UDC 004.056

# An Algorithm for Analyzing the Ethereum Network Blockchain to Detect Illegal Activities

Esmira Abdullaieva[1,a], Leonid Galchynsky[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»*
*Educational and Research Institute of Physics and Technology*

## Abstract

This work is devoted to the research of the blockchain network, in particular, aimed at detecting illegal activity in the Ethereum network using forensic methods. The paper describes the concepts and basic vulnerabilities related to the Ethereum network and the integration of graph analysis to develop an algorithm that scrutinizes Ethereum's transaction structure for illegal activities, including money laundering. In addition, the study includes an analysis of the very structure of Ethereum and the blockchain, which allows insight into the identification and analysis of various aspects of their functioning. The research results are used for the software implementation of the study and improvement of the security level of the blockchain network, including the creation of advanced software solutions for network analysis and protection of the integrity of the blockchain ecosystem. This integrated methodology aims to protect the integrity of blockchain ecosystems.

Keywords: blockchain, network analysis, Ethereum, money laundering, forensics, integrated approach

## Introduction

Blockchain technology, hailed as one of the most disruptive advances of the digital age, has rapidly reshaped various industries worldwide. Its decentralised architecture, immutable ledger, and cryptographic security have laid the foundation for innovation. Ethereum, in this context, stands as a beacon of progress, constantly pushing the boundaries of what is achievable with intelligent contracts and decentralized applications.

However, along with its rapid development, the rise in popularity of blockchain has also revealed its dark side. The qualities that make it so powerful—anonymity, accessibility, and decentralization—unwittingly create fertile ground for criminals to engage in illegal activities, including money laundering. This highlights a complex challenge facing the blockchain community: harnessing its transformative potential while preventing exploitation.

As blockchain continues to permeate society, addressing these vulnerabilities becomes not only a regulatory compliance issue but a fundamental prerequisite for its sustainable development. Only by working to improve transparency, security protocols, and the regulatory framework can we balance innovation and accountability and ensure blockchain continues to drive positive change in the global landscape[1].

## 1. Overview of the Ethereum protocol

Ethereum is an open-source blockchain platform that allows developers to create and deploy smart contracts and decentralized applications (dApps). Each node in the network maintains a copy of the registry, and consensus is reached through a decentralized mechanism that ensures trust and security. Each node on the Ethereum network maintains a full copy of the blockchain, which serves as a distributed ledger that records all intelligent contract transactions and interactions. Consensus is achieved through a decentralized mechanism that ensures trust and security across the network. This decentralized approach means no one person controls the network, making it resistant to censorship and interference. Having conducted a detailed review of the Ethereum network, it is possible to highlight the main concepts of the protocol[2, 3]:

- Decentralized Applications (dApps): These applications built on the Ethereum blockchain take advantage of its decentralized nature and innovative contract capabilities. dApps enable trusted interactions between users without intermediaries or central authorities. They cover many use cases, including decentralized finance (DeFi), gaming, and decentralized autonomous organizations (DAOs).
- Smart contracts: are self-executing contracts with terms encoded directly into the code. When certain events occur, they automatically apply predefined conditions and perform actions. Smart contracts reduce the likelihood of human error or manipulation and allow for the automation of various processes.
- Ethereum Virtual Machine (EVM): EVM is a decentralized execution environment that executes Smart Contracts on the Ethereum network. It is a

[a]esmira.abdullaeva@gmail.com

universal runtime environment and offers a standardized platform for executing code in Ethereum intelligent contract languages such as Solidity. EVMs ensure the security and integrity of brilliant contract execution by isolating each contract in its isolated software environment. This allows other contracts or external sources to intervene.

- Consensus mechanism: Ethereum initially used a Proof of Work (PoW) consensus mechanism similar to Bitcoin, in which miners must solve complex mathematical puzzles to confirm transactions and add new blocks to the blockchain. Ethereum 2.0 moves to a more scalable consensus mechanism known as Proof of Stake (PoS). PoS relies on validators elected to create new blocks and secure the network based on the amount of cryptocurrency they have and are willing to betäs collateral. Compared to PoW, PoS has greater scalability, security, and less energy, making it ideal for the future development of the Ethereum network.

## 1.1. Functionality of the Ethereum protocol

In Ethereum, the system is based on interaction between accounts, each with a unique 20-byte address. These accounts interact by exchanging values and data, resulting in changes to the system's overall state. An account description typically includes the following components[3, 4]:

- Nonce: A numeric counter that ensures the uniqueness of each transaction, thus preventing reuse.
- Ether Balance: Displays the current amount of currency stored in the account.
- Contract Code: Contains the executable code for the contract accounts, if applicable.
- Data Storage: The account's internal memory is initially empty.

A transaction is created on the Ethereum network to send ether (the cryptocurrency used in Ethereum or interact with smart contracts. This transaction is like a digital message that tells the network what operation will be performed. Transactions are the core of the Ethereum network, simplifying the transfer of cryptocurrency and the execution of smart contracts. Each transaction has several components that determine its behavior and impact on the Ethereum blockchain. Constituent transactions:

- Sender Address: Identifies the account that initiated the transaction.
- Recipient address: specifies the recipient of the message or funds.
- Ethereum Amount: This is the amount of Ethereum that will be transferred during the transaction.
- Data Field: This optional field may contain additional information or parameters required for the transaction. For standard wireless transmission, this field is usually empty. Smart contract interaction can contain coded function calls and parameters.
- Gas limit (STARTGAS): defines the maximum amount of gas the sender is willing to consume for the transaction. Gas represents the computing resources required to complete a transaction.
- Gas price (GASPRICE): indicates the price the sender is willing to pay for a gas unit. This determines the transaction fee and affects its priority for inclusion in blocks.
- Nonce: A unique number associated with the sender's account that ensures the uniqueness of each transaction from that account. This prevents repeated attacks and ensures the order of operations on the account.

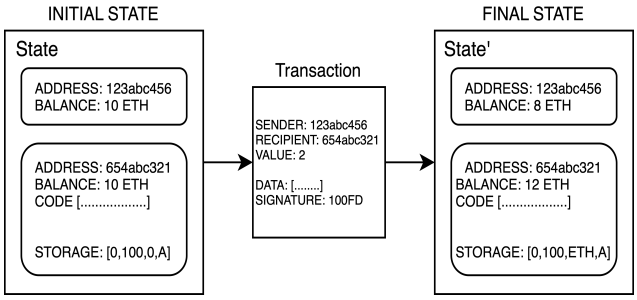


Figure 1. State transition function

One of the main elements of Ethereum is the state transition function (Fig. 1)[5], which is essentially called during the execution of a transaction. This function defines how the state of the contract changes in response to a transaction. The transition from one state to another is governed by the rules and logic programmed into the smart contract. Ethereum's state transition function, APPLY(S, TX) -> S', can be defined as the process in which the current blockchain state S is changed to a new state S' due to applying a TX transaction. This process includes several key steps that ensure validation, execution of transactions, and state changes according to Ethereum rules.

Ethereum's security relies heavily on the security of its smart contracts, including its state transition functionality. Vulnerabilities in smart contracts can lead to security breaches and loss of funds. Because Ethereum is permissionless, anyone can deploy smart contracts, increasing the risk of attackers deploying or exploiting vulnerabilities. The state transition feature extends the attack surface of smart contracts, making thorough testing and auditing critical to identifying and remediating potential security flaws.

Additionally, smart contracts are immutable after deployment, highlighting the importance of securing the transaction transition function before deployment. Any vulnerabilities or flaws in the function's code cannot be patched after deployment, leaving the contract vulnerable to exploitation. The Ethereum network validates transactions by performing a state transition function, making it critical to maintain the integrity and security of these functions to ensure the overall security of Ethereum.

Unauthorized access to funds or confidential data in smart contracts can facilitate the laundering of ill-

gotten funds by transferring them through multiple accounts or converting them into different cryptocurrencies. Exploiting vulnerabilities such as re-entry attacks or transaction manipulation can further aid in manipulating transactions to hide the source or destination of funds involved in money laundering schemes.

### 1.2. The main vulnerabilities of the Ethereum protocol

As a decentralized platform, Ethereum has its own set of vulnerabilities and problems. Some of the vulnerabilities of the Ethereum protocol are presented below[2, 6]:

1. Vulnerabilities of smart contracts. The guarantee of execution of the agreement will correspond to the logic prescribed in the smart contract. After executing the predefined logic, the final state of the network will remain unchanged. However, the correct execution of the smart contract code cannot guarantee its complete security. Key vulnerabilities can be considered[7]:
   - Coding errors: smart contracts are written in different programming languages, requiring developers to be careful. Any errors in the code can lead to undesirable consequences, including loss of funds or unauthorized access.
   - Re-entry Attacks: An attack that occurs when an attacker successfully attempts to repeatedly call a function in a smart contract before its initial execution is complete.
   - Manipulation of timestamps: control of timestamps by miners can lead to potential manipulations that will affect the outcome of the smart contract execution.
   - Lack of privacy: The information on the blockchain is publicly available, so access to the smart contract code may cause privacy issues.
   - Risks of Centralization: While decentralizing the blockchain, smart contracts may rely on centralized services or components that may create single points of failure or trust.
2. Privacy Issues: Although Ethereum transactions are pseudonymous, meaning they are not directly linked to actual individuals, transaction patterns and metadata can still be analyzed to identify relationships between addresses and potentially reveal illegal activity. However, privacy-enhancing techniques and ring signatures can mask transaction details and increase anonymity, creating opportunities for money laundering.
3. Decentralized Exchanges (DEX): Decentralized exchanges built on Ethereum allow users to trade cryptocurrencies without the need for centralized intermediaries. While this facilitates decentralization and resistance to censorship, it also creates challenges for regulatory oversight and compliance, potentially facilitating money laundering through anonymous trading and cross-border transactions.
4. Tokenization: The Ethereum platform allows the creation of custom tokens using smart contracts that can represent various digital assets, securities, or tokens tied to real-world assets. Tokenization can be used to launder money by issuing and transferring tokens to hide the flow of funds and bypass traditional regulatory controls.

Researchers from different countries proposed various methods of combating attackers who use vulnerabilities in the Ethereum network[2, 6]. In this work, we will focus on one of the problems of this network.

## 2. The problem of money laundering in the Ethereum network

Money laundering is a concern in Ethereum due to its pseudonymous nature. Although all transactions are visible on the blockchain, participants' identities are not necessarily linked to their addresses. This allows criminals to hide the source of their funds. The decentralized nature of the blockchain and pseudonymous transactions on the Ethereum network create significant obstacles to combating money laundering. Research results of recent years have shown the following opportunities for abuse of this type[2, 1, 8].

- Pseudonymity: Ethereum transactions are conducted between cryptographic addresses, not real persons. Although addresses can be traced, they often do not directly reveal the identity of the person or organization behind them. This makes attributing transactions to specific participants difficult, promoting anonymity for potential money launderers.
- Sophisticated transaction schemes: Money launderers often use sophisticated methods to hide the origin and destination of funds. They may use mixing services, tumblers, or multiple intermediaries to hide the trail of transactions, making it challenging to trace illicit funds through the network.
- Smart Contracts: Ethereum's smart contracts feature enables the creation of complex financial instruments and decentralized applications (DApps). While they can offer innovative solutions, they also create opportunities for money laundering, as smart contracts can be used to automate transactions and facilitate illegal activities without direct human intervention.
- Decentralization: Ethereum operates on a decentralized network of nodes, making it difficult for any organization to track or control all transactions. Such decentralization can make it more challenging to comply with anti-money laundering (AML) regulations and detect suspicious activity compared to traditional financial systems where centralized authorities have more control.
- Cross-Border Transactions: Cryptocurrencies like Ethereum enable cross-border transactions with minimal hassle, allowing money launderers to quickly move funds between jurisdictions without needing traditional financial intermediaries. This makes it difficult for law enforcement agencies to coordinate and track illegal flows of funds.
- Regulatory Challenges: The regulatory landscape

surrounding cryptocurrencies is still evolving, with varying levels of oversight and enforcement in different jurisdictions. The lack of regulatory clarity can create loopholes that money launderers use to conduct illegal activities on the Ethereum network.

## 2.1. Regulation of cryptocurrency

The legislative framework for cryptocurrency in Ukraine currently needs to be clarified. Although no specific legislation applies explicitly to cryptocurrency, the country pays significant attention to preventing money laundering. The current legal environment does not officially recognize cryptocurrency as a recognized currency or financial instrument. As a result, there needs to be more special regulatory acts regulating transactions with cryptocurrencies. Ukraine follows the guidelines of the Financial Action Task Force (FATF) in combating money laundering (AML). Consequently, financial institutions must implement anti-money laundering protocols for cryptocurrency transactions despite the lack of full regulation in the cryptocurrency space. As Ukraine explores the area of cryptocurrency legislation, its progress is currently on hold as it seeks to synchronize its regulations with future guidelines set out by the European Union[9, 10].

Thus, although there are no specific rules for cryptocurrency, anti-money laundering practices apply to cryptocurrency transactions that pass through Ukrainian financial institutions.

# 3. Mechanism of money laundering in the Ethereum network

Money laundering in the Ethereum network, as in any cryptocurrency network, usually involves converting illegally obtained funds into legitimate assets or making tracing difficult. Although Ethereum does not facilitate money laundering, its decentralized and pseudonymous nature can be used for such purposes. Here's an overview of how money laundering could potentially happen on the Ethereum network[11, 12, 13]:

1. Acquisition of Ethereum (ETH): Criminals obtain Ethereum in various ways, such as hacking, fraud, or illegal transactions.
2. Tumbler/Mixer: To hide the origin of funds, criminals often use tumblers or mixers. These services pool Ethereum from multiple users and then redistribute it, making it difficult to trace the source of the funds.
3. Layering: The criminals then engage in a series of operations to further conceal the origin of the funds. They can use multiple wallets and conduct transactions across numerous addresses, exchanges, and decentralized finance (DeFi) platforms.
4. Integration: Laundered Ethereum is being integrated into the legitimate financial system. This may include conversion to other cryptocurrencies or fiat currencies through exchanges or use to purchase goods and services.

It is important to note that while these mechanisms may facilitate money laundering, they are not exclusive to Ethereum and may also apply to other cryptocurrencies. However, Ethereum's smart contract feature and the evolving DeFi ecosystem create additional complexities and opportunities for money laundering. In addition, regulators and blockchain analytics firms are increasingly developing tools to track and detect suspicious transactions on the Ethereum network.

# 4. Ethereum protocol analysis model

Currently, there are several developments of methods and implementations for detecting suspicious transactions for the Ethereum network[2, 13, 14]. Some of them use visual control, which is useful, for example, in Fig. 2, but more is needed for timely detection of illegal transactions, which requires the development of more sophisticated approaches.

## 4.1. Formalized model

Using a formalized model to analyze transactions on the Ethereum network offers a comprehensive means of detecting potential money laundering activity. This approach allows for a more thorough investigation of transaction patterns, revealing irregularities that may indicate illegal financial behavior.

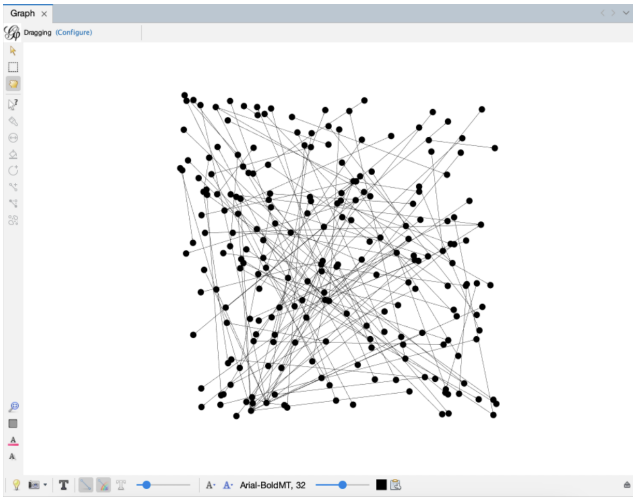


Figure 2. Visualization of the graph of transactions

In the Ethereum model, the graph G=(V, E) represents transactions (Fig. 2), with vertices in V representing wallet addresses and edges in E symbolizing transactions between them. This includes details such as transaction cost, timestamp, and gas cost. Applying machine learning algorithms, such as anomaly detection or clustering techniques, to the subgraphs of S allows for identifying patterns indicative of money laundering activity, with the algorithm estimating the probability (p) of such illegal behavior.

In addition, this approach helps identify suspicious transaction patterns and allows you to adapt to new money laundering tactics. By constantly learning new data and adjusting its detection methods, the system becomes more adept at flagging suspicious behavior, thus

increasing the overall security measures of blockchain networks.

This methodology can be applied in various ways to detect money laundering[10, 8]:

1. Pattern Recognition: The model can identify patterns such as frequent transactions between seemingly unrelated entities, huge transactions, or transactions involving high-risk jurisdictions.
2. Analysis of behavior. By analyzing transaction history and comparing it to typical user behavior, the system can flag anomalies that may indicate suspicious activity, such as sudden transaction volume or frequency changes.
3. Cluster Analysis: Identifying clusters of wallets involved in circular transactions or complex networks of interconnected transactions, common strategies in money laundering schemes.
4. Anomaly Detection: Using anomaly detection techniques to flag transactions that significantly deviate from normal behavior, such as transactions occurring at unusual times or involving unusually high transaction fees.
5. Integration with Anti-Money Laundering (AML) systems: Integrate with existing AML systems to enhance their capabilities by providing blockchain-specific information and data.

By combining these approaches, the model can effectively detect potential money laundering activities on the Ethereum network and contribute to efforts to combat financial crimes in the digital realm.

## 4.2. Analysis model

As blockchain platforms increasingly become the basis for digital transactions worldwide, they also attract sophisticated financial crimes such as money laundering. To solve this problem, an analytical model was developed to thoroughly analyze blockchain transactions and effectively identify signs of money laundering.

The model uses data mining techniques to monitor, analyze, and flag suspicious activity in decentralized networks. By integrating components such as pattern recognition, behavioral analysis, cluster analysis, anomaly detection, and integration with anti-money laundering (AML) systems, the model provides a comprehensive set of tools to detect and respond to illicit financial flows without compromising its strengths. blockchain technology[8].

This flowchart design (Figure 3) describes a model for detecting potential money laundering activity in blockchain transactions. It is worth looking at each component to understand how they interact and contribute to the system's overall functionality[1, 11].

1. Pattern recognition.
   **Purpose:** Identifies typical and suspicious blockchain transaction patterns that may indicate money laundering.
   **Input:** transaction data such as amounts, timestamps, and wallet addresses.
   **Results:** revealed patterns that cause concern, for example:

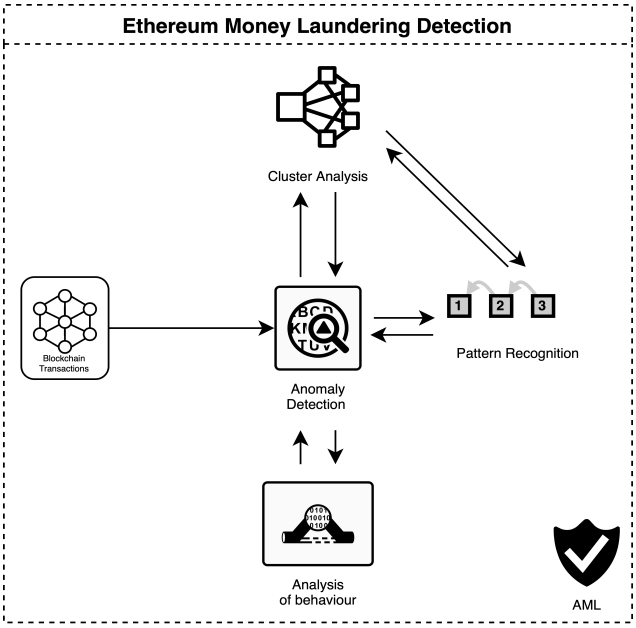


Figure 3. Block diagram of the algorithm for detecting suspicious transactions

   - Frequent transactions between seemingly unrelated individuals.
   - Transactions that are unusually large compared to typical models.
   - Operations involving jurisdictions known for high risks of financial crimes.

   **Meaning:** revealed regularities are crucial for further analysis. They are related to behavioral and cluster analysis and refine the detection of potentially illegal activity.
2. Analysis of behavior.
   **Purpose:** Analyzes object behavior based on historical data and identified patterns to identify deviations from typical activity.
   **Input:** transaction history, user profiles, and patterns identified using pattern recognition.
   **Results:** marks that signal deviations from typical behavior, for example:
   - Sudden changes in transaction volume or share.
   - Unexpected introduction of new wallet addresses in transaction chains.

   **Meaning:** Flags from this step are fed into the anomaly detection system to assess risk and the potential need for alerts.
3. Cluster analysis.
   **Purpose:** identifies clusters of wallets that can coordinate activity indicative of structured laundering schemes.
   **Input:** wallet and transaction network addresses obtained from transaction data.
   **Results:** identified clusters involved in:
   - Circular transactions designed to obfuscate the money trail.
   - Complex interconnected networks that create a web of transactions to hide the true source

and destination of funds.
**Meaning:** This data provides a map of related activities and potential collusions fed into the anomaly detection function to highlight activities that deviate significantly from the norm.

4. Anomaly detection.
**Objective:** focuses on detecting highly irregular transactions potentially indicative of money laundering.
**Input:** comprehensive transaction data and insights from behavioral analysis and cluster analysis.
**Results:** alerts generated for transactions that exhibit abnormal patterns such as:
   - Transactions occurring at non-standard times may be aimed at avoiding attention.
   - Unusually high transaction fees that can be used to accelerate the movement of illicit funds.

   **Meaning:** alerts and findings are forwarded to integrate anti-money laundering systems to leverage existing frameworks for robust response.
5. Integration with anti-money laundering (AML) systems.
**Objective:** improves the existing anti-money laundering system by integrating new findings and improving the system's response to identified threats.
**Inputs:** all flags and alerts from previous steps and comprehensive analysis of transaction patterns and behavior.
**Results:** enhanced discovery capabilities that allow:
   - Detailed analysis of identified risks.
   - Notify the relevant authorities for possible actions.
   - Regulatory compliance updates based on the latest data.

   **Meaning:** the integration results are used to continuously refine and improve all previous steps, creating a feedback loop that increases system performance over time.

The model creates a powerful mechanism for detecting and responding to potential money laundering activity on the blockchain by systematically processing and analyzing transaction data through these interconnected components. Each step builds on the previous ones, providing a detailed understanding of individual transactions and broader trading patterns, thereby improving the effectiveness of existing anti-money laundering strategies.

## 4.3. Illegal activity detection metrics

Detecting illegal activities, such as money laundering on the Ethereum network, involves analyzing patterns of transactions and behavior that deviate from the norm. Several critical indicators that can be used have been identified for practical analysis[13, 8]:

Table 1. Money laundering detection metrics

| Metrics | Description |
|---|---|
| Frequency and volume of transactions | High-frequency transactions or huge transactions inconsistent with typical wallet activity. Monitoring them can help spot sudden spikes in |
| Interacting wallets | Monitoring the number of interacting wallets, especially if transactions are repeated between multiple wallets or create loops back to the original wallet |
| Anomalous transaction patterns | Detection of patterns such as laundering chains (breakdown of large sums into smaller amounts at many addresses) or sudden consolidation suggesting possible stages of laundering |
| Transaction Fees | Abnormally high fees or gas prices may signal urgency or a willingness to pay more to speed up transactions, which may be associated with illegal activity |
| Temporal Patterns | Examining Transaction Timing to detect suspicious patterns, such as transactions occurring at unusual times, which may be an attempt to avoid detection |
| Compliance Review | Ensuring Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance by all parties involved in significant transactions |

In summary, metrics to detect illegal activities, such as money laundering on the Ethereum network, are essential to maintain blockchain transactions' integrity and security. These metrics include analysis of transaction frequency, volumes, interacting wallets, and the use of smart contracts to detect anomalous behavior that deviates from typical patterns.

Using advanced techniques such as graph theory, machine learning, and artificial intelligence, these metrics enable a more granular and practical approach to monitoring and detecting suspicious activity.

## 4.4. Ethereum Blockchain Transaction Analysis

To effectively identify potential money laundering activity (Fig. 4) in the Ethereum blockchain, it is worth using a reliable methodology. We will analyze the results of the executed code and describe how each phase of the methodology contributes to the detection of suspicious actions.

The implemented code provides a complete overview of the transaction dynamics of the Ethereum network and highlights potential artifacts that may indicate money laundering. During the program's execution, a connection to Ethereum was established; the current block number is 19862271 with 183 transactions - this primary data is crucial to initiate real-time monitoring of transactions within a particular block, which serves as the basis for further analysis.

The first stage of the analysis will be identifying addresses with significantly large balances, indicating potential control points or centers of financial flow in the network. This is also consistent with pattern recognition, as detecting large balances may signal the need

```
❯ python3 main.py
[+] Connected to Ethereum
[+] Current block number: 19862271
[+] Transactions in block: 183
[+] Getting address balance started
[+] Getting address ended in 56 seconds
[+] Addresses with a large balance:
        [>] Address: 0xf89d7b9c864f589bbF53a82105107622B35EaA40 Balance: 21291.60
        [>] Address: 0xA7EFAe728D2936e78BDA97dc267687568dD593f3 Balance: 77431.27
        [>] Address: 0xC02aaA39b223FE8D0A0e5C4F27eAD9083C756Cc2 Balance: 3056306.93
        [>] Address: 0x6774Bcbd5ceCeF1336b5300fb5186a12DDD8b367 Balance: 51683.00
[+] Finding suspicious transactions started
[+] Finding suspicious transactions ended in 0.00022292137145996094 seconds
[+] Finding bots activity started
        [x] Bot: 0xf9cAFEb32467994e3AFfd61E30865E5Ab32ABE68
[+] Finding bots activity ended in 0.00021505355834960938 seconds
[+] Finding large transactions started
        [x] Large transaction found:
                From: 0x0C67746F88e2EF258Ee83A72DBdA59C766502eFb
                To: 0xC36442b4a4522E871399CD717aBDD847Ab11FE88
                Value: 279 ether
[+] Finding large transactions ended in 0.0006039142608642578 seconds
[+] Finding high frequency transactions started
from
0x46340b20830761efd32832A74d7169B29FEB9758    15
0xae2Fc483527B8EF99EB5D9B44875F005ba1FaE13    15
0xDFd5293D8e347dFe59E90eFd55b2956a1343963d    15
0xf89d7b9c864f589bbF53a82105107622B35EaA40    15
0x75e89d5979E4f6Fba9F97c104c2F0AFB3F1dcB88    15
Name: count, dtype: int64
to
0xdAC17F958D2ee523a2206206994597C13D831ec7    182
0x3fC91A3afd70395Cd496C647d5a6CC9D4B2b7FAD    135
0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48     46
0x8143182a775C54578c8B7b3Ef77982498866945D     35
0x6982508145454Ce325dDbE47a25d4ec3d2311933     31
Name: count, dtype: int64
[+] Finding high frequency transactions ended in 262.28284335136414 seconds
```

Figure 4. Work of Algorithm

for further scrutiny. These accounts may be central to money laundering stages, where large sums of money are moved to conceal their origin.

One important step directly related to the detection of transactions that may fall outside the standard transaction norms is the detection of anomalies based on defined criteria, such as connections to blocked addresses.

In turn, the detection of addresses controlled by a bot can indicate automated repetitive transactions, which are often used in money laundering schemes. Bots can create an artificial increase in transaction volume or frequency, which differs from transaction patterns and refers to the analysis of non-human-driven behavior.

The pattern recognition value carries the detection of a transaction worth 37 ethers, which is considered significant compared to typical transactions. Cash transactions that differ significantly from the norm may indicate possible layering or integration stages of money laundering, where considerable amounts are moved to combine illicit funds with legitimate assets.

Several addresses with high transaction rates were detected, indicating potential smurfing activity where small transactions are used to avoid detection. Such high-frequency patterns of transactions from specific addresses help identify clusters of accounts operating in concert, potentially indicating structured money laundering operations.

Each output of the software code provides important information that is included in the complex analytical system[14, 15]:

- Pattern recognition. Studying the size and frequency of transactions based on data makes it possible to detect anomalies that indicate unconventional behavior of transactions.
- Analysis of behavior. Analyzing transaction patterns for regularity and comparing them to historical data helps pinpoint anomalies created, for example, by robots or frequent small transactions.
- Cluster analysis. Identifying addresses with high balances and frequent transactions allows for the clustering of related accounts that may cooperate for money laundering.
- Detection of anomalies. Quick checks on transactions that meet specific suspicious criteria allow you to flag high-risk activities for further investigation immediately.

Combining raw software code data with advanced analytical techniques improves the detection of potential money laundering activities in Ethereum transactions. This integrated approach highlights individual suspicious activities and provides a holistic view of potentially interconnected transactions, significantly aiding the fight against financial crimes in the blockchain space.

Below is a pseudocode (Listing 1) representation that illustrates how these analytical processes were implemented programmatically to monitor transactions on the Ethereum blockchain:

```
function processEthereumData(web3,
    startBlock, endBlock):
Initialize knownMaliciousAddresses,
    largeTransactionThreshold
Initialize data structures for
    suspiciousTransactions, botActivities,
     largeTransactions
Open a transaction log file with a
    timestamped filename

for each blockNumber from startBlock to
    endBlock:
    block = getBlock(web3, blockNumber)
    for each transaction in block.
        transactions:
        Record basic transaction details
            in the log file

        if transaction.from or transaction
            .to is in
            knownMaliciousAddresses:
            Log and store the suspicious
                transaction

        if (transaction.from, transaction.
            to) is a repeated pair in
            botActivities:
            Increment the count indicating
                 potential bot activity
        else:
            Initialize the pair in
                botActivities

        if transaction.value in Ether
            exceeds
            largeTransactionThreshold:
            Log and store the large
                transaction

Close the transaction log file
Log summary statistics of the process (
    total transactions processed,
    suspicious, bots detected, large
    transactions)

Return structured data containing details
    on suspicious, bot, and large
```

```
transactions
```

Listing 1. Pseudocode of forensics algorithm

## 5. Conclusions

This study considered methods of analyzing the Ethereum network's blockchain to detect illegal activities, particularly money laundering. The main result of the work is the development of an algorithm that allows you to thoroughly check Atheneum's transactional structure using forensics and graph analysis methods. It has been determined that smart contracts and decentralized applications, which are the basis of Ethereum's functioning, can also be used to carry out illegal activities.

An Ethereum protocol analysis model has been developed to detect anomalous transactions and schemes that indicate money laundering. This model's application increases network security, providing more effective detection and prevention of illegal financial transactions.

Thus, the integration of anomaly detection, cluster analysis, behavioral analysis, and pattern recognition methods into a comprehensive transaction analysis model of the Ethereum blockchain effectively combats money laundering and other financial crimes, contributing to the improvement of the blockchain ecosystem's transparency and security.

## References


1. *Абдуллаєва Е.*, *Гальчинський Л.* Алгоритм аналізу блокчейн мережі Ethereum для виявлення незаконної діяльност // Теоретичні і прикладні проблеми фізики, математики та інформатики. — 2023. — 12 трав. — С. 225—227.
2. *Топчій М.*, *Гальчинський Л.* Підвищення рівня безпеки смарт-контрактів у мережі Ethereum від шахрайства за рахунок використання реверсивних токенів // Collection of Scientific Papers «Л'ОГОЕ», — 2022-11-11. — С. 14—21.
3. Blockchain: A new perspective in cyber technology / T. Venkat Narayana Rao, P. P. Likhar, M. Kurni, S. K. — 2022. — P. 33–66.
4. What is blockchain technology? — URL: https://www.ibm.com/topics/blockchain.
5. Full Guide to Contrastive Learning. — URL: https://subscription.packtpub.com/book/data/9781787125445/7/ch07lvl1sec49/ethereum-blockchain.
6. *T. K.* Digital forensics of cryptocurrency wallet. — 2022-05-20. — P. 14–21.
7. *Goyal H.*, *B. S.* Blockchain Forensics in Policing and It's Global Scenario // Lupine Publishers. — 2022-05-25.
8. *Lorenz J. S.* Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity // Information Management School. — 2021-03.
9. Anti-money Laundering (AML) in Cryptocurrency. — URL: https://encord.com/blog/guide-to-contrastive-learning.
10. *Boneh D.*, *Drijvers M.*, *Neven G.* Models and Simulation of Blockchain Systems // Cryptology ePrint Archive - IACR. — 2020-11.
11. *Fu Q.*, *Wu J.* Does Money Laundering on Ethereum Have Traditional Traits? // Cryptology ePrint Archive - IACR. — 2023-05.
12. *Alharby M.* Models and Simulation of Blockchain Systems // School of Computing Newcastle University. — 2020-11.
13. Bitcoin Money Laundering Detection via Subgraph Contrastive Learning / S. Ouyang, Q. Bai, H. Feng, B. Hu // mdpi. — 2021-04.
14. *Salisu S.*, *Filipov V.*, *Penne B.* Blockchain Forensics: A Modern Approach to Investigating Cyber-Crime in the Age of Decentralisation. — 2022-06-30.
15. *Acharya A.* Full Guide to Contrastive Learning. — 2023-07-14.