DOI: 10.55643/fcaptp.4.57.2024.4500

Serhiy Lyeonov
D.Sc. in Economics, Professor of the Department of Economic Cybernetics, Sumy State University, Sumy, Ukraine;
e-mail: serhiy.lyeonov@polsl.pl
ORCID: 0000-0001-5639-3008
(Corresponding author)

Milos Tumpach
PhD in Economics, Professor of the Faculty of Business and Management, Brno University of Technology, Brno, Czech Republic;
ORCID: 0000-0003-3389-6803

Gabriella Loskorikh
PhD in Economics, Associate Professor of the Department of Accounting and Auditing, Ferenc Rakoczi II Transcarpathian Hungarian College of Higher Education, Beregove, Ukraine;
ORCID: 0000-0002-5402-7220

Hanna Filatova
PhD in Economics, Assistant of the Department of Accounting and Taxation, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-7547-4919

Yaroslav Reshetniak
Assistant of the Department of Economics, Entrepreneurship and Business Administration, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0003-0806-0801

Ruslan Dinits
PhD Student of the Department of Economic Cybernetics, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-9785-2167

Received: 26/06/2024
Accepted: 19/08/2024
Published: 31/08/2024

© Copyright
2024 by the author(s)

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

NEW AML TOOLS: ANALYZING ETHEREUM CRYPTOCURRENCY TRANSACTIONS USING A BAYESIAN CLASSIFIER

ABSTRACT

The emergence of cryptocurrencies as a form of digital payments has contributed to the emergence of numerous opportunities for the implementation of effective and efficient financial transactions, however, new fraud and money laundering schemes have emerged, as the anonymity and decentralization inherent in cryptocurrencies complicate the process of monitoring transactions and control by governments and law enforcement agencies. This study aims to develop a mechanism for analyzing transactions in the Ethereum cryptocurrency using a Bayesian classifier to identify potentially suspicious transactions that may be related to terrorist financing and money laundering. The Bayesian approach makes it possible to consider the probabilistic characteristics of transactions and their interrelationships to increase the accuracy of detecting anomalous and potentially illegal transactions. For the analysis, data on transactions of the Ethereum currency from June 2020 to December 2022 were taken. The developed mechanism involves determining a set of characteristics of transaction graph nodes that identify the potential for their use in illegal financial transactions and forming intervals of their permissible values. The article presents cryptocurrency transactions as an oriented graph, with the nodes being the entities conducting transactions and the arcs being the transactions between the nodes. In assessing the risks of using cryptocurrencies in money laundering, the number/amount of transactions to and from the respective node, the balance of these transactions (absolute value), and the type of node were considered. The analysis showed that among the 100 largest nodes in the network, 11 were identified as having a «critical» risk level, and the most closely connected nodes were identified. This methodology can be used not only to analyze the Ethereum cryptocurrency but also for other cryptocurrencies and similar networks.

Keywords: cryptocurrency, Ethereum, blockchain, terrorist financing, money laundering, transaction analysis, Bayesian classifier

JEL Classification: D73, G28, O33, F52

INTRODUCTION

Today, money laundering is one of the key threats to the global economy, undermining the stability of financial systems and facilitating the financing of terrorism and organized crime. Existing methods of combating money laundering usually focus on identifying suspicious transactions in banking systems and other financial institutions (Benachour and Tarhlissia, 2024). However, the emergence of cryptocurrencies has led to new and unique challenges. The use of cryptocurrencies for money laundering poses significant risks. Many cryptocurrency platforms do not require users to disclose personal information, which allows criminals to conceal their identities. For example, LocalBitcoins, before amending its policies, allowed users to buy and sell Bitcoin without going through the Know Your Customer (KYC) procedure. This made the platform popular among those who wished to remain anonymous. According to research, until 2019, a significant portion of illegal Bitcoin transactions were conducted through platforms that did not require KYC. In general, a significant number of crypto exchanges are decentralized and do not require users to undergo KYC procedures. In particular, users can interact with the platform using crypto wallets (e.g., MetaMask) that are not tied to their personal data.

On the one hand, this allows them to remain anonymous, but on the other hand, it leads to the realization of criminal actions.

Another risk arising with the emergence of cryptocurrencies is the difficulty of tracing them. As a rule, crypto transactions are carried out using specialized tools that conceal the origin and/or destination of crypto transactions by mixing funds from a random and large number of users, making the process of tracking transactions almost impossible. Examples of such tools include mixers (such as CoinJoin) or obfuscators.

In addition, it is worth mentioning that a significant part of cryptocurrencies is endowed with an extremely important property for the current digital conditions – the property of instant implementation of transactions. Unfortunately, this feature is also useful for attackers, because such a speed of any operations with cryptocurrencies complicates the process of detecting illegal actions in real time.

Thus, developing cryptocurrencies and blockchain technology opens up vast opportunities for financial transactions without being tied to traditional financial institutions (Zarutska et al., 2024). At the same time, this anonymity creates potential risks of misuse of such transactions for terrorist financing and money laundering.

It should be noted that the analysis of cryptocurrency transactions for their legality is one of the key tasks facing scientists and practitioners today. In general, the existing methods of analyzing digital currency transactions are based solely on heuristic techniques. That is, most of the existing monitoring and control methods do not take into account or only partially take into account the previously listed properties inherent in cryptocurrency transactions. The complexity of the transaction structure in the blockchain is also not taken into account. Therefore, it is important to develop a mechanism that would not only allow responding to potentially suspicious transactions but also allow the data to analyze a large flow of historical transaction data.

LITERATURE REVIEW

Money laundering is one of the most severe threats to financial security, ranking third in the world in terms of risk after drug trafficking and financial fraud (Kozhushko (2023). Therefore, it is not surprising that the scientific literature contains numerous studies on money laundering and the impact of such illegal operations on the country's and society's development.

In general, the analysis of research and publications on this topic demonstrates the complexity and multifaceted nature of this problem and the importance of a comprehensive approach to its solution. It should be noted that the predominant part of scientific research on the topic under study is devoted to the impact of money laundering operations on the economic and financial security of the country and their transformation under the influence of the digitalization of the economy (Dluhopolskyi & Danyliuk (2023)).

At the same time, Djouadi et al. (2024), Alabdullah (2023) and Mazurenko et al. (2023b) have shown in their studies that money laundering primarily reduces the efficiency of economic systems and scares away investors. Shafranova et al. (2024), Mazurenko et al. (2023a), and Dobrovolska et al. (2021) emphasized that money laundering operations distort market and intuitive mechanisms, making them inefficient and illegitimate, which ultimately leads to the collapse of the country's economic system.

An innovative study – by Dobrovolska et al. (2024c), in which researchers examined the impact of the shadow economy, harsh court sentences for corrupt officials, tax pressure, and restrictions on business on creating a fair investment environment.

Studies that consider different types of money laundering transactions are essential. For example, Shafranova et al. (2024) distinguished between structured laundering transactions, transactions through fictitious companies, speculative transactions with the purchase and subsequent resale of real estate, the use of offshore accounts and companies, and illegal transactions with cryptocurrencies and securities. It should be noted that this typology is the most common, but it needs to be more comprehensive and requires further research. At the same time, it is essential to consider not only the types (kinds) of money laundering operations but also to study their impact on state institutions and financial security. An example of such a study is Djalilov et al. (2015).

It is also worth mentioning that it is impossible to study the concept of money laundering without studying its relationship with banking transactions since, in fact, most of such illegal transactions are carried out through banking institutions.

In particular, Vasilyeva et al. (2016) and Leonov et al. (2019) emphasized the need to analyze banks' financial transactions to identify suspicious patterns and anomalies that may indicate money laundering and other corruption schemes.

A separate area of research is considering the impact of rising corruption and money laundering on society and the innovation potential of the economy (Vasylieva and Kasyanenko, 2013). Leonov et al. (2014) and Kuzior et al. (2022) note that money laundering leads to a decrease in trust in financial institutions, increased social inequality, demotivation, and reduced social activity, weakening of the legal system, the lower reputation of the country, etc. An interesting study is Kovbasyuk et al. (2024), in which the researchers propose to predict the corrupt actions of public officials, taking into account both ethical and pragmatic approaches.

However, it should be noted that for a comprehensive understanding of the impact of money laundering, it is crucial to consider both economic and social consequences in their inextricable link, as these aspects are closely interconnected and shape the country's overall state. When studying the impact of corruption and money laundering, it is also worth considering the indicators and analyzing the reports published by World Bank experts. As correctly noted by Kuzmenko et al. (2023), such official reports provide essential insights into how money laundering affects the economic and financial security of the state, and they also contain expert comments on possible ways to combat this phenomenon.

The analysis of research and publications shows that, in general, researchers use a variety of research sources (reports of international organizations such as Transparency International and the OECD – Roba & Moulay (2024); publications of other researchers (Zámek and Zakharkina, 2024; Niftiyev and Kheyirkhabarli, 2024; Bilan et al. (2022)). At the same time, methods and tools depend on the purpose of the study. Bozhenko et al. (2023) used a method of modelling corruption perception patterns based on associative rules. Kuzmenko et al. (2020) used bifurcation analysis methods to assess the risks of public institutions laundering money. Djouadi et al. (2024) studied the relationship between money laundering and economic sustainability using dynamic threshold panel data.

One of the most relevant areas of research at the moment is the study of the transformation of money laundering schemes under the influence of digitalization Kuzior et al. (2023), Polishchuk (2023), Castro Iragorri, and Saengchote (2023), Dobrovolska et al. (2024a; 2024b).

At the same time, the critical place among such studies is occupied by those who examine the use of cryptocurrencies for money laundering and the impact of such operations on the economy and society. This topic is simultaneously the most significant and the least researched, given the total number of studies on this topic. However, the topic's novelty can explain the small number of publications.

Reports of the Financial Action Task Force (FATF) (2014, 2015) indicate the main risks of money laundering and terrorist financing associated with virtual currencies.

In general, researchers argue that cryptocurrencies are attractive to criminals due to a number of inherent properties, such as anonymity, decentralization, and cross-border transactions, and the difficulty of tracing the identity of users and sources of funds (Priyadarshi and Singh, 2024). In addition, cryptocurrencies are often used on black markets and darknet platforms (Saengchote & Castro-Iragorri, 2023).

According to Koibichuk & Dotsenko (2023), and Nurgaliyeva et al. (2023), in most countries of the world, cryptocurrency transactions are only partially subject to financial monitoring and regulation by the state and therefore are attractive tools for money laundering. At the same time, in the scientific community, the critical method proposed to be considered for preventing money laundering is using blockchain technologies (Polishchuk et al. (2019)).

Such a lack of development on the part of state authorities is primarily due to the lack of effective tools for analyzing money laundering operations carried out with the help of cryptocurrencies. In this case, the use of a Bayesian classifier to identify potentially suspicious transactions that may be related to terrorist financing and money laundering may be a new effective approach, which emphasizes the need for further research in this area.

AIMS AND OBJECTIVES

This study aims to develop a methodology for analyzing transactions in the Ethereum cryptocurrency using a Bayesian classifier to identify potentially suspicious transactions related to terrorist financing and money laundering. This methodology can be used not only to analyze the Ethereum cryptocurrency but also for other cryptocurrencies and similar networks.

DOI: 10.55643/fcaptp.4.57.2024.4500

To achieve this goal, the following tasks were set:

- to analyze the issues of money laundering and terrorist financing through crypto transactions;
- to develop an algorithm for analyzing crypto transactions using a Bayesian classifier;
- to conduct a study based on data on Ethereum currency transactions to identify potentially suspicious transactions that may be related to terrorist financing and money laundering.

METHODS

Cryptocurrency transactions can be represented as a directed graph, with the nodes being the entities carrying out the transactions and the arcs being the transactions between the nodes.

Nodes are characterized by the amount on the account and the type, which will be described below. Arcs are characterized by the amount of transactions between two nodes, respectively.

Thus, it is proposed to form the following system of 6 indicators for assessing the risks of using cryptocurrency for money laundering and terrorist financing for the nodes of the graph:

- $K1$ – the number of transactions to this node;
- K2 is the number of transactions from this node;
- $K3$ – the amount of transactions to this node;
- $K4$ – the amount of transactions from this node;
- $K5$ – transaction balance (absolute value);
- $K6$ – node type.

Consider the methodology for calculating each of these node characteristics:

- $K1$ – is calculated as the number of arcs leading to a given node. The information is taken directly from the transaction graph (Financial Action Task Force (FATF) (2014), 2015)).
- This indicator is necessary to consider the fact that a potential criminal will choose a node with a large number of incoming transactions for laundering, so it is more difficult to detect among them. Therefore, a figure that is too high is suspicious.
- $K2$ – is calculated as the number of arcs leading from a given node. The information is taken directly from the transaction graph (Financial Action Task Force (FATF) (2014), 2015)).
- This indicator is mandatory due to the fact that outgoing transactions are an indicator of financial turnover, and too many of them are potentially attractive to criminals. The second reason is that a large number of outgoing transactions may indicate the presence of transaction patterns those criminal elements can use. This makes it necessary to pay attention to nodes with a high score.
- $K3$ – calculated as the sum of the values of all transactions leading to a given node. Similar to $K1$, a high value is more attractive to criminals (Financial Action Task Force (FATF) (2014), 2015)).
- $K4$ – calculated as the sum of the values of all transactions originating from a given node. Similar to $K2$, a high value is more attractive to criminals (FATF (2014, 2015)).
- $K5$ – balance may seem to be an indicator directly related to the previous two. Indeed, if we have a large K3 and a corresponding K4, the balance will be small. However, if the balance is too high, this may indicate potential attempts to accumulate or release large amounts of money (Financial Action Task Force (FATF) (2014), 2015)) (sufficient, for example, to spend on military equipment and the like). Therefore, this indicator should also be taken into account. The indicator is calculated as the absolute value of the difference between $K3$ and $K4$ (formula (1)):

$$K5 = |K3 - K4| \quad (1)$$

where, $K6$ – some node types are always suspicious and require verification.

Node types are specified in the dataset. Nodes with the following types are considered suspicious (Financial Action Task Force (FATF) (2014), 2015)):

1. *Dex (decentralized exchange):* this type of node indicates a decentralized exchange where users can exchange cryptocurrency assets for each other without the mediation of a centralized organization. Such exchanges allow users to trade with each other without having to entrust their funds to a third party (decentralized exchanges can be used to exchange cryptocurrencies anonymously, making them attractive for money laundering or other illegal activities. In addition, due to the lack of regulation, there may be a possibility of price manipulation).
2. *Bridge:* Nodes of the «bridge» type indicate platforms or services that enable cross-platform exchange or integration between different blockchains or cryptocurrency networks. This can include bridges between different blockchains to move assets or exchange between them (a bridge can be used to move funds between different blockchains, which can make it difficult to trace the origin of funds or even be used to move funds from criminal activity to other blockchains).
3. *Derivatives:* such nodes indicate platforms or services that provide the ability to enter into transactions on derivative financial instruments based on cryptocurrencies or blockchain assets. This may include trades in futures, options, swaps, and other derivatives (trading in derivatives may raise suspicion due to the high risk and possibility of speculative transactions that may conceal the true nature of transactions or manipulate the market).
4. *Lending:* «Lending» nodes point to platforms or services that provide lending or borrowing services for cryptocurrencies or stablecoins. Users can use their digital assets as collateral for a loan or lend cryptocurrency in exchange for interest (lending platforms can be used to transfer funds with a high degree of anonymity, making it difficult to trace the origin of funds. In addition, loans can be used to legalize funds or to finance illegal activities).

This study proposes to use a Bayesian classifier to analyze transactions in the Ethereum cryptocurrency. A Bayesian classifier is a powerful machine-learning tool that allows you to classify data based on the probability of events occurring. The proposed model is built based on historical transaction data and its analysis to identify patterns characteristic of potentially suspicious transactions.

In the first stage, a set of characteristics of the nodes of the transaction graph is determined, indicating the potential for using them for money laundering and terrorist financing.

In the second stage, acceptable values are formed for the characteristics identified in the first stage of the study.

In the third stage, binary indicators are formed depending on the values obtained in the second stage. If the indicator is within the permissible limits, it takes the value «0»; otherwise – «1».

The sum of the obtained indicators is an indicator for further calculating the riskiness of a particular node in the graph.

After introducing the general context of our study on using a Bayesian classifier to analyze Ethereum transactions, we turn to the process of generating binary indicators. This research stage is key because it is where we turn the collected data into measuring tools for risk assessment. If we look at each of the three stages, we see a consistent process of converting node characteristics into numerical values and then into binary indicators. This procedure allows objectively determining the degree of risk associated with each node in the graph. Moreover, this methodology is transparent and easily justified enough to be adapted for other similar studies.

So, convert the indicators $K1 - K6$ to binary.

For Ki, $i = 1 \div 5$, the arithmetic mean is used as a separator (formula (2)):

$$K_{bin_i} = \begin{cases} 1 & at\ the\ value \quad K_i > K_{avg_i} \\ 0 & at\ the\ value \quad K_i \le K_{avg_i} \end{cases} \tag{2}$$

For $K6$, as described above, the following separation principle was used (3):

$$K_{bin_6} = \begin{cases} 1 & at\ the\ value \quad K_6 \in \{dex, bridge, derivatives, lending\} \\ 0 & otherwise \end{cases} \tag{3}$$

Using a Bayesian classifier

A Bayesian classifier is a statistical machine learning algorithm that uses Bayes' theorem to classify objects according to certain characteristics. In the context of analyzing cryptocurrency transactions, a Bayesian classifier can be used to identify potentially suspicious transactions by assigning probabilities to each transaction.

DOI: 10.55643/fcaptp.4.57.2024.4500

Typically, Bayesian classifiers are used for binary classification: an object can belong to one of two classes. However, in the context of analyzing cryptocurrency transactions, the possibility of more complex classifications may be appropriate, for example, classifying transactions into 'suspicious' and 'non-suspicious' categories.

A Bayesian classifier builds a probability model for each class based on the training data. Once trained, the model can be used to classify new objects by calculating the probability of each object belonging to each class and selecting the class with the highest probability.

In the context of analyzing cryptocurrency transactions, a Bayesian classifier can help separate potentially suspicious transactions from normal ones, which will contribute to the effective detection of terrorist financing and money laundering.

Denote by $P(H_1)$ the a priori probability that the node is risky and $P(H_2) = 1 - P(H_1)$ – that the node is non-risky. These indicators are determined before the start of the study and are further taken as 0.5. The array of binary data is denoted by $= \{B_i\}$, $i = 1 \div 6$.

The desired a posteriori probability can be calculated using the formula (4):

$$P_B(H_1) = \frac{1}{1+e^{L+\left|\lambda+\ln\frac{P(H_2)}{P(H_1)}\right|}} \quad (4)$$

Where:

$$\lambda = \ln\frac{g}{b} \quad (5)$$

$$L = -2g\lambda \quad (6)$$

Here, b is the probability that the processed data contains the binary value «0», and g – is the probability that the processed data contains the binary value «1».

They are calculated as follows (formula (7)):

$$\begin{aligned} g_k &= \frac{\sum_{k=1}^{n} B_k}{n} \\ b_k &= 1 - g_k \end{aligned} \quad (7)$$

On the basis of the results obtained $P_B(H_1)$, an indicator is obtained – a posterior probability that this node is risky and should be checked taking into account the data obtained.

It is also noteworthy that in cases where the array of binary values consists of only zeros or only ones, it is advisable to calculate its boundary instead of the formula.

The following risk assessment scale is proposed:

- if $0 \le P_B(H1) < 0.3$, normal risk level;
- if $0.3 \le P_B(H1) < 0.5$, an increased level of risk;
- if $0.5 \le P_B(H1) < 0.7$, high risk level;
- if $0.7 \le P_B(H1) \le 1$, critical risk level.

RESULTS

For processing, data on transactions of the Ethereum currency from June 2020 to December 2022 were taken.

Due to the large number of nodes in the graph, 100 nodes with the highest indicator «usdStk» (account in dollars) were selected for the study. Accordingly, $K_i(i = 1 \div 5)$ was calculated considering their average values. For a complete analysis of the graph, due to the unevenness of the distribution, it would be advisable to use the modal or median value instead of the arithmetic mean.

The following results were obtained (Table 1).

Table 1. A posteriori probability of a node being a risky node.

Probability (rounded to 3 decimal places)	Number of nodes
0.000	61
0.105	8
0.240	9
0.500	8
0.558	3
0.745	5
1.000	6

Since this study assumes that these 6 factors can fully determine whether a node is risky, there are several cases with zero and one probability. However, this is only an indicator of riskiness. That is, a one in the probability indicator will only indicate that this node should be monitored. The histogram (Figure 1) shows the distribution of nodes by a posteriori probabilities.

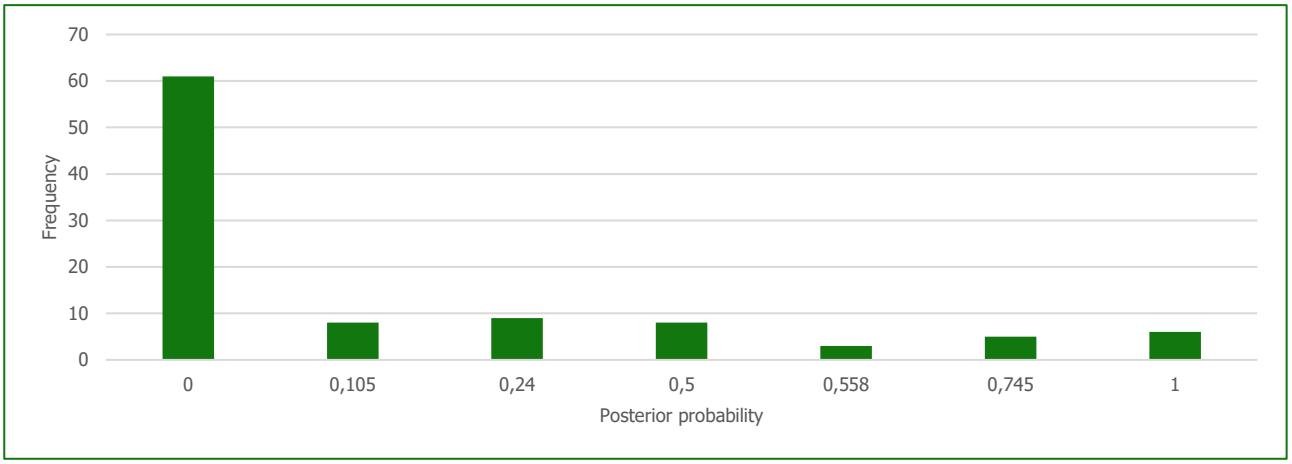

Figure 1. Results of the Bayesian analysis.

Thus, we can observe that most nodes have a zero-risk level. The distribution of nodes by a posteriori probabilities is almost identical. Using the proposed risk assessment scale, we can identify risk groups that will allow us to determine the need for a more thorough analysis of only those nodes that are in the critical risk group. Guided by the principles of a risk-oriented approach, limited resources can be focused on high-risk objects and operations. The advantages of this approach are as follows:

1. This significantly increases the effectiveness of AML measures, as resources are not spent on a thorough analysis of low-risk customers. Prioritization helps reduce the transaction analysis cost and allows you to focus on the most important tasks.
2. With a risk-based approach, organizations can analyze and assess in detail the risks associated with individual customers, products, or services. Risk assessments can be dynamic and consider changes in customer behaviour or the external environment, allowing for a rapid response to new threats.
3. Given that many countries require financial institutions to use a risk-based approach as part of their AML programs. Compliance with these requirements helps avoid fines and other sanctions, and implementing effective AML measures based on risk assessment reduces the likelihood of an institution's involvement in money laundering, which protects its reputation.
4. A risk-based approach allows organizations to quickly adapt their AML strategies in response to new risks or changes in legislation. In addition, each customer or transaction can be assessed individually, allowing for more effective detection and prevention of illegal activity. Implementing a risk-based approach reduces the need to over-collect information from low-risk customers, which increases their loyalty and satisfaction. Low-risk customers experience less stress when going through KYC procedures, making interacting with them more convenient.

DOI: 10.55643/fcaptp.4.57.2024.4500

5. Implementing a risk-based approach reduces the need for excessive information collection from low-risk customers, increasing their loyalty and satisfaction. Low-risk customers experience a lower burden during KYC procedures, which makes interaction with them more convenient.

6. Using modern analytical tools and algorithms for risk assessment allows automation of the process of identifying suspicious transactions and reducing the number of false positives. The risk-based approach allows for predicting potential threats based on analyzing large amounts of data and historical transactions.

A risk-based approach to AML is appropriate because of its ability to use resources more efficiently, improve the accuracy of risk assessment, ensure regulatory compliance, adapt to change, improve customer experience, and increase the effectiveness of suspicious transaction detection. This approach helps regulators and financial institutions create a more effective and flexible AML strategy, which is a key factor in today's dynamic financial environment. The breakdown by risk groups is as follows (Figure 2):

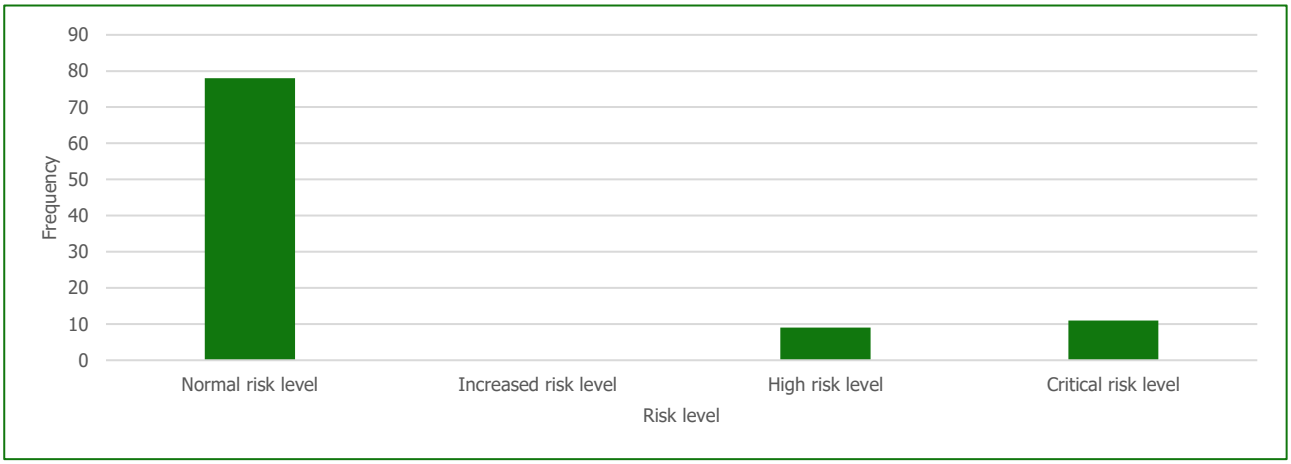

Figure 2. Distribution of nodes by risk groups.

Thus, it is proposed to monitor 11 nodes (Table 2), the risk level of which is defined as «Critical».

Table 2. Identifiers and names of critical nodes.

Node ID	Node Name
2	1inch
5	Ghost
17	Avalanche
24	Binance
40	Compound
45	Curve
5777	Maker
5887	Polygon
5888	Polygonbridge
5900	Sushiswap
5908	Uniswap

AML (Anti-Money Laundering) measures are a key component of the fight against financial crimes such as money laundering and terrorist financing. In order to effectively prevent these crimes, it is important to identify and implement AML measures in accordance with the risk level of the objects of control. Aggregated recommendations for implementing such measures at different risk levels are presented in Table 3.

Table 3. AML procedures and measures for different risk groups.

Risk level	Procedures	Measures
Normal	Know Your Customer (KYC)	Customer identification and collection of basic personal information
		Verification of identity documents (e.g. passport, driver's license)
	Transaction Monitoring	Regular review of transactions to identify suspicious activity
		Using Automated Transaction Monitoring Software
	Staff Training	Regular training of employees on AML policies and procedures
		Familiarization with methods for detecting and responding to suspicious activities
	Reporting	Regular reporting to regulators and compliance with local legal requirements
Increased	Advanced KYC Procedures Additionally	Collection of additional information about the object (for example, sources of income)
		In-depth verification of documents and ties
	In-depth Transaction Monitoring	More frequent and detailed review of transactions
		Using more sophisticated algorithms to identify suspicious patterns
	Risk Assessment	Periodic assessment of risks associated with the facility and its activities
		Using different tools and methods to determine the level of risk
	Enhanced Staff Training	In-depth training of employees to identify more complex money laundering schemes
		Introduction to the latest AML methods and technologies
High	Enhanced KYC Procedures	Conducting due diligence on Politically Exposed Persons (PEPs) and their loved ones
		Gathering more detailed information about financial activities and sources of income
	More Frequent and Thorough Monitoring	Daily or weekly transaction overview
		Use of specialized tools for in-depth analysis of transactions and behavioural models of the object
	Advanced Risk Assessments	In-depth risk analysis and assessment for each high-risk facility
		Introduction of additional control measures, such as restrictions on certain types of transactions
	Specialized Training	Conducting special courses and training for employees working with high-risk clients
		Training on new methods of detecting and combating money laundering
Critical	Enhanced Due Diligence Procedures	In-depth analysis and verification of all aspects of the facility's activities
		Constant updating and verification of information about the object and its activities
	Intensive Transaction Monitoring	Continuous real-time monitoring
		Use of specialized analytical tools to immediately identify suspicious transactions
	Immediate Risk Assessment	Conduct regular and emergency risk assessments for each critical facility
		Imposing measures, such as freezing accounts, pending the completion of the investigation
	Cooperation with Law Enforcement Agencies	Immediately report and cooperate with law enforcement authorities in case of suspicious activity
		Providing all the necessary information for the investigation
	Advanced Training & Certification	Ensuring that all employees working with critical-level customers receive extensive training and certification in AML
		Conduct regular trainings and knowledge updates

Effective implementation of AML measures at different risk levels requires a comprehensive approach that includes thorough customer analysis, ongoing transaction monitoring, regular staff training, and cooperation with regulatory and law enforcement agencies. These measures help detect and prevent illegal financial transactions at all risk levels.

In addition, the data obtained can be further used to analyze other nodes that are not included in the hundred considered. For example, Figure 3 shows 50 nodes (Table 3) that are in direct contact with 10 to 11 critical nodes each, and some of them are also in contact with each other. Since the nodes were evaluated for features that would attract fraudsters in one way or another, it also makes sense to check these nodes.

DOI: 10.55643/fcaptp.4.57.2024.4500

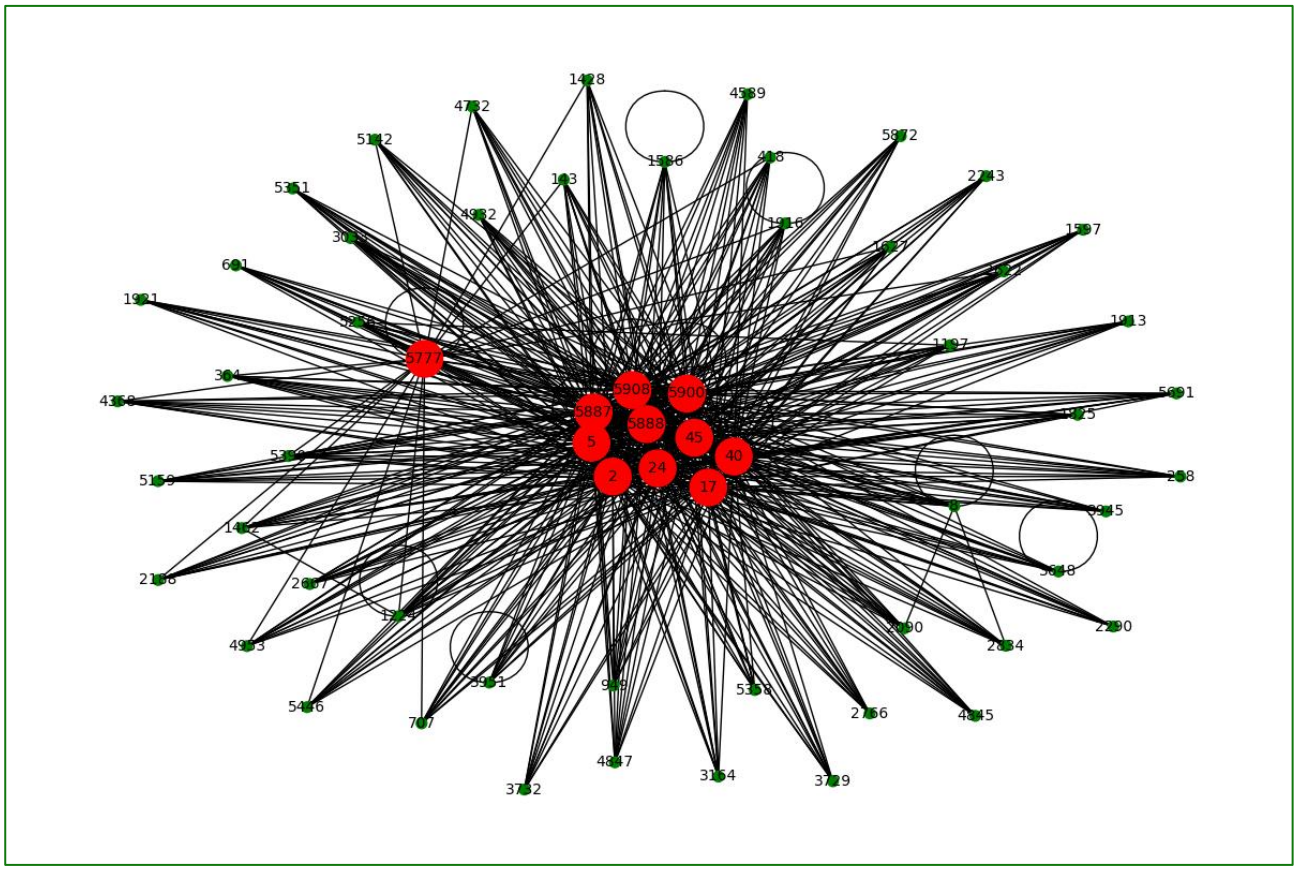

Figure 3. Graph of nodes in close contact with critical ones.

In Figure 3, red indicates critical nodes, and green indicates those in contact with at least 10 of them. Notably, none of the nodes marked in green belong to the ones we have previously investigated. The identified activity is suspicious and, therefore, should be thoroughly investigated.

Table 3. Identifiers and names of nodes that contact at least 10 critical.

Node ID	Node Name	Node ID	Node Name	Node ID	Node Name
1921	eoa0x556d0e	2090	eoa0x5d5d77	3033	eoa0x83b049
258	eoa0x0948f7	1197	eoa0x35fad2	1627	eoa0x472388
8	Alamedaresearch	1586	eoa0x454ebb	3164	eoa0x896bbb
5256	eoa0xe9eb39	691	eoa0x1d32db	5351	eoa0xee1268
2188	eoa0x610bd9	949	eoa0x290aa9	3945	eoa0xad1fb9
5390	eoa0xeff8db	1462	eoa0x40b6ee	2667	eoa0x7431f3
143	eoa0x041272	5691	eoa0xfd7bb4	364	eoa0x0e4606
4368	eoa0xc16ccf	1597	eoa0x45dbe3	4589	eoa0xcad9c9
3729	eoa0xa42856	2622	eoa0x727f85	4845	eoa0xd56683
2834	eoa0x7ae823	3648	eoa0xa09b73	4847	eoa0xd573a9
1428	eoa0x3f2d41	2243	eoa0x6353df	5358	eoa0xee713a
3732	eoa0xa45f5e	707	eoa0x1e1be9	5872	Oapital
5142	eoa0xe3f098	4932	eoa0xda222a	2290	eoa0x6543a9
1825	eoa0x50a068	5446	eoa0xf2a453	3951	eoa0xad6e76
418	eoa0x10c0e4	1224	eoa0x36ffc6	1913	eoa0x54cbd3
5159	eoa0xe51941	2766	eoa0x786a58	4732	eoa0xd03dae
1916	eoa0x5521cf	4953	eoa0xdb1730		

Thus, the results of the analysis of the Ethereum cryptocurrency transactions shown in Figure 3 and their decryption shown in Table 3 make it possible to assert that this scientific and methodological approach is acceptable for use and that the same algorithm can be used to analyze transactions in other cryptocurrencies.

DISCUSSION

Consequently, using cryptocurrencies for terrorist financing and money laundering poses a significant challenge to financial systems and regulators. The findings presented in this paper provide evidence that crypto payments can be used to conceal the origin of such illicit funds, which is consistent with the findings of Niftiyev and Kheyirkhabarli (2024).

In addition, the conclusions presented in this study based on the analysis results are consistent with the generally accepted conclusions presented in the scientific studies of Shafranova et al. (2024), Dobrovolska et al. (2021). However, simultaneously, the results provide new insights into the possibilities of analyzing crypto transactions.

In particular, the study differs conceptually from Djouadi et al. (2024) in focusing exclusively on historical transaction data for the Ethereum cryptocurrency. At the same time, Djouadi et al. (2024) use several variables in their study to analyze the impact of corruption and financial fraud on the country's economy. However, the general conclusions are the same in both scientific works, particularly regarding the negative effects of financial fraud, including through the implementation of crypto payments, on investor confidence and, in general, on the country's financial and economic system.

The critical difference between this study and Niftiyev and Kheyirkhabarli (2024) and Nurgaliyeva et al. (2023) is its practical orientation, i.e., not only an emphasis on understanding the theoretical concepts of the use of cryptocurrencies in illegal financial transactions but also an emphasis on the practical analysis of such transactions to identify potentially suspicious transactions.

Also, compared with previous studies, there are some key differences and innovations in the approach used in this article. In particular, unlike Kuzmenko et al. (2020), which used bifurcation analysis methods to assess the risks of money laundering by public institutions, and Bozhenko et al. (2023), in which researchers used a method of modelling corruption perception patterns based on associative rules, this study uses the Bayesian annihilation method, which is a more appropriate tool for analyzing potentially suspicious crypto transactions from normal ones. The application of this method will contribute to the effective detection of terrorist financing and money laundering committed through cryptocurrencies.

As a solution to address the identified shortcoming in Koibichuk & Dotsenko (2023), regarding the lack of monitoring of cryptocurrency transactions in most countries, this study contains a developed and scientifically based mechanism for analyzing crypto transactions.

Despite the valuable information provided, the study presented in this article has certain limitations, in particular, the analysis was limited by the availability and quality of transaction data for only one cryptocurrency, extracted from only one cryptocurrency exchange. However, this shortcoming can be eliminated by supplementing and implementing further research.

CONCLUSIONS

Within the article's framework, the Ethereum cryptocurrency transaction graph is studied. A methodology has been developed for analyzing transactions in the Ethereum cryptocurrency using a Bayesian classifier to identify potentially suspicious transactions that may be related to terrorist financing and money laundering. The proposed scientific and methodological approach made it possible to identify nodes that are potentially attractive to fraudsters based on intuitive binary indicators: the number of transactions to and from a given node, the amount of transactions to and from a given node, the balance of transactions, and the type of node.

We note that these indicators are the most obvious for use within the industry, and this set can be supplemented or modified depending on the task to which the described tools are applied. Accordingly, this methodology can be used not only to analyze the Ethereum cryptocurrency but also for other cryptocurrencies and similar networks.

Among the 100 largest nodes in the network, 11 were identified as having a risk level that can be assessed as «critical», and the nodes that are most closely connected to them were also identified.

DOI: 10.55643/fcaptp.4.57.2024.4500

Thus, the developed methodology for analyzing crypto transactions using a Bayesian classifier has demonstrated a high degree of efficiency, reliability, and accuracy in detecting suspicious transactions, using the Ethereum cryptocurrency as an example.

Testing the model on accurate data has confirmed the possibility of its use in practical anti-money laundering conditions. In general, the use of the proposed methodology and analysis methodology contributes to increasing the transparency and security of financial crypto transactions, which is an important step in ensuring the financial and economic stability of the country.

Further research could be directed to:

- applying the developed scientific and methodological mechanism to analyze transactions on other cryptocurrencies, such as Bitcoin, Litecoin, etc. Such an extension of the existing research will allow for a more in-depth analysis to identify potentially suspicious transactions that may be related to terrorist financing and money laundering. In general, it should be noted that for further effective development of an efficient system for monitoring, detecting and combating financial fraud, money laundering, and terrorist financing, it is essential to take into account the maximum possible number of key cryptocurrencies and transactions on them;
- integration with existing methods to expand the analysis. In particular, in order to analyze the impact of the identified potentially suspicious crypto transactions on the financial and economic system, it is possible to use additional models that take into account several factors (including those that characterize the financial stability of the country, such as GDP, investments, etc;)
- analyzing the impact of new regulatory measures on the effectiveness of money laundering detection in cryptocurrency networks and developing recommendations for regulatory policy.

It should be noted that when developing any analysis mechanism, it is also important to consider the mechanism of its implementation in real life, which may be the next stage of the study.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Reshetniak Yaroslav, Lyeonov Serhiy*
Data curation: *Filatova Hanna, Dinits Ruslan*
Formal Analysis: *Tumpach Milos, Reshetniak Yaroslav*
Methodology: *Loskorikh Gabriella, Reshetniak Yaroslav, Filatova Hanna, Tumpach Milos*
Software: *Dinits Ruslan, Filatova Hanna*
Resources: *Lyeonov Serhiy, Tumpach Milos*
Supervision: *Lyeonov Serhiy*
Validation: *Reshetniak Yaroslav, Tumpach Milos*
Investigation: *Loskorikh Gabriella, Reshetniak Yaroslav, Filatova Hanna, Tumpach Milos*
Visualization: *Dinits Ruslan, Loskorikh Gabriella*
Project administration: *Lyeonov Serhiy*
Funding acquisition: *Tumpach Milos, Loskorikh Gabriella*
Writing – review & editing: *Lyeonov Serhiy, Tumpach Milos, Reshetniak Yaroslav*
Writing – original draft: *Reshetniak Yaroslav, Filatova Hanna*

FUNDING

This article was supported by the Ministry of Education and Science of Ukraine (project No. 0123U101945 - National security of Ukraine through prevention of financial fraud and money laundering: war and post-war challenges) and VEGA agency (project VEGA 1/0638/23 - Reputationial risk of an auditing company as a reflection of the sentiment on Twitter).

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva,T. (2023). Company Cybersecurity System: Assessment, Risks and Expectations. *Production Engineering Archives, 29*(4), 379-392. https://doi.org/10.30657/pea.2023.29.43
2. Castro Iragorri, C., & Saengchote, K. (2023). Replication Data for: Network Topology in Decentralized Finance. *Universidad del Rosario, V2.* https://doi.org/10.34848/6LQXAQ,
3. Saengchote, K., & Castro-Iragorri, C. (2023). Network Topology in Decentralized Finance. *Documentos de Trabajo, 020782*. https://dx.doi.org/10.2139/ssrn.4469783
4. Financial Action Task Force (FATF). (2015). Financial Action Task Force (FATF). http://www.fatf-gafi.org
5. Financial Action Task Force (FATF). (2014). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. http://www.fatf-gafi.org
6. Alabdullah, T.T.Y. (2023). The impact of financial technology and risk management practices on corporate financial system profitability: evidence from Kuwait. *SocioEconomic Challenges, 7*(3), 141-151. https://doi.org/10.61093/sec.7(3).141-151.2023
7. Benachour, A., & Tarhlissia, L. (2024). The evolution and development of electronic payment in a bank. Case study: CPA-Bank. *Financial Markets, Institutions and Risks, 8*(1), 1-15. https://doi.org/10.61093/fmir.8(1).1-15.2024
8. Bilan, S., Šuleř, P., Skrynnyk, O., Krajňáková, E., & Vasilyeva, T. (2022). Systematic Bibliometric Review of Artificial Intelligence Technology in Organizational Management, Development, Change and Culture. *Business: Theory and Practice, 23*(1), 1-13. https://doi.org/10.3846/btp.2022.13204
9. Bozhenko, A., Krawczyk, D., Hałuszko, K., & Ozarenko, V. (2023). Data-Mining Modeling of Corruption Perception Patterns Based on Association Rules. *Business Ethics and Leadership, 7*(4), 181-189. https://doi.org/10.61093/bel.7(4).181-189.2023
10. Djalilov, K., Lyeonov, S., & Buriak, A. (2015). Comparative studies of risk, concentration and efficiency in transition economies. *Risk Governance and Control: Financial Markets and Institutions, 5*(4CONT1), 178-187. https://doi.org/10.22495/rgcv5i4c1art7
11. Djouadi, I., Zakane, A., & Abdellaoui, O. (2024). Corruption and Economic Growth Nexus: Empirical Evidence From Dynamic Threshold Panel Data. *Business Ethics and Leadership, 8*(2), 49-62. https://doi.org/10.61093/bel.8(2).49-62.2024
12. Dluhopolskyi, O., & Danyliuk, I. (2023). ECONOMIC EVALUATION OF THE ELECTRONIC PUBLIC PROCUREMENT SYSTEM: THE CASE OF PROZORRO 2018-2022. *Socio-Economic Relations in the Digital Society*, *4*(50), 95-111. https://doi.org/10.55643/ser.4.50.2023.517
13. Dobrovolska, O., & Rozhkova, M. (2024a). Development of the Country's Sustainable Cyberspace Strategy to Ensure the Country's National Security. *SocioEconomic Challenges, 8*(2), 197-214. https://doi.org/10.61093/sec.8(2).197-214.2024
14. Dobrovolska, O., Ortmanns, W., Dotsenko, T., Lustenko, V., & Savchenko, D. (2024b). Health Security and Cybersecurity: Analysis of Interdependencies. *Health Economics and Management Review, 5*(2), 84-103. https://doi.org/10.61093/hem.2024.2-06
15. Dobrovolska, O., Sonntag, R., Mynenko, S., & Kosyk, D. (2024c). A Fair Investment Environment: The Impact of the Shadow Economy, the Harshness of the Courts Against Corrupt Officials, Tax Pressure and Restrictions on Business. *Business Ethics and Leadership, 8*(2), 200-218. https://doi.org/10.61093/bel.8(2).200-218.2024
16. Dobrovolska, O., Marhasova, V., Momot, O., Borysova, L., Kozii, N., & Chyzhyshyn, O. (2021). Evolution and current state of money circulation in Ukraine and the world. *Estudios de Economia Aplicada, 39*(5). https://doi.org/10.25115/eea.v39i5.5042
17. Koibichuk, V., & Dotsenko, T. (2023). Content and Meaning of Financial Cyber Security: a Bibliometric Analysis. *Financial Markets, Institutions and Risks, 7*(1), 145-153. https://doi.org/10.21272/fmir.7(1).145-153.2023
18. Kovbasyuk, L., Vakulenko, Y., Ivanets, I., Bozhenko, V., & Kharchenko, D. (2024). Forecast of Corruption: From Ethical to Pragmatic Considerations. *Business Ethics and Leadership, 8*(2), 184-199. https://doi.org/10.61093/bel.8(2).184-199.2024
19. Kozhushko, I. (2023). Transformation of Financial Services Industry in Conditions of Digitalization of Economy. *Financial Markets, Institutions and Risks, 7*(4), 189-200. https://doi.org/10.61093/fmir.7(4).189-200.2023
20. Kuzior, A., Arefiev, S., & Poberezhna, Z. (2023). Informatization of innovative technologies for ensuring macroeconomic trends in the conditions of a circular economy. *Journal of Open Innovation: Technology, Market, and Complexity, 9*(1), 10–20. https://doi.org/10.1016/j.joitmc.2023.01.001
21. Kuzior, A., Arefieva, O., Kovalchuk, A., Brożek, P., & Tytykalo, V. (2022). Strategic Guidelines for the Intellectualization of Human Capital in the Context of Innovative Transformation. *Sustainability, 14*, 11937. https://doi.org/ 0.3390/su141911937
22. Kuzmenko, O., Bilan, Y., Bondarenko, E., Gavurova, B., & Yarovenko, H. (2023). Dynamic stability of the financial monitoring system: Intellectual analysis. *PLoS ONE, 18*(1 January). https://doi.org/10.1371/journal.pone.0276533
23. Kuzmenko, O., Šuleř, P., Lyeonov, S., Judrupa, I., & Boiko, A. (2020). Data mining and bifurcation analysis of the risk of money laundering with the involvement of financial institutions. *Journal of International Studies, 13*(3), 332-339. https://doi.org/10.14254/2071-8330.2020/13-3/22
24. Leonov, S., Frolov, S., & Plastun, V. (2014). Potential of institutional investors and stock market development as an

DOI: 10.55643/fcaptp.4.57.2024.4500

alternative to households' savings allocation in banks. *Economic Annals-XXI, 11-12*, 65-68. http://soskin.info/en/material/1/about-journal.html

25. Leonov, S., Yarovenko, H., Boiko, A., & Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. *Paper presented at the CEUR Workshop Proceedings, 2422*, 297-307. http://ceur-ws.org/
26. Mazurenko, O., Tiutiunyk,I., Grytsyshen, D., Daňo, F., Artyukhov, A., & Rehak, R. (2023a). Good governance: Role in the coherence of tax competition and shadow economy. *Problems and Perspectives in Management*, *21*(4), 757-770. https://doi.org/10.21511/ppm.21(4).2023.56
27. Mazurenko, O., Tiutiunyk, I., Cherba, V., Artyukhov., A., & Yehorova, Y. (2023b). Shadow tax evasion and its impact on the competitiveness of the country's tax system. *Public and Municipal Finance*, *12*(2), 129-142. https://doi.org/10.21511/pmf.12(2).2023.11
28. Mouna, B., & Yassine, M. (2024). Business Leadership in E-Commerce in the USA: The Impact of Blockchain Technology. *Business Ethics and Leadership, 8*(1), 116-128. http://doi.org/10.61093/bel.8(1).116-128.2024
29. Niftiyev, I., & Kheyirkhabarli, M. (2024). The Impact of Covid-19 Pandemic on Cryptocurrency Adoption in Investments: a Bibliometric Study. *SocioEconomic Challenges, 8*(1), 154-169. https://doi.org/10.61093/sec.8(1).154-169.2024
30. Nurgaliyeva, A., Blikhar, M., & Oleksiv, R. (2023). Financial and Legal Principles of Cryptocurrency Market Regulation. *Socio-Economic Relations in the Digital Society*, *3*(49), 116-123. https://doi.org/10.55643/ser.3.49.2023.508
31. Priyadarshi, A., & Singh, P. (2024). Role of FinTech Apps in Increasing Investment Decisions: A Study on the Capital Market. *Financial Markets, Institutions and Risks, 8*(2), 186-197. https://doi.org/10.61093/fmir.8(2).186-197.2024
32. Polishchuk, Y. (2023). FinTech future trends. In monograf: The European Digital Economy: Drivers of Digital Transition and Economic Recovery (1st ed.). Lubacha, J., Mäihäniemi, B., & Wisła, R. (Eds.). Routledge. https://doi.org/10.4324/9781003450160
33. Polishchuk, Y., Ivashchenko, A. & Dyba, O. (2019). Smart-contracts via blockchain as the innovation tool for smes development. *Ikonomicheski Izsledvania, 2*8(6), 39-53. http://www.iki.bas.bg/en/economic-studies-journal-0
34. Roba, M., & Moulay, O. K. (2024). Risk Management in Using Artificial Neural Networks. *SocioEconomic Challenges, 8*(2), 302-313. https://doi.org/10.61093/sec.8(2).302-313.2024
35. Shafranova, K., Navolska, N., & Koldovskyi, A. (2024). Navigating the digital frontier: a comparative examination of Central Bank Digital Currency (CBDC) and the Quantum Financial System (QFS). *SocioEconomic Challenges, 8*(1), 90-111. https://doi.org/10.61093/sec.8(1).90-111.2024
36. Tiutiunyk, I., Mazurenko, O., Spodin, S., Volynets, R., & Hladkovskyi, M. (2022). The Nexus Between International Tax Competitiveness and the Shadow Economy: a Cross-Countries Analysis. *Financial and Credit Activity Problems of Theory and Practice*, *1*(42), 196–205. https://doi.org/10.55643/fcaptp.1.42.2022.3703
37. Vasilyeva, T., Sysoyeva, L., & Vysochyna, A. (2016). Formalization of factors that are affecting stability of ukraine banking system. *Risk Governance and Control: Financial Markets and Institutions, 6*(4), 7-11. https://doi.org/10.22495/rcgv6i4art1
38. Vasylieva, T. A., & Kasyanenko, V. O. (2013). Integral assessment of innovation potential of Ukraine's national economy: A scientific methodical approach and practical calculations. *Actual Problems of Economics, 144*(6), 50-59. https://www.scopus.com/record/display.uri?eid=2-s2.0-84923539973&origin=resultslist
39. Zámek, D., & Zakharkina, Z. (2024). Research Trends in the Impact of Digitization and Transparency on National Security: Bibliometric Analysis. *Financial Markets, Institutions and Risks, 8*(1), 173-188. https://doi.org/10.61093/fmir.8(1).173-188.2024
40. Zarutska, O., Dobrovolska, O., Masiuk, I., Sonntag, R., & Ortmanns, W. (2024). Risk management through a Kohonen map bank business model survey: The case of Ukraine. *Banks and Bank Systems*, *19*(2), 221-233. https://doi.org/10.21511/bbs.19(2).2024.18

Леонов С., Тумпач М., Лоскоріх Г., Філатова Г., Решетняк Я., Дініц Р.

НОВІ ІНСТРУМЕНТИ БОРОТЬБИ З ВІДМИВАННЯМ ГРОШЕЙ: АНАЛІЗ ТРАНЗАКЦІЙ ІЗ КРИПТОВАЛЮТОЮ ETHEREUM ЗА ДОПОМОГОЮ БАЙЄСІВСЬКОГО КЛАСИФІКАТОРА

Поява криптовалют як однієї з форм цифрових розрахунків сприяла виникненню численних можливостей для реалізації оперативних та ефективних фінансових операцій, утім одночасно з їх появою утворилися нові схеми шахрайств і відмивання коштів, адже анонімність і децентралізація, що притаманні криптовалютам, ускладнюють процес моніторингу транзакцій і контролю з боку урядів та правоохоронних органів. Метою цього дослідження є розроблення механізму аналізу транзакцій у криптовалюті Ethereum із використанням байєсівського класифікатора для виявлення потенційно підозрілих операцій, що можуть бути пов'язані з фінансуванням тероризму та відмиванням незаконних доходів. Застосування байєсівського підходу дозволяє враховувати ймовірнісні характеристики транзакцій та їхні взаємозв'язки, підвищити точність виявлення аномальних і потенційно незаконних операцій. Для аналізу взято дані про транзакції валюти Etherum від червня 2020 року до грудня 2022. Розроблений механізм передбачає

визначення набору характеристик вузлів графу транзакцій, що ідентифікують потенційну можливість їх використання в незаконних фінансових операціях, формування інтервалів їхніх допустимих значень. Транзакції в криптовалюті у статті представлено у вигляді орієнтовного графу, вузлами якого є суб'єкти, що здійснюють транзакції, а дугами – безпосередньо самі транзакції між вузлами. При оцінюванні ризиків використання криптовалюти в процесах легалізації кримінальних доходів ураховано кількість / суму транзакцій до та від відповідного вузла, сальдо цих транзакцій (абсолютне значення) й тип вузла. Результати аналізу продемонстрували, що серед 100 найбільших вузлів мережі виявлено 11 таких, рівень ризику яких можна оцінити як «критичний», а також виявлено ті вузли, що найбільш тісно з ними контактують. Ця методика може бути використана не лише для аналізу криптовалюти Etherum, але й для інших криптовалют і подібних мереж.

Ключові слова: криптовалюта, Ethereum, блокчейн, фінансування тероризму, відмивання коштів, аналіз транзакцій, байєсівський класифікатор

JEL Класифікація: D73, G28, O33, F52

DOI: 10.55643/fcaptp.4.57.2024.4500