Int. J. Adv. Eng. Pure Sci. 2023, 35(3): 285-296
DOI: 10.7240/jeps.1224416

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

Investigation of Cryptocurrency-Centered Money Laundering Scenarios in Terms of Digital Forensics

Düzgün KÜÇÜK [1], **Ömer Faruk YAKUT** [1], **Emre ÇAKAR** [1], **Fatih ERTAM** [1]

[1]Fırat Üniversitesi, Teknoloji Fakültesi, Adli Bilişim Mühendisliği Bölümü, Elazığ, Türkiye

Abstract
This study contributes to the literature on tracking money laundering activities. It is important that the proposed methods are applied only to individuals under suspicion of crime and within the framework of existing legal regulations, without violating individual rights and freedoms. The use of relevant methods should adhere to ethical and legal limitations, taking into account important aspects such as privacy and personal data protection.

The main innovation of this study is the presentation of blockchain-based analysis methods for monitoring cryptocurrencies and detecting criminals' money laundering techniques. This study examines how criminals use tools such as cryptocurrency mixers to hide their traces and create illicit money flows. Based on the study findings, monitoring methods are proposed for mixers with low transaction counts and simple operation logic. However, tracking becomes more challenging in complex mixers with a higher volume of transactions, where it is more likely for criminals to blend in with other users.

This study provides a significant contribution by focusing on the opportunities provided by blockchain technology in detecting money laundering activities. It also serves as a valuable resource for identifying steps in digital evidence analysis and tracking processes.

In this study, an approach that will detect money laundering is presented through sample scenarios by bringing a broad perspective to crypto money-based money laundering methods, which are very difficult to trace due to their nature. In addition, it is expected that the difficulties in the implementation of the proposed approach will be clearly addressed and will shed light and inspire further study.
Keywords: Bitcoin, clustering heuristics, cryptocurrency, blockchain, digital forensics, digital evidence, coin mixers, money laundering, cryptocurrency tracking

Öz
Bu çalışma, kara para trafiğinin takibi konusunda literatüre katkıda bulunmayı amaçlamaktadır. Önerilen yöntemlerin yalnızca suç şüphesi altındaki kişilere uygulanması ve mevcut yasal düzenlemeler çerçevesinde bireysel hak ve özgürlükleri ihlal etmemesi önemlidir. Etik ve yasal sınırlamalara uygun olarak ilgili yöntemlerin kullanımı, mahremiyet ve kişisel veri koruması gibi önemli yönleri dikkate almalıdır.

Bu çalışmanın ana yeniliği, kripto para birimlerinin izlenmesi ve suçluların para aklama yöntemlerinin tespiti için blockchain tabanlı analiz yöntemlerinin sunulmasıdır. Makalede, suçluların kripto para karıştırıcıları gibi araçları kullanarak izleri kaybettirmesi ve kara para trafiği oluşturması incelenmiştir. Çalışma sonuçlarına göre, düşük işlem sayısına sahip ve basit işlem mantığına sahip karıştırıcılar için izleme yöntemleri önerilmiştir. Ancak daha karmaşık ve daha fazla işlem yapılan karıştırıcılar için izlemenin zor olduğu ve suçluların diğer kullanıcılar arasında izlerinin kaybolmasının daha olası olduğu belirlenmiştir.

Bu çalışma, suçluların para aklama faaliyetlerini tespit etmede blockchain teknolojisinin sağladığı olanaklara odaklanarak önemli bir katkı sağlamaktadır. Ayrıca, sayısal delil analizi ve takip süreçleri için adımların belirlenmesi açısından da değerli bir kaynak oluşturmaktadır.

Bu çalışmada; yapısı gereği iz sürmenin çok zor olduğu kripto para merkezli kara para aklama yöntemlerine geniş bir bakış açısı getirilerek, örnek senaryolar üzerinden kara para aklamayı tespit edecek bir yaklaşım sunulmaya çalışılmıştır. Ayrıca önerilen yaklaşımın uygulamadaki zorlukları açık bir şekilde ele alınarak daha sonra yapılacak çalışmalara ışık tutması ve ilham vermesi beklenmektedir.
Anahtar Kelimeler: Bitcoin, kümeleme buluşsal yöntemleri, kripto para, blok zincir, adli bilişim, dijital kanıt, coin karıştırıcıları, kara para aklama, kripto para takibi

Corresponding Author: Fatih ERTAM**, Tel:** 0424 237 00 00 -7640**, e-posta:** fatih.ertam@firat.edu.tr

Submitted: 26.12.2022, **Revised:** 24.05.2023, **Accepted:** 27.06.2023

I. INTRODUCTION

The phenomenon of cryptocurrency, considered one of the greatest technological advancements in the digital world, has rapidly gained popularity and attracted significant public attention [1]. Cryptocurrency is a digital asset that employs cryptography to secure transactions and maintain control within its own system. Consequently, transactions are conducted autonomously without the involvement of any central authority, safeguarding the privacy of individuals' personal information [1].

Transactions within cryptocurrency are recorded on the blockchain, ensuring data integrity; however, the sender and receiver details remain undisclosed if the 'private key' is unknown to researchers [2]. Bitcoin, the first cryptocurrency, was introduced by an enigmatic individual or group known as Satoshi Nakamoto on January 9, 2009 [3]. Nakamoto announced the publication of the initial version of Bitcoin, an electronic cash system usinga peer-to-peer network to prevent double spending, operating independently of servers or central authorities [3].

After this announcement, numerous valid and invalid cryptocurrencies flooded the market due to high demand, substantial price fluctuations, and intense public interest [4]. While this situation has victimized thousands of people, it has also been exploited by illegal organizations for activities like money laundering [5]. Criminals and terrorists have swiftly leveraged Bitcoin's unique characteristics, such as its peer-to-peer structure and pseudo-anonymity, to facilitate extensive financing and money laundering schemes [5].

Governments, on one hand, defend Bitcoin as a currency to protect their national interests and exhibit tolerance toward it. On the other hand, opposing parties have led to a bureaucratic war, hindering the establishment of comprehensive regulations and classifications for cryptocurrency, thereby preventing the surpassing of existing legal boundaries [6]. Money serves as a vital element supporting illegal terrorist and criminal organizations, allowing them to survive and sustain their activities [7]. These groups acquire financing through various means, including government sponsorships, illegal trade, extortion, theft, support donations, and personal wealth [8]. The centralization of currencies and the development of control mechanisms have driven these entities to shift their focus to cryptocurrencies.

The decentralized nature of cryptocurrencies has proven advantageous in many regions, bypassing existing banking systems, especially in areas plagued by corruption. However, this unregulated and decentralized structure has raised significant concerns for governments and intelligence agencies. The supposed anonymity of cryptocurrency users implies that personal information may never be disclosed; however, in certain special cases, the structure can be traced to multiple computers or identified through a specific public key associated with the user. Additionally, the instantaneous and irreversible nature of international cryptocurrency transactions, detached from existing banking systems, further reinforces the uncontrolled aspect of this structure [6].

II. RELATED WORKS

Studies on detecting money laundering methods using cryptocurrencies are novel and up date. Despite these negative aspects, efforts have been made to understand the structures of cryptocurrency derived from criminal proceeds and to transform the various stages of digital forensics analysis of devices used in cryptocurrency transactions into more concrete processes [2]. These efforts involve clustering heuristics, attribution tags, and analyzing cryptocurrency payment flows to investigate criminal activities, highlighting key components of modern cryptocurrency analytical techniques [9]. However, the proposed clustering method and the diversity of input-output transactions in coin mixers have not been addressed. Another study discussed different approaches to detecting cryptocurrency mining in corporate networks, presenting two detection methods and practices to prevent the unauthorized use of company resources [10]. Advancements in learning algorithms, such as logistic regression (LR), random forest (RF),multi-layer perceptron (MLP), and graph convolutional networks (GCN), hold promise for anti-money laundering efforts and predicting illicit transactions [11]. Although the association of cryptocurrencies with various crimes such as narcotics, firearms, money laundering, terrorism, child abuse, and ransom attacks may seem negative, the development of specialized analytical tools can facilitate the detection of large criminal networks [12].

The aim of this study is to provide preliminary information on detecting wallets involved in money transfers through public crypto transactions, considering the available money laundering methods for law enforcement in this dark realm. The article is organized as follows: the first part explains definitions and expressions related to cryptocurrencies, the second part reviews relevant literature, the third part provides detailed explanations of existing money transfer methods, the fourth section presents scenarios for monitoring coin mixers and proposes a detection method, the fifth chapter includes a sample application for law enforcement and digital forensics experts, demonstrating tools and scanners for analyzing wallet movements. The final section evaluates and discusses the results.

The unique contributions of this study are as follows:

- Introducing an approach to detect money laundering and suspicious wallet movements in cryptocurrency transfers, which operate outside the control of central authorities and are untraceable.
- Discussing methods related to laundering proceeds of crime using cryptocurrencies and providing insights for future studies in identifying these methods.
- Offering detailed information on various money laundering methods used in the world of cryptocurrencies.
- Providing recommendations for analyzing and tracking these money laundering methods.
- Examining scenarios for tracking suspects through the input and output values of coin mixers, a widely used method for money laundering, and presenting detection approaches.
- Including tools and methods that digital forensic experts can use for tracing activities in the world of cryptocurrencies.

III. MATERIALS AND METHOD

3.1. Cryptocurrency

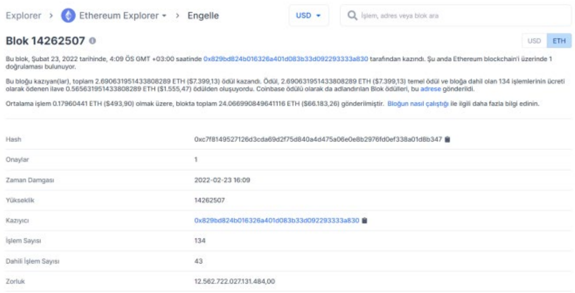
Cryptocurrency is an electronic payment system that operates on the basis of cryptographic evidence, allowing direct transactions between any two willing parties. Its peer-to-peer (P2P) nature eliminates the need for central banks or verifiers to facilitate and authenticate transactions. It operates on a fully decentralized and distributed open-source software platform, enabling users to connect and participate in the network at any time [9]. The Bitcoin system comprises essential components for executing these transactions, including cryptocurrencies, wallets, public-private keys, and the blockchain [10]. Users use digital wallets to store their cryptocurrencies, which provide them with an account number. However, it is uncommon for users to input real credentials when acquiring a wallet [9]. Each wallet, and therefore each user, is associated with a public and private key. The public key is shared across the network and is used to generate cryptocurrency addresses, sign transactions, and verify payments [9]. In essence, the public key represents the address to which the cryptocurrency is sent and is also used to verify the signatures of transactions signed with the private key. While it is possible to derive a public key from a private key, the reverse is not possible. Therefore, it is crucial for users to securely store their private keys. Moreover, since the user in possession of the keys associated with the cryptocurrency is the only person capable of transferring it, the loss of keys renders the cryptocurrency inaccessible [11]. On the other hand, the blockchain is a publicly accessible ledger that records every transaction. Each record contains the public keys of both the sender and the receiver, along with the transaction amount and timestamp. Users can acquire cryptocurrencies through online purchases, cryptocurrency vending machines, or mining. Mining refers to the process in which miners solve complex mathematical problems to validate transactions and add them to the blockchain [12].

3.2. What is Money Laundering?

Money laundering refers to the process in which criminals disguise illicit funds as legitimate money, investments, or financial assets [13]. This operation is designed to make the proceeds from illegal activities, such as drug trafficking, appear to originate from lawful sources. Once the illegal funds have been laundered, the perpetrator can freely spend or invest the illicit income in legitimate assets. Money laundering poses a significant threat to the global economy, undermines the integrity of financial systems, and funds further criminal activities that impact community safety and well-being [14].

3.3. Blockchain Explorer

When transactions occur on public networks such as Bitcoin and Ethereum, the data is transformed into a unique value through cryptographic transactions. These unique values are stored in blocks, and all users can access them. Not only the transaction hashes but also the hash values of all wallets and transactions associated with those wallets are publicly available. This feature has both positive and negative aspects. On one hand, it allows for easy tracking of "how much cryptocurrency is held in which wallet" and "when transfers were made in a particular wallet." However, the owners of these wallets remain anonymous and their identities are unknown. In other words, there are numerous wallets and transactions, but the individuals behind these wallets are unidentified. The websites or programs that visualize all cryptocurrency blocks and present them to the public are known as "Blockchain Explorers."



Blok 14262507

Bu blok, Şubat 23, 2022 tarihinde, 4:09 ÖS GMT +03:00 saatinde 0x829bd824b016326a401d083b33d092293333a830 tarafından kazındı. Şu anda Ethereum blockchain'i üzerinde 1 doğrulaması bulunuyor.

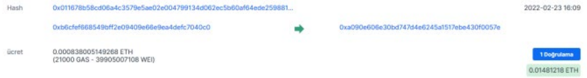
Bu bloğu kazıyan(lar), toplam 2.690631951433808289 ETH ($7.399,13) ödül kazandı. Ödül, 2.690631951433808289 ETH ($7.399,13) temel ödül ve bloğa dahil olan 134 işlemlerinin ücreti olarak ödenen ilave 0.565631951433808289 ETH ($1.555,47) ödülden oluşuyordu. Coinbase ödülü olarak da adlandırılan Blok ödülleri, bu adrese gönderildi.

Ortalama işlem 0.17960441 ETH ($493,90) olmak üzere, blokta toplam 24.066990849641116 ETH ($66.183,26) gönderilmiştir. Bloğun nasıl çalıştığı ile ilgili daha fazla bilgi edinin.

Hash	0xc7f8149527126d3cda69d2f75d840a4d475a06e0e8b2976fd0ef338a01d8b347
Onaylar	1
Zaman Damgası	2022-02-23 16:09
Yükseklik	14262507
Kazıyıcı	0x829bd824b016326a401d083b33d092293333a830
İşlem Sayısı	134
Dahili İşlem Sayısı	43
Zorluk	12.562.722.027.131.484,00

Figure 1. Blockchain Explorer

As shown in Figure 1, the content of an Ethereum block retrieved from Blockchain.com, one of the most well-known blockchain explorers, is shown. Here, it is easy to access a lot of information about the block, from which the miner approves the block [15].



Hash	0x011678b58cd06a4c3579e5ae02e004799134d062ec5b60af64ede259881...		2022-02-23 16:09
	0xb6cfef668549bff2e09409e66e9ea4defc7040c0	0xa090e606e30bd747d4e6245a1517ebe430f0057e	
ücret	0.000838005149268 ETH (21000 GAS - 39905007108 WEI)		1 Doğrulama 0.01481218 ETH

Figure 2. Web page view showing registration information for cryptomoney transfers

As shown in Figure 2, the interface of these browsers provides access to information such as the amount of money transferred between wallets and the corresponding charges. Each transaction also has a cryptographic summary. Based on the available information, it can be concluded that the data on the blockchain is transparent in terms of transaction details but anonymous in terms of the identities involved.

3.4. Anti-Money Laundering Act (AML)

The Anti-Money Laundering Act (AML) encompasses regulations and laws aimed at preventing the transfer and laundering of illegal funds. AML software typically detects suspicious behaviors, including large fund transfers, consistent inflow of funds into an account, and cross-checks against watch lists. AML measures are not limited to cryptocurrencies but apply to all assets and currencies, subject to AML regulations [16].

3.5. Anti-Money Trace and Money Laundering Methods

Just as the use of anonymity technologies makes it challenging to identify individuals, the use of cryptocurrencies can make it difficult to hold specific individuals accountable for money laundering activities. However, by tracing a particular cryptocurrency account to the corresponding exchange, it may be possible to establish a connection between the laundered money and other accounts of the individual [17]. For instance, if the funds in a wallet account are obtained illegally, and the wallet address is known, the transactions performed by that wallet can be tracked, revealing the wallets to which the funds are transferred. However, criminals are aware of this situation and have developed various methods to launder their money.

3.5.1. Buying NFT (Non-Fungible-Token) at exorbitant prices

This method is prevalent in the real world and has been practiced for a considerable time. For example, purchasing worthless paintings for thousands of dollars or buying products of little value at excessively high prices on online platforms can be cited as examples. NFTs, known for their unique product/artwork value, are often used for money laundering purposes. Criminals employ two main methods to evade detection in tracked wallets. In the first method, they create a new wallet and purchase their own NFTs at inflated prices. In the second method, they negotiate with an NFT seller and buy the seller's NFT at a higher price, obtaining a significant portion of the paid amount back from the seller.

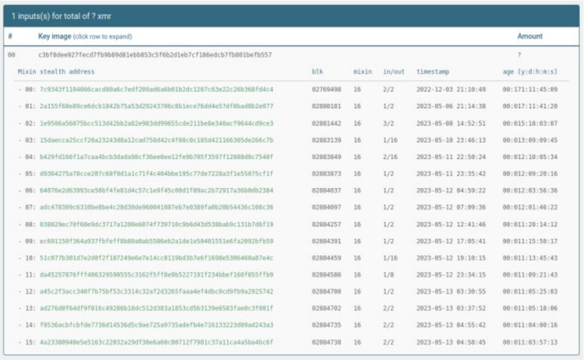
3.5.2. Selling on exchanges in the dark web

Criminals frequently employ this method to convert their traceable cryptocurrencies (such as Bitcoin and Ethereum) into Monero, as tracking transactions in Monero is nearly impossible. Additionally, since these exchanges do not require authentication, criminals can easily sell their cryptocurrencies. AlphaBay Market serves as an example of such exchanges.

3.5.3. Converting black coins to cryptocurrencies like Monero

Monero is a cryptocurrency that uses a variety of privacy-enhancing technologies to hide transactions and make them anonymous. One of the key technologies that Monero uses is ring signatures.

The ring signature is a signature technique used by Monero to ensure transaction privacy. In this method, a user initiating a transaction creates a "ring" that includes signatures from randomly selected other users. This ring is used to hide the real identity of the user initiating the transaction and make it untraceable. Monero utilizes Bulletproofs+ with a ring signature size of 16. This means that each transaction contains 16 signatures. As a result, it becomes even more challenging to infer the identity of the user initiating the transaction and to track the transactions [30].



1 inputs(s) for total of ? xmr

#	Key image (click row to expand)	Amount
00	c3bf8dee927fecd7fb9b89d81ebb853c5f6b2d1eb7cf186edcb7fb801befb557	?

Mixin stealth address	blk	mixin	in/out	timestamp	age [y:d:h:m:s]
- 00: 7c9343f1104866cacd80a6c7edf209ad6a6b01b2dc1207c63e22c26b368fd4c4	02769498	16	2/2	2022-12-03 21:10:49	00:171:11:45:09
- 01: 2a155f68e89ce6dcb1842b75a53d29243706c8b1ece76dd4e57df8bad8b2e077	02880181	16	1/2	2023-05-06 21:14:38	00:017:11:41:20
- 02: 1e9506a56075bcc513d42bb2a82e983dd99655cde211be8e340acf9644cd9ce3	02881442	16	3/2	2023-05-08 14:52:51	00:015:18:03:07
- 03: 15daecca25ccf20a23243d8a12cad758d42c4f08c0c185d421166305de266c7b	02883139	16	1/16	2023-05-10 23:46:13	00:013:09:09:45
- 04: b429fd166f1a7caa4bcb3dada98cf36ee0ee12fe9b705f3597f12888d0c7540f	02883849	16	2/16	2023-05-11 22:50:24	00:012:10:05:34
- 05: d9364275a78cce207c68f9d1a1c71f4c404bbe195c77de7228a3f1e55075cf1f	02883873	16	1/2	2023-05-11 23:35:42	00:012:09:20:16
- 06: 64076e2d63993ce58bf4fe81d4c57c1e9f45c08d1f89ac2b72917a36b0db2384	02884037	16	1/2	2023-05-12 04:59:22	00:012:03:56:36
- 07: adc478309c6310be8be4c28d30de960041087eb7e0389fa0b20b54436c108c36	02884097	16	1/2	2023-05-12 07:09:36	00:012:01:46:22
- 08: 038029ec70f60e9dc3717a1200e6074f739710c9b6d43d538bab9c131b7d6f19	02884257	16	1/2	2023-05-12 12:41:46	00:011:20:14:12
- 09: ec691150f364a937fbfeff8b80a0ab5586eb2a1de1e50401551e6fa2092bfb59	02884391	16	1/2	2023-05-12 17:05:41	00:011:15:50:17
- 10: 51c077b301d7e2d0f2f187249e6e7e14cc8119bd3b7e6f1698e5306460a87e4c	02884459	16	1/16	2023-05-12 19:10:15	00:011:13:45:43
- 11: da45257876fff406329590555c3162f5ff8e9b5227191f234bbef160f055ffb9	02884586	16	1/8	2023-05-12 23:34:15	00:011:09:21:43
- 12: a45c2f3acc340f7b75bf53c3314c32af2d3265faaa4ef4dbc0cd9fb9a2925742	02884700	16	1/2	2023-05-13 03:30:55	00:011:05:25:03
- 13: ad276d0f64df9f016c49286b18dc512d383a1853cd5b3139e6583fae0c3f001f	02884702	16	2/2	2023-05-13 03:37:52	00:011:05:18:06
- 14: f9536acbfcbfde7736d14536d5c9ae725a9735adefb4e716133223d09ad243a3	02884735	16	2/2	2023-05-13 04:55:42	00:011:04:00:16
- 15: 4a23380940e5e5163c22032a29df30e6a60c80712f7981c37a11ca4a5ba4bc6f	02884738	16	2/2	2023-05-13 04:58:45	00:011:03:57:13

Figure 3. Contents of Monero transaction [31]

In Figure 3, addresses that signed the input part of the Monero transaction with the address "b1e814aed40bf79a2b652753edca346d15bae90ee4d3 63c25b9c0d915a82430f" can be seen. There are 16 addresses, and these signatures are specifically generated for the address receiving XMR (Monero's cryptocurrency). The signature addresses for the sender address are different from those shown in Figure 3.

3.5.4. Real-world face-to-face shops by withdrawing cryptocurrencies to cold wallet

In this method, criminals transfer funds from their hot wallets to portable digital wallets known as cold wallets. After withdrawing the funds to a cold wallet, they sell them at a price lower than the market rate. Unsuspecting buyers, enticed by the opportunity to purchase cryptocurrencies below market price, conduct the exchange in person for cash. It is understood from the web pages that such buyers started their activities by opening liaison offices [32, 33]. On the other hand, it is possible to make cash payments by using crypto money ATMs, which are active in many places [34]. However, if the buyer of the cold wallet is unaware of its origin and subsequently transfers the funds to an authenticated exchange for selling, the recorded transactions on the network can easily reveal the trail leading to the cold wallet.

3.5.5. Using online gambling sites

In this method, criminals deposit the cryptocurrencies they want to launder into their accounts on online gambling sites that accept cryptocurrency payments. They then engage in betting activities to avoid raising the suspicion. Finally, they withdraw the funds from their accounts, effectively converting the illicit funds into clean money. Typically, multiple gambling accounts are used to minimize attention. If online gambling companies detect large sums of cryptocurrencies in user accounts, they are likely to become suspicious of the account holder [17].

3.5.6. Purchasing real-world barter services with coins or tokens

Tokens are used in the real world to acquire services or products. For instance, a movie theater chain operating in various provinces of Turkey may issue a token exclusively redeemable for purchasing tickets at its theaters. Criminals can convert their cryptocurrencies into tokens and use them to purchase services (e.g., UBER rides, movie theater tickets) and products. If the clearing service provider maintains records, there is a high likelihood of detecting and apprehending criminals. Additionally, criminals may collaborate with a barter service provider and purchase a product worth 0.01 BTC for 1 BTC, thereby laundering their money. In certain cases, they might engage in larger-scale money laundering by acquiring a service that is unlikely to occur for 10 BTC. Moreover, during these transactions, they can easily conduct illicit activities by establishing a company or charity organization on paper to present a legitimate front.

3.5.7. Using cryptocurrency mixers

Cryptocurrency mixing involves aggregating cryptocurrencies from different users and transferring the funds to the designated accounts of the sending users at specific intervals [18].

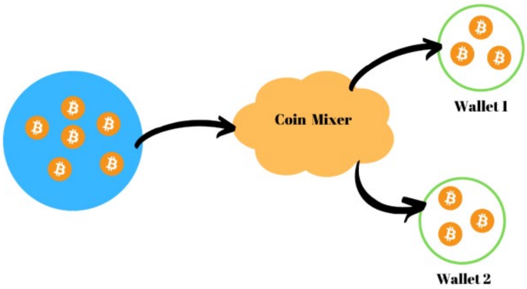
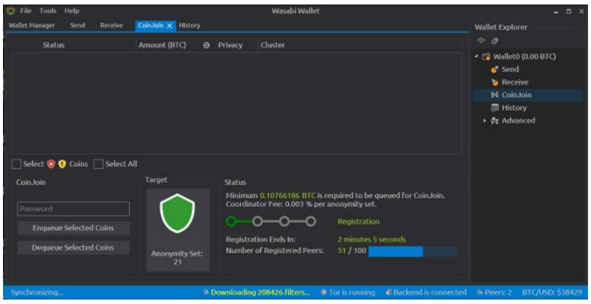


Figure 4. Coin mixer

While some cryptocurrency mixers trade at user-specified times (such as setting the outputs to be made 24 h after the login), some trade after reaching a certain number of entries or after the time required for the next round has elapsed. For example, Wasabi Wallet, one of the most used mixers in the world, makes one round when the number of entries is 100 or every 1 h (Figure.5).



Anonymity Set: 21

Minimum 0.10766186 BTC is required to be queued for CoinJoin.
Coordinator Fee: 0.003 % per anonymity set.

Registration

Registration Ends In: 2 minutes 5 seconds
Number of Registered Peers: 51 / 100

Synchronizing... Downloading 208426 filters... Tor is running Backend is connected Peers: 2 BTC/USD: $38429

Figure 5. Wasabi Wallet Application

Also, mixers with a significant number of users are less likely to be identified as guilty, as some mixers operate on the principle of torrents. In other words, they circulate funds between their own accounts before sending them to the destination address. This method makes it nearly impossible to trace the criminal.

Cryptocurrency mixers can sometimes take the form of a wallet, while other times smart contracts can be designed as mixers [19]. Networks that do not support smart contracts, such as the Bitcoin network, employ bitcoin wallets as mixers. Users who wish to avoid tracking download mixer wallets and transfer their cryptocurrencies from their own wallets to these mixer wallets, where the funds from different users accumulate in a single wallet [20]. Websites like unijoin.io, coinomize.biz, and yomix.io provide coin mixing services and allow users to specify when the mixed cryptocurrencies will exit the mixer [21, 22, 23].

When transferring cryptocurrencies to a mixer wallet, users can choose which wallets the outputs will be sent to and the duration before the outputs are sent. During the login process, a user can send their crypto funds to the mixer in a single transaction and set the outputs to be sent to six different wallets. Moreover, the execution times of these transactions can vary, making it quite challenging to predict which output corresponds to which input value.

In networks that support smart contracts, such as the Ethereum network, smart contracts can also function as cryptocurrency mixers. Smart contracts designed in these networks can act as wallets, hold funds, send funds to other addresses, and most importantly, they are decentralized [24]. Therefore, organizations or groups can create a coin mixer using smart contracts, simultaneously send funds to the smart contract, and forward the outputs to different accounts.

IV. SCENARIO AND DETECTION APPROACHES FOR MONITORING COIN MIXERS

Criminals using coin mixers do not always send the coins they input into the mixer to specific output accounts. In additionally, they have the option to stagger the transfers of the requested funds to the specified output accounts. For example, a user wanting to launder money may transfer a portion of the funds two hours after the initial transaction, and the remaining amount after 72 h. The higher the number and volume of transactions in a mixer per unit of time, the lower the probability of leaving a trace. However, in mixers with very few transactions, suspicious outputs can be traced.

4.1. The Reliability of Cryptocurrency Mixers

For a cryptocurrency mixer to be considered reliable, it must be decentralized and have a large user base.

Decentralization: Security is paramount for a coin mixer, and decentralization is a crucial aspect. Mixers managed by a central system require users to trust an institution or individual, which is not preferred. With transactions managed from a central location, security forces can easily access the obtained records. In short, decentralization is the most important factor for ensuring the safety of a coin mixer.

Number of Users: Another important factor is the number of users using the coin mixer. The anonymity of transactions carried out in a coin mixer is directly proportional to the number of users. Therefore, the more people using a mixer, the more difficult it becomes to track transactions.

4.2. Tracking Scenarios for Cryptocurrency Mixers

One consideration in monitoring mixer processes is the ratio of inputs to outputs. If the number of inputs is high and the number of outputs is lower than the number of inputs, the number of accounts to be tracked will decrease.

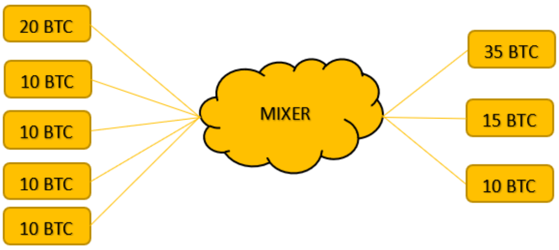


Figure 6. Too many inputs, too few outputs Coin Mixer

As seen in Figure 6, the total number of BTC transferred to the mixer is 60 and the total number of BTC released is 60. When the scenario in Figure 6 is examined, if the person being followed is the owner of the account that transfers 20 BTC and there are three transactions as output, 15 BTC, 10 BTC and 35 BTC, there are different partners working together with the person being tracked. This account should also be followed, as it will result that other accounts transferring to the mixer are associated with this person.

```
function checkInputOutputRatio(transferredInputs, outputTransactions):
    if transferredInputs.length > 0 and outputTransactions.length < transferredInputs.length:
        return true
    else:
        return false
```

If all of the criminal's wallets are being tracked and there are transactions from the criminal's wallets among the entries into the mixer, all the criminal's wallets should be considered as one wallet.

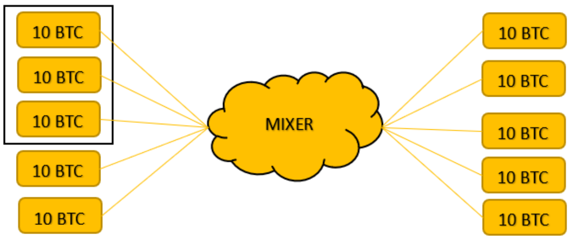


Figure 7. Scenario where suspicious wallets enter the Coin Mixer

As shown in Figure 7, cryptocurrencies from different accounts entering the mixer, which works simply, should be treated as one transaction, and it should be known that all three transactions exiting the mixer are accounts associated with this account. If a mixer takes a set of inputs that will increase its average daily trading volume, the outputs of these inputs are likely to be noticed. This is somewhat similar to the fact that the larger and more ostentatious parent duck is easily distinguished from the baby ducks.

```
function identifyHighVolumeTransaction(inputTransactions, outputTransactions, dailyTradingVolume):
    for transaction in outputTransactions:
        if transaction.value > dailyTradingVolume:
            associatedInput = findAssociatedInput(transaction, inputTransactions)
            if associatedInput is not None:
                associateTransactions(associatedInput, transaction)
```

In this pseudocode, inputTransactions represents the list of input transactions entering the mixer, outputTransactions represents the list of output transactions exiting the mixer, and dailyTradingVolume represents the average daily trading volume. The function identifyHighVolumeTransaction iterates over each output transaction. If the value of the transaction is greater than the daily trading volume, it indicates a high-volume transaction. The function then attempts to find the associated input transaction for the high-volume output transaction by calling the findAssociatedInput function. If an associated input transaction is found, the associateTransactions function is called to associate the input and output transactions.

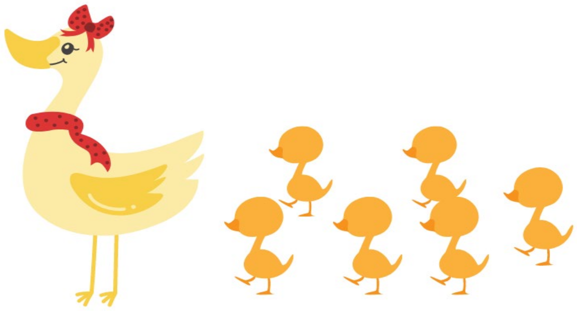


Figure 8. Transaction volume and visibility

As shown in Figure 8, there are no essential features that distinguish baby ducks from each other. If a person says that one of the baby ducks is guilty, it is difficult to guess which baby is guilty. But if he says that the culprit is the biggest and most developed duck (parent duck), it is very easy to determine which he means. The throughput in the mixers was just like in this example. On the other hand, in a scenario where a criminal steal 500 BTC and keeps it all in one wallet. There are two possible scenarios if this criminal wants to use a mixer to avoid being tracked:

In the First Option; After distributing all the money in your wallet to different wallets, transferring them to the mixer and increasing the number of entries, reducing the likelihood of being tracked. This option is also divided into two.

A. The partial outflow of money that is entered in parts.

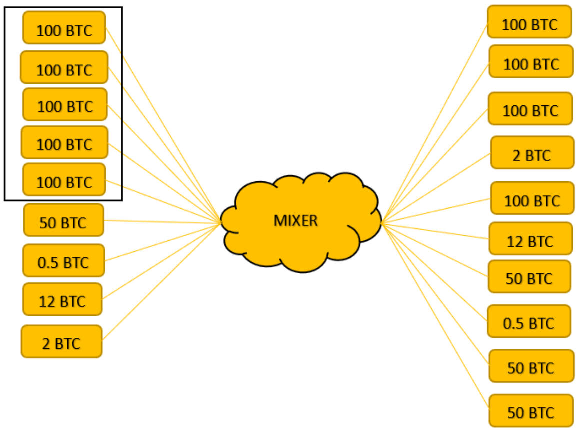


Figure 9. Segmented Entry and Segmented Exit scenario

In a scenario visualized in Figure 9, if the total value of the transfers in the black box is 500 BTC and it belong to the criminal being tracked, the sum of the inputs excluding the inputs made by the criminal can be calculated as 4.5 BTC. When we look at the output values, it is necessary to focus on values greater than 64.5 BTC or 50 BTC. In Figure 9, the suspect has provided 5 inputs of 100 BTC, and there are 4 transactions of 100 BTC as output. In this case, it can be thought that the criminal extracted a transfer with a value of 100 BTC by dividing it out. When examined carefully, there is one 50 BTC transaction as the input value, while there are 3 50 BTC transactions in the output values. That is, it can be said that the criminal split the 100 BTC input into two 50 BTC. One of the important points here is that it is certain that the outputs of 100 BTC belong to the criminal and these transactions should be followed.

```
function trackSplitTransactions(totalTransferValue, inputs, outputs):
    criminalInputs = filterCriminalInputs(inputs)
    sumOfExcludedInputs = calculateSumOfExcludedInputs(criminalInputs)

    for transaction in outputs:
        if transaction.value > (totalTransferValue - sumOfExcludedInputs):
            associateTransactionWithCriminal(transaction)
```

In this pseudocode, totalTransferValue represents the total value of transfers in the black box, inputs represent the list of input transactions, and outputs represents the list of output transactions. The function trackSplitTransactions first filters out the inputs made by the criminal using the filterCriminalInputs function. It then calculates the sum of the inputs excluded from the criminal using the calculateSumOfExcludedInputs function.

B. The money that is entered piecemeal comes out in less pieces or in one piece.

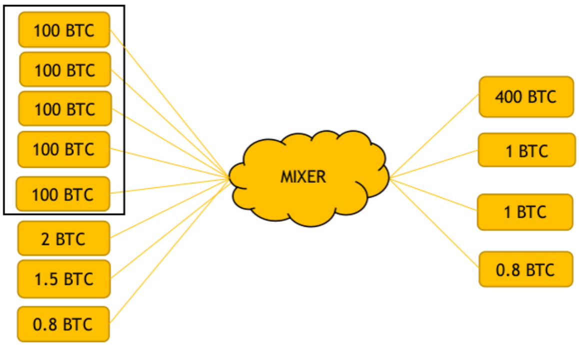


Figure 10. Partial entry, mass exit scenario

As can be seen in Figure 10, the 5 accounts of the criminal that were followed provided 100 BTC input to the mixer. Looking at the output values, there is an eye-catching 400 BTC transaction. On the other hand, there is a high probability that the person who ordered this action is the aforementioned criminal. If attention is paid, it will be understood that the total value of the inputs does not match the total value of the outputs. So, it is likely that the said criminal will extract the remaining BTCs at a different time.

```
function trackMismatchedInputsOutputs(inputs, outputs):
    totalInputValue = calculateTotalInputValue(inputs)
    totalOutputValue = calculateTotalOutputValue(outputs)
    if totalInputValue != totalOutputValue:
        potentialRemainingValue = totalInputValue - totalOutputValue
        identifyPotentialRemainingTransactions(potentialRemainingValue, inputs)
```

In this pseudocode, inputs represent the list of input transactions, and outputs represent the list of output transactions. The function trackMismatchedInputsOutputs first calculates the total value of the inputs using the calculateTotalInputValue function and the total value of the outputs using the calculateTotalOutputValue function.

Next, the function checks if the total input value is different from the total output value. If they do not match, it suggests mismatched inputs and outputs situation. The function then calculates the potential remaining value by subtracting the total output value from the total input value. It calls the identifyPotentialRemainingTransactions function to identify any transactions that may be associated with the remaining value.

In the Second Option; It is to transfer all the money in the wallet to the mixer in one go. This option is also divided into two.

A. Collective outflow of money that is entered collective.

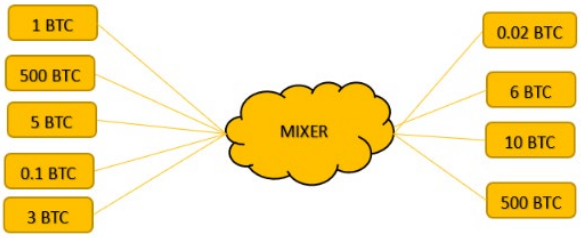


Figure 11. Batch Entry Mass Exit Scenario

In the scenario in Figure 11, the criminal made 500 BTC entries. When the values coming out of the mixer are examined, an; outflow of 500 BTC has been observed. This 500 BTC output is probably the aforementioned culprit.

```
function trackTotalInputOutput(inputValue, outputValue):
    if inputValue == outputValue:
        identifiedCriminal = true
        markAsCriminal(identifiedCriminal)
```

In this pseudocode, inputValue represents the total value of the inputs made by the criminal, and outputValue represents the total value of the outputs observed from the mixer. The function trackTotalInputOutput compares the input and output values. If they are equal, it indicates that the total input and output values match, suggesting that the identified criminal is associated with the 500 BTC output. The function then marks the identified criminal using the markAsCriminal function.

B. Partial outflow of money that is entered collectively.

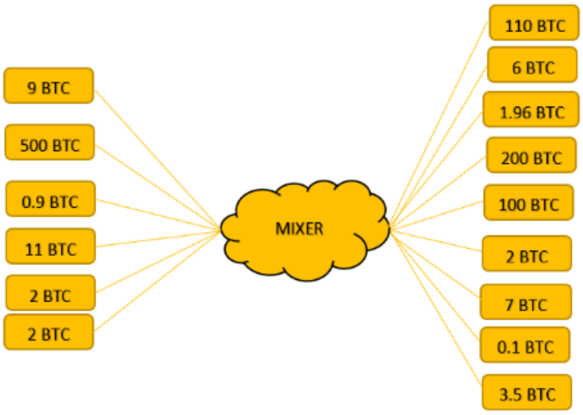


Figure 12. Batch Entry Split Exit scenario

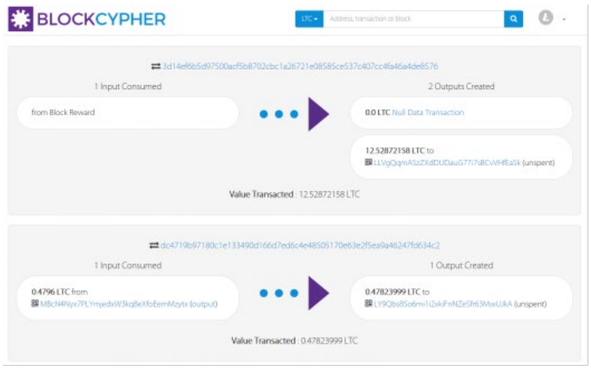
In the scenario in Figure 12, the aforementioned criminal has transferred 500 BTC, and the outputs of any round after the transfer are shown in the image. If we look at the outputs, there are three (100 BTC, 200 BTC, 110 BTC) values that are much more than normal output values. Looking at these available data, it can be said that the aforementioned criminal has a high probability of transferring 310 BTC of 500 BTC in this round. The accounts to which these outputs are transferred and the next transactions of those accounts should be followed.

```
function analyzeOutputs(outputs):
    for each output in outputs:
        if output > normalOutputThreshold:
            identifiedCriminal = true
            transferValue = output
            markAsCriminal(identifiedCriminal, transferValue)
            break
```

In this pseudocode, outputs represent the list of output values observed in the scenario. normalOutputThreshold is a threshold value that determines what is considered a normal output value. The function analyzeOutputs iterates over each output value and checks if it exceeds the normal output threshold. If an output value is higher than the threshold, it indicates a suspicious transaction. The function then marks the identified criminal using the markAsCriminal function and stores the transfer value for further analysis.

V. SAMPLE APPLICATION FOR TRACKING CRYPTOCURRENCY TRANSACTIONS

In open blockchain networks, the transaction performed by the account is clearly recorded in the ledger, so it is not known to whom the transactions occurred [25].



3d14ef6b5d97500acf5b8702cbc1a26721e08585ce537c407cc4fa46a4de8576

1 Input Consumed — 2 Outputs Created

from Block Reward

0.0 LTC Null Data Transaction

12.52872158 LTC to LLVgQqmASzZXdDUDauG77i7sBCVVHfEaSk (unspent)

Value Transacted : 12.52872158 LTC

dc4719b97180c1e133490d166d7ed6c4e48505170e63e2f5ea9a46247fd634c2

1 Input Consumed — 1 Output Created

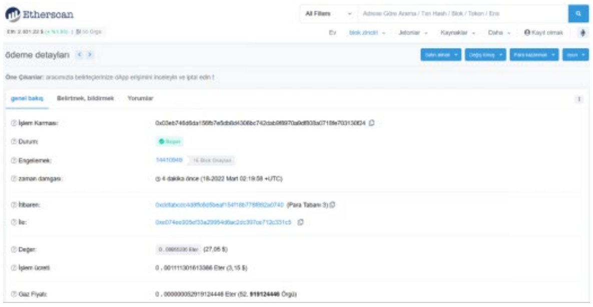
0.4796 LTC from MBcN4Nyx7PLYmjedxW3kq8eXfoEemMzytx (output)

0.47823999 LTC to LY9Qbs8So6mi1i2xkiFnNZeSfr63MwUJkA (unspent)

Value Transacted : 0.47823999 LTC

Figure 13. Two transactions that occurred in the Litecoin block [26].

As shown in the example in Figure 13, it can be easily understood by looking at the ledger which outputs are from which account and when the outputs occurred. This provides an advantage in terms of forensic computing. If a cryptocurrency wallet/transaction is to be tracked in a forensic investigation, only information provided by an explorer should not be trusted. To avoid any doubt, transactions on more than one explorer must be followed and the information obtained from the explorers must be compared. If the case is an important case such as a terrorism case, the wallet ledger in question should be downloaded and research should be done on that ledger.



Öne Çıkanlar: aracınızda belirteçlerinize dApp erişimini inceleyin ve iptal edin !

İşlem Karması: 0x03eb746d6da158fb7e5db8d4306bc742dab9f8970a9df808a0718fe703130f24

Durum: Başarı

Engellemek: 14410049 16 Blok Onayları

zaman damgası: 4 dakika önce (18-2022 Mart 02:19:58 +UTC)

İtibaren: 0xddfabcdc4d8ffc6d5beaf154f18b778f892a0740 (Para Tabanı 3)

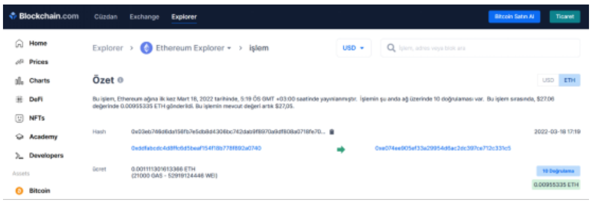
İle: 0xe074ee905ef33a29954d6ac2dc397ce712c331c5

Değer: 0.00955335 Eter (27,05 $)

İşlem ücreti: 0.001111301613386 Eter (3,15 $)

Gaz Fiyatı: 0.000000052919124446 Eter (52.919124446 Örgü)

Figure 14. Screenshot taken from etherscan.io [27]



Özet

Bu işlem, Ethereum ağına ilk kez Mart 18, 2022 tarihinde, 5:19 ÖS GMT +03:00 saatinde yayınlanmıştır. İşlemin şu anda ağ üzerinde 10 doğrulaması var. Bu işlem sırasında, $27.06 değerinde 0.00955335 ETH gönderildi. Bu işlemin mevcut değeri artık $27,05.

Hash 0x03eb746d6da158fb7e5db8d4306bc742dab9f8970a9df808a0718fe70... 2022-03-18 17:19

0xddfabcdc4d8ffc6d5beaf154f18b778f892a0740 → 0xe074ee905ef33a29954d6ac2dc397ce712c331c5

Ücret 0.001111301613386 ETH (21000 GAS - 52919124446 WEI)

10 Doğrulama

0.00955335 ETH

Figure 15. Screenshot taken from Blockchain.com [28]

When the screenshots taken from Etherscan.io shown in Figure 14 and the screenshots taken from Blockchain.com shown in Figure 15 of the same transaction are examined; It is seen that both contain the same information for the same transaction value (hash value). This confirms the value of the transaction in question and between which accounts it took place.

5.1. Ways to Follow for Suspicious Accounts

There are two ways for a suspected cryptocurrency wallet to be tracked by the digital forensic investigator, downloading the Coin ledger and obtaining information from third-party sites.

A. Downloading the Coin Ledger.

This method is quite difficult. Because after the notebook is downloaded, an explorer is also needed to navigate on that notebook. In addition, even if the explorer is written, if the tracked wallet has made too many transactions and there are complex transactions that cannot be examined manually, another tool should be written to determine the relationship between the accounts that perform these transactions. Also, since the blockchain technology used by every cryptocurrency is not the same, these transactions need to be repeated for every cryptocurrency.

B. Collecting Information Using Third Party Sites Like Maltego.

If the followed account has made too many transactions, it is very tedious and time consuming to manually track these transactions and link the accounts where the transactions occurred. For such cases, the use of information-gathering tools such as Maltego eases the processing load of the reviewer. Before starting the process in Maltego, the add-on to be monitored must be installed. Related add-ons can be listed by clicking on the “Cryptocurrency” category in the Add-ons section. In the example in this study, it was continued with the Tatum plugin made by Maltego himself. Other options are also available. For example, the Blockchain.info (Bitcoin) plugin pulls data from Blockchain.com.

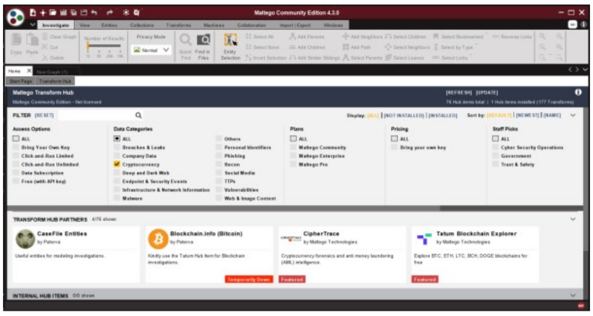


Figure 16. The Screenshot of Maltego homepage [29]

After the selection is made and the plugin is installed, a new review page should open.

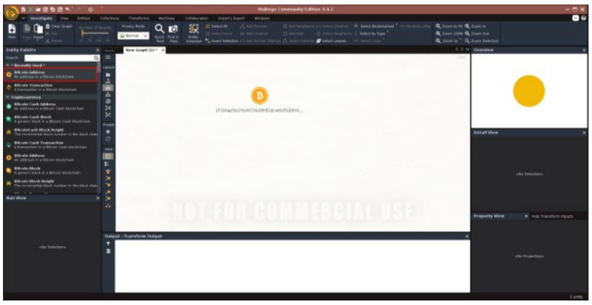

Maltego Community Edition 4.3.1
Entity Palette
Bitcoin Address
Bitcoin Transaction
New Graph (1)
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4...
NOT FOR COMMERCIAL USE
Output - Transform Output

Figure 17. Wallet/transaction tracking screen-1 [29]

The “Bitcoin Address” option on the left side of the page that opens should be selected and the address to be followed should be entered here. The resulting shape should be right-clicked with the mouse and the Tatum Blockchain Explorer option should be selected in the pop-up menu.

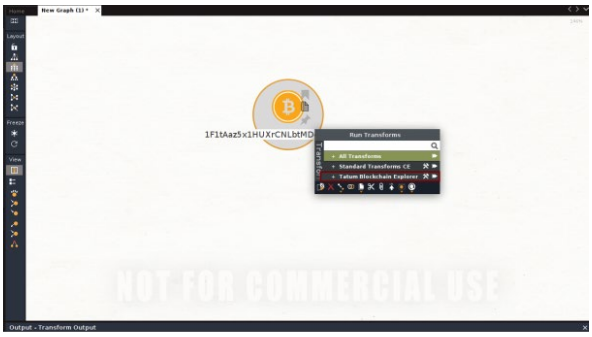


Figure 18. Wallet/transaction tracking screen-2 [29]

A choice must be made among the options that appear, according to the purpose of the examiner. For example, "To Input Address" option should be selected if it is desired to determine from which wallet the funds transferred to the said wallet come from. This option only finds transactions from other wallets. But the "To Input Transaction" option reflects UTXO inputs and normal transactions.

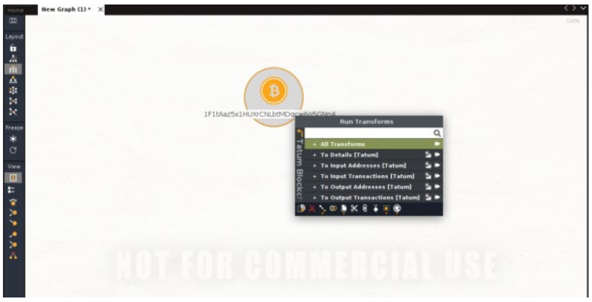

New Graph (1)
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4
Run Transforms
Tatum Blockch
+ All Transforms
+ To Details [Tatum]
+ To Input Addresses [Tatum]
+ To Input Transactions [Tatum]
+ To Output Addresses [Tatum]
+ To Output Transactions [Tatum]
NOT FOR COMMERCIAL USE

Figure 19. Wallet/transaction tracking screen-3 [29]

An image of the selection screen is shown in Figure 19. Controls can be provided on wallets by making relevant selections on this screen.

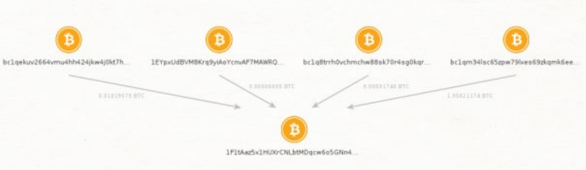

bc1qekuv2664vmu4hh424jkw4j0kt7h...
1EYpxUdBVM8Krq9yiAoYcnvAF7MAWRQ...
bc1q8trrh0vchmchw88sk70r4sg0kqr...
bc1qm34lsc65zpw79lxes69zkqmk6ee...
0.01019579 BTC
0.00006695 BTC
0.00591740 BTC
1.95821174 BTC
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4...

Figure 20. “To Input Address” Window [29]

As shown in Figure 20, after selecting the "To Input Address" option, it can be clearly seen that 11 wallets have been transferred to the address we have followed. The same process can be applied to a user who send money. Thus, the number of suspicious wallets can be increased.

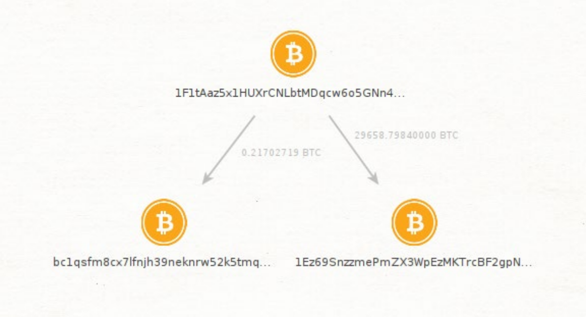

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4...
0.21702719 BTC
29658.79840000 BTC
bc1qsfm8cx7lfnjh39neknrw52k5tmq...
1Ez69SnzzmePmZX3WpEzMKTrcBF2gpN...

Figure 21. Applying the “To Input Address” option to other addresses [29]

Figure 21 shows the screenshot showing that money transfers made to the address are also clearly visible because of applying the "To Input Address" option to other addresses. One of the points that should not be forgotten here is “time”. As these outputs are all transactions so far, follow-up needs to be done considering the time of the crime.

VI. CONCLUSIONS

Using blockchain technology, cryptocurrencies have become significant financial instruments for criminal and terrorist organizations, enabling them to pursue their objectives through their decentralized structure, peer- to- peer processing, and user anonymity. Undoubtedly, as digital transformation unfolds rapidly, crimes have transitioned into virtual realms, leading to the development of numerous unique money laundering methods in the criminal world. However, these crimes cannot escape the untraceable methods brought forth by the digital age. While criminals continue to employ methods and platforms to conceal their activities, law enforcement agencies are determined to combat these activities. Consequently, states, intelligence organizations, and law enforcement units must systematically understand existing systems and expose criminal methods.

This study highlights blockchain-based methods in the context of money laundering. It discusses the methods and steps digital investigators should follow when monitoring cryptocurrency wallets, transactions, and money laundering techniques implemented using blockchain-based systems. One of these methods, namely the use of mixers to hide money trails, is examined through the creation of various scenarios.

While the proposed solutions presented in this study are applicable to mixers with a low volume of transactions and straightforward operational logic, theit process becomes more complex in specific mixers with several transactions, making it challenging to distinguish the targeted criminal from other users. Nevertheless, considering that the blockchain system can contribute to detecting criminals within this intricate and anonymous structure, this study is a significant step toward preventing crimes.

Furthermore, an exemplary application is provided for digital forensic experts and law enforcement officers, outlining the initial steps required to trace such illicit funds. The application proposes an approach for detecting money transfers through manual analysis of transaction ledgers and subsequent analysis using third-party applications.

While crypto-based methods are complex, this study delves into essential clues for tracking illicit funds, which can be invaluable for investigating illicit financial activities. It is anticipated that this study will contribute to the literature and support law enforcement efforts by shedding light on the topics discussed and inspiring new perspectives.

REFERENCES

[1] M. Milutinović, "Cryptocurrency Tt - Крипто Валуте," ***Ekonomika***, vol. 64, no. 1, pp. 105–122, (2018), doi: 10.5937/ekonomika1801105m.

[2] Naqvi, Syed. "Challenges of Cryptocurrencies Forensics: A Case Study of Investigating, Evidencing and Prosecuting Organised Cybercriminals." ***Proceedings of the 13th International Conference on Availability, Reliability and Security*** (2018), doi: 10.1145/3230833.3233290.

[3] "Bitcoin open source implementation of P2P currency - P2P Foundation." http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (accessed May 30, 2022).

[4] "Büyük Kripto Para Birimi Dolandırıcılığı." https://www.forbes.com/sites/jayadkisson/2018/11/20/the-great-cryptocurrency-scam/?sh=4b68b2cf359f (accessed May 29, 2022).

[5] ONS, "Overview of fraud and computer misuse statistics for England and Wales," pp. 1–21, 2018, [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25.

[6] E. Fletcher, C. Larkin, and S. Corbet, "Countering money laundering and terrorist financing: A case for bitcoin regulation," ***Research in International Business and Finance***, 2021, doi: 10.1016/j.ribaf.2021.101387.

[7] M. Freeman, "The sources of terrorist financing: Theory and typology," ***Stud. Confl. Terror.***, 2011, doi: 10.1080/1057610X.2011.571193.

[8] T. A. Hulme, "The ethical and legal aspects of blockchain technology and cryptoassets," in ***Batten-Corbet-Lucey Handbooks in Alternative Investments***, 2020, 10.1515/9783110660807-008.

[9] M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert, and P. Pesch, "Safeguarding the evidential value of forensic cryptocurrency investigations," ***Forensic Sci. Int. Digit. Investig.***, vol. 33, 2020, doi: 10.1016/j.fsidi.2019.200902.

[10] V. Veselý and M. Žádník, "How to detect cryptocurrency miners? By traffic forensics!," ***Digit. Investig.***, 2019, doi: 10.1016/j.diin.2019.08.002.

[11] M. Weber et al., "Anti-Money Laundering in Bitcoin: Experimenting with Graph ***Convolutional Networks for Financial Forensics***," Jul. 2019, doi: 10.48550/arxiv.1908.02591.

[12] G. Tziakouris, "Cryptocurrencies - A forensic challenge or opportunity for law enforcement? An INTERPOL perspective," ***IEEE Secur. Priv.***, 2018, doi: 10.1109/MSP.2018.3111243.

[13] "Money laundering in Australia 2011 | AUSTRAC." https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidanceresources/money-laundering-australia-2011 (accessed Jul. 04, 2022).

[14] K. Singh and P. Best, "Anti-Money Laundering: Using data visualization to identify suspicious activity," ***Int. J. Account. Inf. Syst.***, 2019, doi: 10.1016/j.accinf.2019.06.001.

[15] "Blockchain.com | Login." https://login.bııockchaȋn.com/#/login?product=wallet (accessed Jul. 05, 2022).

[16] M. Brewczyńska, "Financial Intelligence Units: Reflections on the applicable data protection legal framework," ***Comput. Law Secur. Rev.***, 2021, doi: 10.1016/j.clsr.2021.105612.

[17] "Kara Para Aklamayı Önleme (AML) Nedir? | Binance Academy." https://academy.binance.com/tr/articles/what-is-anti-money-laundering-aml (accessed Jul. 05, 2022).

[18] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., &#38; Felten, E. W., **Mixcoin: Anonymity for Bitcoin with accountable mixes** doi: 10.1007/978-3-662-45472-5_31 (2014).

[19] Wang, Z., Chaliasos, S., Qin, K., Zhou, L., Gao, L., Berrang, P., Livshits, B.; Gervais, A. (2023). On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy. ***Proceedings of the ACM Web Conference 2023***, 2022–2032. https://doi.org/10.1145/3543507.3583217

[20] Wu, L., Hu, Y., Zhou, Y., Wang, H., Luo, X., Wang, Z., Zhang, F., &#38; Ren, K. (2021). Towards understanding and demystifying bitcoin mixing services. The Web Conference 2021 - ***World Wide Web Conference, WWW 2021***, 33–44. https://doi.org/10.1145/3442381.3449880

[21] UniJoin, Retrieved May 21, 2023, from https://unijoin.io/en/coinjoin/btc

[22] Coinomize.biz - Start Mixing - Bitcoin Mixer | Bitcoin Blender. Retrieved May 21, 2023, from https://coinomize.biz/start-mixing

[23] Bitcoin Mixer — YoMix.IO. (n.d.). Retrieved May 21, 2023, from https://yomix.io/en/bitcoin-mixer-blender

[24] Su Liu and Jian Wang. DMC: Decentralized Mixer with Channel for Transaction Privacy Protection on Ethereum; ***2nd International Conference on Machine Learning Techniques and NLP (MLNLP 2021)***. https://doi.org/10.5121/csit.2021.111412

[25] Gupta S., Sadoghi M. (2021). Blockchain Transaction Processing. ***Encyclopedia of Big Data Technologies***, 366–376. https://doi.org/10.1007/978-3-319-77525-8_333

[26] "BlockCypher - Blockchain Web Hizmetleri." https://www.blockcypher.com/ (accessed Jul. 13, 2022).

[27] "Ethereum (ETH) Blok Zinciri Gezgini." https://etherscan.io/ (accessed Jul. 13, 2022).

[28] "Blockchain.com | Bitcoin, Ethereum ve daha fazlasını güvenle satın alın." https://www.blockchain.com/ (accessed Jul. 13, 2022).

[29] "Main Page - Maltego." https://www.maltego.com/ (accessed May. 21, 2022).

[30] Chung, Heewon, Kyoohyung Han, Chanyang Ju, Myungsun Kim, and Jae Hong Seo. "Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger." ***Cryptology ePrint Archive***, Paper 2020/735, 2020. doi: 10.1109/ACCESS.2022.3167806.

[31] Blockchain Explorer - MoneroHash. (n.d.). Retrieved May 24, 2023, from https://monerohash.com/explorer/tx/b1e814aed40bf79a2b652753edca346d15bae90ee4d363c25b9c0d915a82430f (accessed May. 21, 2022).

[32] Hakkımızda - NakitCoins. Retrieved July 1, 2023, from https://nakitcoins.com/hakkimizda.

[33] Exchange BTC - Bitcoin exchange network - FlyingAtom. Retrieved July 1, 2023, from https://flyingatom.com/en/exchange-bitcoin/.

[34] Motsi-Omoijiade, I. D. (2018). Financial Intermediation in Cryptocurrency Markets – Regulation, Gaps and Bridges. ***Handbook of Blockchain, Digital Finance, and Inclusion***, Volume 1: Cryptocurrency, FinTech, InsurTech, and Regulation, 207–223. https://doi.org/10.1016/B978-0-12-810441-5.00009-9