels for a particular cryptocurrency based on the level of demand from buyers and sellers. By analyzing this information traders and investors can gain insights into participants' trading strategies and use this information to adjust their own trading decisions.

Besides that, it can be used for analyzing the flow of assets within a blockchain to identify large transactions and movements of funds that may be indicative of market manipulation or other illicit activities. Transaction flow analysis can help traders avoid entering into positions that may be vulnerable to sudden price movements.

Risk Management

Organizations that try to adopt blockchain and DeFi technologies for their businesses should be aware of numerous additional risks [30–32].

Cryptocurrencies are still growing and one of the primary risks is unclear regulations, specifically, legal, and regulatory compliance. Blockchain-based businesses may face challenges in complying with current regulations or in predicting future regulations, which can result in legal and financial penalties or reputational damage. The risk of unclear regulations in blockchain risk management is significant because blockchain technology operates in a regulatory gray area in many countries.

Another set of risks comes from the technical side. Bugs, vulnerabilities, network scalability difficulties can lead to various negative outcomes such as loss or theft of funds [33], network downtime [34], reputational damage and others.

Volatility and liquidity are another two significant risks associated with blockchain and cryptocurrencies [35]. These risks can affect both investors and businesses that use cryptocurrencies for transactions or other purposes. Volatility can lead to significant losses for investors who have invested in cryptocurrencies, as the value of their investments can decrease rapidly. Additionally, businesses that use cryptocurrencies for transactions can be negatively affected by volatility as the value of their transactions can also fluctuate rapidly. Cryptocurrency markets can be relatively illiquid, particularly for less popular cryptocurrencies or during periods of market instability. This illiquidity can make it difficult for investors to sell their cryptocurrencies when they need to, leading to losses. Additionally, illiquidity can create challenges for businesses that use cryptocurrencies for transactions, as it can be difficult to find a buyer or seller for the desired cryptocurrency at a fair market price.

Transaction analysis is a useful tool for risk management in blockchain. It can provide businesses with insights into transaction behavior and patterns, which can be used to identify potential risks and vulnerabilities. Transaction analysis can be used to detect fraudulent activity, such as money laundering or other financial crimes, by analyzing transaction patterns and identifying any unusual or suspicious activity. It can also help businesses monitor compliance with regulations and industry standards by detecting any potential compliance issues. Businesses can determine the level of risk associated with a particular transaction or customer and take appropriate action to manage that risk. Moreover, transaction analysis can help investors and businesses assess the liquidity of cryptocurrencies by analyzing transaction volumes.

Supply Chain Management

Supply chain management in blockchain refers to the use of blockchain technology to track and manage the movement of goods and services through a supply chain. Blockchain technologies provide a transparent and secure platform for tracking and verifying transactions in real-time [36]. Each asset is represented through a unique token. When a party performs transfer of the asset, it also creates and signs a transaction to transfer the token (that represents actual asset) on that blockchain. Transactions are then recorded on the blockchain, and the entire process is transparent for the shareholders. This can help businesses to optimize their supply chain operations, reduce costs, and ensure compliance with relevant regulations and industry standards.

In the supply chain process, blockchain transaction analysis is a core tool, which allows stakeholders to follow the entire process. It allows extracting and analyzing transaction patterns, businesses can gain valuable insights into the movement of goods and services through the supply chain [37–39].

Blockchain Development

Analysis of transactions is also important for blockchain development and its optimization. At different stages of development transactions are analyzed to debug errors [40] and monitor the network health. It is used to get understanding about users' behavior inside the network, to identify their needs and troubles [41]. By analyzing transaction patterns, developers can identify bottlenecks in the blockchain network, such as congested nodes [42] or high transaction fees. The information gained can be used to develop new solutions to optimize the blockchain platform. Such optimization may apply to its performance [43; 44] or security [45]. Additionally, transaction analysis allows developers to detect suspicious activity or DoS attacks and take steps to mitigate the risks [46].

Blockchain Attacks Detection and Prevention

Real-time analysis of transactions is employed for monitoring smart contracts to detect possible attacks and prevent them. The analysis of transaction data in real-time enables the detection of any suspicious activity, allowing for timely intervention to prevent or minimize the impact of an attack.

There are no strict criteria defining what to consider as an attack, therefore various heuristics (detect maximum value transfer, ownership change, contract upgrades) and machine learning algorithms for flow analysis may be used. When a potential attack happens and the algorithm detects it, the stakeholders get notified so they can perform further actions. In situations where immediate response is required, it is possible to configure automated actions, such as temporarily halting the core functionality of a contract.

One such widely used solution is Forta [47]. It gets advantage of transaction analysis to detect and mitigate security threats in decentralized applications and smart contracts. Forta technology is designed to analyze blockchain transactions and data to identify and prevent hacks, exploitations, and other malicious activities. It is stated [48] that the utilization of the system could have prevented numerous attacks and financial losses.

TASKS AND METHODS

Given the applications of the analysis described in the previous sections, we have identified and selected the most frequent and critical tasks to be addressed through blockchain transaction analysis, which can be broadly categorized into three big groups. In this section, we will examine these tasks and the techniques employed to address them.

Linking addresses with identities

A common task in transaction analysis is to identify the owner of the address. By owning an address, we mean that the person holds a private key (or seed/mnemonic phrase) and a corresponding public key, from which the address is created. Because addresses are created using solely cryptographic mechanisms and even before interacting with the chain, it can be impossible to get the real identity of the owner. Fortunately, we do not need to solve the problem where users just create their addresses, but where users actually use them. Similar to this task, there is an opposite one – to find addresses belonging to a certain entity.

One of the most straightforward methods for linking addresses to identities is to require users to disclose their identities when they purchase or sell cryptocurrency with fiat money. This is a prevalent regulatory approach, and most cryptocurrency exchanges now must follow Know Your Customer (KYC) procedures that include several steps to identify the user. KYC procedure typically involves several steps, such as providing identification documents and verifying the user's personal information, in order to confirm the user's identity. Once a user has been successfully identified through this process, their cryptocurrency transactions on the exchange can be linked to their real-world identity, making it easier to track any suspicious activity or money laundering attempts.

When a signed transaction or block is transmitted to other nodes, or a JSON-RPC call is made on a public network, information about the sender, such as their IP address, can be recorded by the nodes and intermediary network devices. This can provide a means of identifying the user in the future. In general, transmitting any information related to a blockchain address to a third-party server, such as making a purchase on a website, searching for a transaction, or checking a balance on a blockchain explorer [49], or using a wallet application that utilizes analytics, can potentially establish a connection between the user and the address.

Another method for mapping entities to addresses is to maintain a record of information related to the blockchain addresses that has been published by the entity or utilize openly accessible databases. One example of such a database is a list of malicious actors [50] or a database of sanctioned addresses, which can be employed during analysis. Social networks scraping may also be helpful, as users often publish addresses of their wallets. The main downside of this approach is you need to set up complex infrastructure and collect a lot of data beforehand, and the identity you are interested in may not be even in this data.

Flow Comprehension

By blockchain transaction flow we refer to sequences of transactions that occur on a blockchain network. These sequences can vary from small to large and have complex structures containing branches and joins. Complex structures may contain valuable information that is not visible at first look and therefore different methods should be applied to extract it.

Occasionally, these sequences can intentionally have intricate structures. Criminal actors often obscure traffic, expecting that investigators will lose track. However, by utilizing the right approaches and tools, it is possible to gain significant insights into the flow and uncover details that may have otherwise remained hidden. In the following sections, we will explore common approaches to analyzing blockchain transaction flows.

One can manually retrieve data from the blockchain using blockchain explorers or similar tools that enable communication with blockchain nodes. Usually, they are web-based tools [51] that enable users to access and navigate the contents of a blockchain. They have a graphical interface to examine and analyze blockchain data, such as transaction records, account addresses, and balances. The primary function of a blockchain explorer is to facilitate the search of specific transactions, verify wallet balances, and examine network metrics. Although blockchain explorers are useful for basic cases, they are not suitable for handling complex cases involving long chains of transactions.

Graph visualization is used to handle the complexity of sequences of transactions. Different kinds of graphs and representations can be used to fit certain needs [52–54]. However, in the majority of cases, it is desirable to present the flow as a graph, in which addresses are represented as nodes and transactions as directed edges (Fig. 2). This format gives an ability to follow the asset transfer in the most natural way. It can still be challenging to comprehend, and as such, it is beneficial to group, filter, highlight, and conceal distinct elements, to extract or segregate valuable information from irrelevant data.

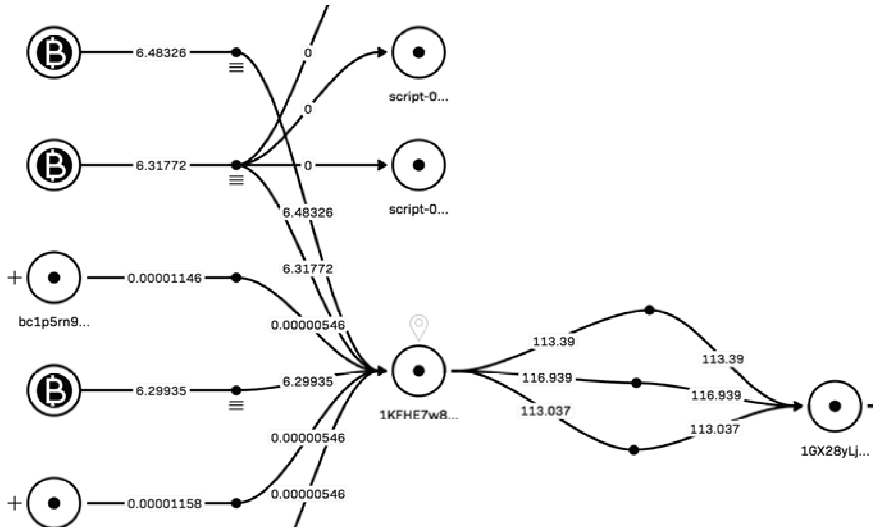

Fig. 2. Graph visualization in Crystal Explorer [55]

For various reasons, users may want to transfer their assets from one network into another or want to exchange one type of assent into another. They use exchange platforms and cross-chain bridges for these purposes. Bad actors who want to obfuscate their traffic can also take advantage of these methods. Additionally, they can use tools such as mixers [56; 57] which can significantly complicate the task of investigators attempting to comprehend the transactional flow. We can define these instruments as conversion protocols. Transactions tracing tools should be aware of different conversion protocols and be robust enough to perform address linking (in cases where theoretically possible). In many cases conversion protocols, such as cross-chain bridges [58], are well-documented and when they are not specifically designed for hiding traffic it can be an easy task to find what is the address of the user in the other network. In cases where no documentation is available or where it is claimed that the system provides absolute anonymity, it may be necessary to perform a manual analysis of the system. A thorough manual analysis of the system can provide valuable insights into its functionality. It helps in understanding the meaning of user transactions and identifying any potential flaws that could be exploited. Additionally, this type of analysis can reveal possibilities of developing new methods to obtain additional information about the transactions or the users [59].

In order to simplify flow analysis, various algorithms can be utilized to discover connections, patterns, and anomalies [60]. They can be used to simplify the view or bring the most important data to the front. These algorithms can be a classic one [61] or machine learning algorithms [62].

There are commercial tools available on the market, such as Chainalysis Reactor, MistTrack and others [63], that provide convenient instruments for flow analysis, including graph visualizations and various other features discussed in this section.

Smart Contract Brakedown

In contrast to the regular banking transactions, blockchain transactions became more than just funds transferring. Smart contracts let writing very complex conditions for transferring funds, and as a result – building additional abstraction layers and protocols. This allowed the creation of a new financial paradigm – DeFi.

With increased complexity, transaction analysis became harder and more time consuming to perform. Calling a certain function on a smart contract and transferring funds can mean different things and therefore prior contract understanding is needed. A call to a smart contract may create a chain of calls with different arguments, including calls to other contracts. A list of methods has been developed to approach the smart contract breakdown.

Manual source code review provides a comprehensive insight into the behavior of a smart contract. This process involves a thorough examination of the code, line by line, to gain understanding of both the overarching concept and the finer points. However, this type of analysis requires extensive knowledge of programming languages, cryptography, and blockchain technology, and can be a time-consuming process. Reading documentation of a product may be helpful and can clarify reasons behind some programming decisions or explain unfamiliar concepts. However, it is not always available.

During a source code review, the availability of the source code is another important aspect to consider. It is common for smart contract source code to be published and, in many cases, it can be found on GitHub. However, having a source code of the contract does not mean the exact same contract is published on the blockchain, therefore a contract verification is needed [64] – to match source code to on-chain bytecode.

In some cases, developers may choose not to make the source code of the contracts publicly available. As a result, alternative techniques are necessary to gain insight into the behavior of the contract through analyzing its bytecode. Generally, the process is called reverse engineering. It is similar to the code review but more complex and requires more effort. The reason for this is that a compiled smart contract contains significantly less information compared to the original code. In cases of optimizations the resulting bytecode gets even more complicated, as human written code is converted into more efficient code patterns. To simplify the reverse engineering process disassemblers (convert bytecode to EVM opcodes) and decompilers are used [65; 66]. Decompilers convert a bytecode to high-level representation. However, due to the loss of information during compilation, the code does not look like the original code.

If we want to look at the actual execution of the smart contract on the chain, block explorers may be helpful for simple cases. Some of them have transaction decoders and can provide execution traces. There are tools developed specifically for transaction decoding, such as Transaction Tracer [67] or similar [68], which provide a call trace, which is a tree of function calls and arguments, made through different contracts during transaction execution. Furthermore, there are tools for local EVM tracing [69], which allow detailed examination of smart contract transactions. Development environments, like Truffle, have even more convenient means to debug on-chain transactions [70].

Automated analysis tools for smart contracts can be used to get a better understanding of smart contracts. Usually, they are divided into two categories – static and dynamic analyzers [71].

Static analysis tools perform contract analysis without running them. Slither framework [72], is one of such tools, is designed to automatically find vulnerabilities, give information about the contract and its functions, give summary about the authorization accesses and many other.

Dynamic analysis tools, on the other hand, perform analysis by executing smart contracts or their parts. Various classes of dynamic analysis tools used for analyzing smart contracts such as symbolic execution tools, Satisfiability Modulo Theories (SMT) solvers, taint analyzers and fuzzers [73]. Mythril, Echidna [74] and Manticore [75] are one of the most widely used tools to find vulnerabilities in the code, to find a set of inputs that transit a program into an unexpected state or to explore all possible states. These tools and approaches are not mutually exclusive, but rather they give different perspectives on how a smart contract works.

Commercial tools like MythX [76] combine static and dynamic approaches to get the best of both worlds and provide most comprehensive results.

Recent research and developments in artificial intelligence (more precisely, large language models such as ChatGPT [77]), allowed using these technologies for explaining the code, reverse-engineering [78] and even for finding vulnerabilities [79]. These tools are already used now and will be even more adopted in the near future to assist during the code analysis.

CONCLUSIONS

Blockchain transaction analysis is a crucial tool for gaining insights into the behavior of users on blockchain networks. From anti-money laundering and fraud detection to supply chain management and tax compliance, there are many applications for transaction analysis in the world of cryptocurrency and beyond.

Despite the challenges posed by the anonymous and decentralized nature of blockchain networks, there is a growing awareness of the importance of transparency and accountability in the cryptocurrency industry. By utilizing the insights gained through transaction analysis, regulators, businesses, and other stakeholders can work together to build a more secure, efficient, and sustainable blockchain ecosystem.

The methods and techniques used in transaction analysis continue to evolve, and there is a growing need for more sophisticated tools to keep pace with the complexity of blockchain networks. Advances in machine learning, graph analysis, and other data science techniques are likely to have a significant impact on the future of blockchain transaction analysis.

In our future work we will analyze multiple blockchain networks to get advantages of their specifics to improve and develop new methods for analyzing transactions. We will dive into protocols at different layers and develop solutions to extract additional information that is not available using traditional methods.

REFERENCES

1. V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform,” *Ethereum.org*. Accessed on: April 24, 2023. [Online]. Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf
2. S. Sharma and M. Naggar, “A New Era for Bitcoin?,” *Binance Research*. Accessed on: April 24, 2023. [Online]. Available: https://research.binance.com/static/pdf/a-new-era-for-bitcoin.pdf
3. “The 2023 Crypto Crime Report,” *Chainalysis.com*, 2023. Accessed on: April 24, 2023. [Online]. Available: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf
4. “Blockchain Security and AML Analysis Report - 2022 Annual,” *Slowmist.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.slowmist.com/ report/2022-Blockchain-Security-and-AML-Analysis-Annual-Report(EN).pdf
5. L. Prinsloo and R. Henderson, “Trail of Brothers Linked to Missing Bitcoin Stash Is Still Murky,” *Bloomberg.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.bloomberg.com/news/articles/2021-06-27/trail-of-brothers-linked-to-missing-bitcoin-stash-is-still-murky
6. L. Prinsloo, “Crypto Losses Probed by South African Cops After Brothers Vanish,” *Bloomberg.com.* Accessed on: April 24, 2023. [Online]. Available: https://www.bloomberg.com/news/articles/2022-01-11/crypto-losses-probed-by-south-african-cops-after-brothers-vanish
7. “Top five most wanted crypto criminals,” *CNBCTV18*. Accessed on: April 24, 2023. [Online]. Available: https://www.cnbctv18.com/cryptocurrency/top-five-most-wanted-crypto-criminals-15897891.htm
8. “The 10 biggest crypto scams on record and the lessons we can learn from them,” *Irishtechnews.ie.* Accessed on: April 24, 2023. [Online]. Available: https://irishtechnews.ie/10biggestcryptoscams/
9. “Protect your privacy,” *Bitcoin.org.* Accessed on: April 24, 2023. [Online]. Available: https://bitcoin.org/en/protect-your-privacy
10. “Ukrainian Cyber Police Department in Collaboration with Crystal,” *Crystalblockchain.com.* Accessed on: April 24, 2023. [Online]. Available: https://crystalblockchain.com/articles/ukrainian-cyber-police-department-now-in-collaboration-with-crystal-blockchain/
11. K. Baker, “What is Ransomware as a Service (RaaS)?,” *crowdstrike.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
12. “Chainalysis in action: U.S. authorities disrupt NetWalker ransomware,” *Chainalysis*. Accessed on: April 24, 2023. [Online]. Available: https://blog.chainalysis.com/ reports/netwalker-ransomware-disruption-arrest/
13. “Rekt - leaderboard,” *rekt.* Accessed on: April 24, 2023. [Online]. Available: https://rekt.news/leaderboard/
14. “SlowMist Hacked - SlowMist Zone,” *Slowmist.io.* Accessed on: April 24, 2023. [Online]. Available: https://hacked.slowmist.io/
15. “The 10 biggest crypto exchange hacks in history,” *Crystalblockchain.com.* Accessed on: April 24, 2023. [Online]. Available: https://crystalblockchain.com/ articles/the-10-biggest-crypto-exchange-hacks-in-history/
16. @officer_cia, “How cross-chain bridges are hacked? A detailed review,” *Mirror.xyz*. Accessed on: April 24, 2023. [Online]. Available: https://officercia.mirror.xyz/ AFkEUuxid1egNm4XdqYEzWEwosPNbz2CNghlNrq7LZQ
17. @officer_cia, “Retrospective: hacks in web3,” *Telegraph*. Accessed on: April 24, 2023. [Online]. Available: https://telegra.ph/Retrospective-hacks-in-web3-10-24

18. SlowMist, "SlowMist AML: Tracking funds laundered by Tornado Cash," *Medium*, Accessed on: April 24, 2023. [Online]. Available: https://slowmist.medium.com/ slowmist-aml-tracking-funds-laundered-by-tornado-cash-3a0e1f637054
19. "New York husband and wife arrested for laundering bitcoin," *Elliptic.co.* Accessed on: April 24, 2023. [Online]. Available: https://www.elliptic.co/blog/elliptic-analysis-new-york-husband-and-wife-arrested-for-laundering-5-billion-in-bitcoin-stolen-from-bitfinex-in-2016
20. "Crystal Blockchain Analytics: Investigation of the Zaif Exchange Hack," *Bitfury.com.* Accessed on: April 24, 2023. [Online]. Available: https://bitfury.com/ content/downloads/bitfury_crystal_zaif_report_23_10_18.pdf
21. "DeviantArt protect: Helping safeguard your art," *Deviantart.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.deviantart.com/team/journal/ DeviantArt-Protect-Helping-Safeguard-Your-Art-884278903
22. "Cryptocurrency regulations around the world," *ComplyAdvantage*. Accessed on: April 24, 2023. [Online]. Available: https://complyadvantage.com/insights/ cryptocurrency- regulations-around-world/
23. T. Akhtar and S. Shukla, "China Makes a Comeback in Bitcoin Mining Despite Government Ban," *Bloomberg.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.bloomberg.com/news/articles/2022-05-17/china-makes-a-comeback-in-bitcoin-mining-despite-government-ban
24. "Cryptocurrency transaction monitoring: What you need to know," *ComplyAdvantage*. Accessed on: April 24, 2023. [Online]. Available: https://complyadvantage. com/insights/transaction-monitoring-cryptocurrencies/
25. "How continuous cryptocurrency transaction monitoring gives compliance teams peace of mind," *Chainalysis*. Accessed on: April 24, 2023. [Online]. Available: https://blog.chainalysis.com/reports/kyt-continuous-monitoring/
26. "Cryptocurrency regulation: How governments around the world regulate crypto," *Chainalysis*. Accessed on: April 24, 2023. [Online]. Available: https://blog.chainalysis.com/reports/cryptocurrency-regulation-explained/
27. N. Asokan, "Financial Intermediaries: their role on real examples," *Agicap.com*. Accessed on: April 24, 2023. [Online]. Available: https://agicap.com/en/article/ financial-intermediaries/
28. M. Morel, "Technical analysis is dead, long live transaction analysis," *CoinDesk*. Accessed on: April 24, 2023. [Online]. Available: https://www.coindesk.com/ layer2/2022/10/26/technical-analysis-is-dead-long-live-transaction-analysis/
29. I.G.A. Pernice, G. Gentzen, and H. Elendner, "Cryptocurrencies and the Velocity of Money," *Cryptoeconomic Systems*, vol. 1, iss. 1, 2021. doi: 10.21428/ 58320208.f212c00e.
30. U.S. Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," *Treasury.gov.* Accessed on: April 24, 2023. [Online]. Available: https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf
31. "Cryptocurrency: Risk management overview," *Wtwco.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.wtwco.com/-/media/WTW/Insights/2019/01/ cryptocurrency-risk-management-overview.pdf
32. "Blockchain risk management," *Deloitte.com*. Accessed on: April 24, 2023. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/ financial-services/us-fsi-blockchain-risk-management.pdf
33. M. White, "Web3 is Going Just Great," *Web3isgoinggreat.com*. Accessed on: April 24, 2023. [Online]. Available: https://web3isgoinggreat.com/
34. S. Kessler and D. Nelson, "Polygon blockchain nodes briefly went out of sync, affecting explorer, sowing confusion," *CoinDesk*. Accessed on: April 24, 2023. [Online]. Available: https://www.coindesk.com/tech/2023/02/22/polygon-blockchain-suffers-apparent-outage/
35. T. Chang, J. Ho, Z. Tirrell, G. Weng, and J. You, "A risk classification framework for decentralized finance protocols," *Soa.org*. Accessed on: April 24, 2023. [Online].

Available: https://www.soa.org/4aa5bb/globalassets/assets/files/resources/research-report/2022/decentralized-finance-protocols.pdf

36. V. Gaur and A. Gaiha, “Building a Transparent Supply Chain,” *Harvard business review*, 2020.
37. P. Dutta, T.-M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities,” *Transportation Research Part E: Logistics and Transportation Review*, vol. 142, Elsevier BV, p. 102067, Oct. 2020. doi: 10.1016/j.tre.2020.102067.
38. R. Pratik, “How AI and Blockchain transforming supply chain management?,” *Intuz.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.intuz.com/blog/ai-and-blockchain-in-supply-chain-management
39. .L. Compagnucci, D. Lepore, F. Spigarelli, E. Frontoni, M. Baldi, and L. Di Berardino, “Uncovering the potential of blockchain in the agri-food supply chain: An interdisciplinary case study,” *Journal of Engineering and Technology Management*, vol. 65, Elsevier BV, p. 101700, Jul. 2022. doi: 10.1016/j.jengtecman.2022.101700.
40. “Incident report: Rootstock peg-out service outage (Fixed),” *Rsk.com*. Accessed on: April 24, 2023. [Online]. Available: https://blog.rsk.co/noticia/incident-report-rsk-peg-out-service-outage/
41. “Data and analytics,” *ethereum.org*. Accessed on: April 24, 2023. [Online]. Available: https://ethereum.org/en/developers/docs/data-and-analytics/
42. “Network congestion,” *Bybit Learn*. Accessed on: April 24, 2023. [Online]. Available: https://learn.bybit.com/glossary/definition-network-congestion/
43. “Scaling,” *ethereum.org*. Accessed on: April 24, 2023. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/
44. S.D. Lerner, “RSK scalability,” *Innovation Stories*. Accessed on: April 24, 2023. [Online]. Available: https://medium.com/iovlabs-innovation-stories/rsk-scalability-c44252f05a4b
45. “State of research: increasing censorship resistance of transactions under proposer/builder separation (PBS),” *HackMD*. Accessed on: April 24, 2023. [Online]. Available: https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance
46. R. Behnke, “How blockchain DDoS attacks work,” *Halborn*. Accessed on: April 24, 2023. [Online]. Available: https://www.halborn.com/blog/post/how-blockchain-ddos-attacks-work.
47. “Forta: a decentralized runtime security solution for automated threat detection and prevention on smart contracts,” *Forta.network*. Accessed on: April 24, 2023. [Online]. Available: https://docs.forta.network/en/latest/2022-7-11%20Forta%20Litepaper.pdf
48. Forta, “How to use Forta’s Threat Intel Data,” *Notion*. Accessed on: April 24, 2023. [Online]. Available: https://forta.notion.site/How-Forta-alerted-on-past-hacks-71e63d933ef5426d92642a8019708d48
49. D. Nelson and M. Hochstein, “Leaked slides show how Chainalysis flags crypto suspects for cops,” *CoinDesk*. Accessed on: April 24, 2023. [Online]. Available: https://www.coindesk.com/business/2021/09/21/leaked-slides-show-how-chainalysis-flags-crypto-suspects-for-cops/
50. “Bitcoin abuse database,” *Bitcoinabuse.com*. Accessed on: April 24, 2023. [Online]. Available: https://www.bitcoinabuse.com/
51. *Etherscan.io*. Accessed on: April 24, 2023. [Online]. Available: https://etherscan.io/
52. N. Tovanich, N. Heulot, J.-D. Fekete, and P. Isenberg, “Visualization of Blockchain Data: A Systematic Review,” *IEEE Transactions on Visualization and Computer Graphics*, vol. 27, no. 7, pp. 3135–3152, Jul. 01, 2021. doi: 10.1109/tvcg.2019.2963018.
53. J.S. Tharani, E.Y.A. Charles, Z. Hou, M. Palaniswami, and V. Muthukkumarasamy, “Graph Based Visualisation Techniques for Analysis of Blockchain Transactions,” *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, Oct. 04, 2021. doi: 10.1109/lcn52139.2021.9524878.

54. “The ultimate guide to graph visualization,” *Cambridge-intelligence.com*. Accessed on: April 24, 2023. [Online]. Available: https://info.cambridge-intelligence.com/graph-visualization-white-paper
55. “Crystal,” *Crystalblockchain.com*. Accessed on: April 24, 2023. [Online]. Available: https://explorer.crystalblockchain.com/
56. “Introducing cross-Chain Investigations to Reactor,” *Chainalysis*. Accessed on: April 24, 2023. [Online]. Available: https://blog.chainalysis.com/reports/cross-chain-investigations/
57. “How cryptomixers allow cybercriminals to clean their ransoms,” *Intel471*. Accessed on: April 24, 2023. [Online]. Available: https://intel471.com/blog/ cryptomixers-ransomware
58. “Blockchain bridges: An industry overview,” *Rsk.com.* Accessed on: April 24, 2023. [Online]. Available: https://blog.rsk.co/noticia/blockchain-bridges-an-industry-overview/
59. T. Tironsakkul, M. Maarek, A. Eross, and M. Just, “Tracking Mixed Bitcoins,” *arXiv*, 2020. doi: 10.48550/ARXIV.2009.14007.
60. M. J. Shayegan and H. R. Sabor, “A Collective Anomaly Detection Method Over Bitcoin Network.” arXiv, 2021. doi: 10.48550/ARXIV.2107.00925.
61. Z. Wu, J. Liu, J. Wu, Z. Zheng, and T. Chen, “TRacer: Scalable Graph-based Transaction Tracing for Account-based Blockchain Trading Systems,” IEEE Transactions on Information Forensics and Security. Institute of Electrical and Electronics Engineers (IEEE), pp. 1–1, 2023. doi: 10.1109/tifs.2023.3266162.
62. J. Siegenthaler, *Blockchain Clustering with Machine Learning*. Switzerland: University of Basel, 2020.
63. “Top 32 blockchain analysis tools,” *Startup Stash*. Accessed on: April 24, 2023. [Online]. Available: https://startupstash.com/blockchain-analysis-tools/
64. “Verifying smart contracts,” *ethereum.org*. Accessed on: April 24, 2023. [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/verifying/
65. “Bytecode Decompilation,” *Contract Library*. Accessed on: April 24, 2023. [Online]. Available: https://library.dedaub.com/decompile
66. “Online Solidity Decompiler,” *Online Solidity Decompiler*. Accessed on: April 24, 2023. [Online]. Available: https://ethervm.io/decompile/
67. *OpenChain Monorepo*. Accessed on: April 24, 2023. [Online]. Available: https://github.com/openchainxyz/openchain-monorepo
68. @w1nt3r_eth, “A list of power tools (and their hidden features) that security researchers use to investigate hacks,” *Twitter*. Accessed on: April 24, 2023. [Online]. Available: https://twitter.com/w1nt3r_eth/status/1597998923226177543
69. “EVM tracing,” *go-ethereum*. Accessed on: April 24, 2023. [Online]. Available: https://geth.ethereum.org/docs/developers/evm-tracing
70. “Announcing our fully featured, portable solidity debugger,” *Trufflesuite.com*. Accessed on: April 24, 2023. [Online]. Available: https://trufflesuite.com/blog/announcing-full-portable-solidity-debugger/
71. ConsenSys Diligence, “Static and dynamic analysis - ethereum smart contract best practices,” *Github.io*. Accessed on: April 24, 2023. [Online]. Available: https://consensys.github.io/smart-contract-best-practices/security-tools/static-and-dynamic-analysis/
72. J. Feist, G. Grieco, and A. Groce, “Slither: A Static Analysis Framework for Smart Contracts,” *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. IEEE, May 2019. doi: 10.1109/wetseb.2019.00008.
73. “Fuzzing,” *ConsenSys Diligence*. Accessed on: April 24, 2023. [Online]. Available: https://consensys.net/diligence/fuzzing/

74. G. Grieco, W. Song, A. Cygan, J. Feist, and A. Groce, “Echidna: effective, usable, and fast fuzzing for smart contracts,” *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*. ACM, Jul. 18, 2020. doi: 10.1145/3395363.3404366.
75. M. Mossberg et al., “Manticore: A User-Friendly Symbolic Execution Framework for Binaries and Smart Contracts,” *2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, Nov. 2019. doi: 10.1109/ase.2019.00133.
76. “MythX: Preparing for a smart contract audit,” *Mythx.io*. Accessed on: April 24, 2023. [Online]. Available: https://mythx.io/about/
77. “GPT-4,” *Openai.com*. Accessed on: April 24, 2023. [Online]. Available: https://openai.com/product/gpt-4
78. S. Bubeck et al., “Sparks of Artificial General Intelligence: Early experiments with GPT-4,” *arXiv*, 2023. doi: 10.48550/ARXIV.2303.12712.
79. D. Guido, “Codex (and GPT-4) can’t beat humans on smart contract audits,” *Trail of Bits Blog*. Accessed on: April 24, 2023. [Online]. Available: https://blog.trailofbits.com/2023/03/22/codex-and-gpt4-cant-beat-humans-on-smart-contract-audits/

Received 12.05.2023

INFORMATION ON THE ARTICLE

Yaroslaw Yu. Dorogyy, ORCID: 0000-0003-3848-9852, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Ukraine, e-mail: argusyk@gmail.com

Vadym Yu. Kolisnichenko, ORCID: 0009-0009-6472-2807, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Ukraine, e-mail: vadym.kolisnichenko@gmail.com

АНАЛІЗ БЛОКЧЕЙН-ТРАНЗАКЦІЙ: КОМПЛЕКСНИЙ ОГЛЯД ЗАСТОСУВАНЬ, ЗАВДАНЬ ТА МЕТОДІВ / Я.Ю. Дорогий, В.Ю. Колісніченко

Анотація. Аналіз блокчейн-транзакцій є потужним інструментом для отримання інформації про дії та поведінку учасників у блокчейн-мережах. Розглянуто застосування, завдання та методи, пов’язані з аналізом блокчейн-транзакцій. Розглянуто різні способи використання аналізу транзакцій, починаючи від його інструментальної ролі в розробленні блокчейн-систем і закінчуючи його ключовим значенням у сфері кримінальних розслідувань. Із використанням загальних методів і технології, що застосовуються у ході такого аналізу, розкрито приховані уявлення та знайдено інформацію, яка є неочевидною. Мета рукопису – всебічний погляд на важливе значення аналізу блокчейн-транзакцій із розкриттям його ключової ролі у криптовалютній індустрії та широкий спектр застосувань поза нею.

Ключові слова: блокчейн-транзакції, аналіз транзакцій, відстеження транзакцій, аналіз потоків, блокчейн криміналістика.