UDC 343.1:65.012.8+004 DOI: https:// doi.org/ 10.32631/ pb.2023.3.09

VITALIY VIKTOROVYCH NOSOV,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Counteracting Cybercrime;
https:// orcid.org/ 0000-0002-7848-6448,
email: vitnos.g@gmail.com;

OLEKSANDR VOLODYMYROVYCH MANZHAY,
Candidate of Law, Professor,
Kharkiv National University of Internal Affairs,
Department of Counteracting Cybercrime;
https:// orcid.org/ 0000-0001-5435-5921,
e-mail: sofist@ukr.net;

VICTORIA OLEKSANDRIVNA KOVTUN,
Cyber Police Department of the National Police of Ukraine,
2nd Department (Open Source Analysis) of
the 4th Directorate (Operational and Analytical
Support and Open Source Analysis);
https:// orcid.org/ 0000-0003-1263-5970,
email: cybercop322@gmail.com

TECHNICAL, FORENSIC AND ORGANIZATIONAL ASPECTS OF WORK WITH MONERO CRYPTOCURRENCY

The forensic, organizational and technical features of the work of law enforcement agencies with the Monero cryptocurrency in the context of conducting pre-trial investigations and operational-detective activities are analyzed. The development of the Monero system is described. The reasons and trends in the use of Monero by offenders are outlined, and the scheme of operation of this payment system, which ensures its increased confidentiality, is also shown. Examples of criminal offenses in which Monero is used are given. The OpenAlias functionality is disclosed to facilitate work with Monero addresses. The possibility of identifying participants in Monero transactions is studied. It is stated that there are currently no effective methods of such identification without knowledge of the public address and the corresponding keys, especially if users use additional protective mechanisms such as connecting to the TOR network. The features of the forensic investigation of computer equipment used to work with Monero
are disclosed. It was found that the most effective is the study of traces of work with Monero, which are removed from the relevant computer equipment of the person of interest. Useful information can be stored in RAM, on disk, partially in network traffic. Artifacts that should be paid attention to during the inspection and search were identified. Atomic exchange was modeled

(Atomic Swaps) XMR to determine the trace picture and identify artifacts of increased attention during the implementation of forensic procedures. The fact of the implementation of an atomic exchange to obfuscate traces may be evidenced by the presence of specific software files on the disk that were used for this purpose. An algorithm for extracting XMR using multisig
addresses is proposed, from which it is possible to withdraw funds only when applying digital signatures of several people. The operation of this algorithm is simulated in the Stagenet test network. It is concluded that law enforcement agencies should focus on classic investigative and operational measures to identify Monero users of interest. At the same time, there are effective mechanisms for documenting traces of work with the Monero payment system and confirmed methods for extracting passphrases to crypto wallets and other sensitive information about the movement of funds in the Monero system from computer equipment.

Keywords: *cryptocurrency, Monero, law enforcement agencies, combating crime, fixing traces.*

Original article

INTRODUCTION. The emergence of blockchain-based technologies has opened up new opportunities for individuals who wish to conduct financial and other transactions remotely, anonymously, and without the help of a third party, such as a bank. At the initial stage, cryptocurrency transactions were mostly focused on working with Bitcoin or Ethereum. However, the situation has changed over time, and today you can already see dozens and hundreds of

new projects for the creation and support of cryptocurrency assets.

Interest in the cryptocurrency market and technology is often shown not only by good-natured users, but also by criminals. Virtual assets are increasingly becoming an acceptable form of payment for many illegal activities, mainly due to their ability to

individual cryptocurrencies to perform anonymous transactions remotely. J. Sampson (2018) also points out that working with digital coins can be destructive and dangerous due to the nature of the software,

which is used for this. Cryptocurrency users seeking privacy rely on anonymization methods such as

CoinJoin and ring transactions. By using such technologies, good users potentially provide anonymity to malicious actors (Keller, Florian, Böhme, 2021).

Currently, cryptocurrency assets are most often used to obtain illicit benefits, pay for drug deals, in schemes related to human trafficking, contract killings, extortion, fraud, and money laundering. For example, during the study of the content of the Legalizer website in early 2022

It was found that the largest number of online drug stores with the ability to pay with cryptocurrency is concentrated in the cities of Kharkiv, Kyiv, Odesa, Dnipro, Lviv, Mykolaiv, and Zaporizhia.

It should be noted that previously the main currencies in criminal schemes were Bitcoin or Ethereum. However, the technology of their operation does not fully allow for maintaining anonymity. To overcome this problem, several new cryptocurrencies have been developed that guarantee the confidentiality of transactions and anonymity for their users (in particular ZCash, Monero, etc.) (Damgård et al., 2021).

From a privacy perspective, Monero's key innovation is its use of the ring confidential transaction protocol.

(RingCT) to hide the sender address and transaction amount, as well as using a stealth address to hide the recipient address chewer. Monero has become a medium of exchange on the black market. Three of the five largest black markets accept Monero as a means of payment. Cybercriminals have realized that using Bitcoin allows them to reveal their identity through blockchain transactions, so they are increasingly demanding ransoms in Monero coins (Zhang, Xu,

2022). For example, in a global context, Bitcoin was used in drug deals despite being traceable, while Monero became untraceable in 2017 due to an update to its privacy (Bahamazava, Nanda, 2022).

Given the above, it is extremely important for law enforcement agencies to master the methodology of identifying participants in Monero transactions, conducting proper forensic research of computer equipment used for Monero transactions, and seizing the relevant crypto assets.

PURPOSE AND OBJECTIVES OF THE RESEARCH. In previous works, we have already addressed some issues of law enforcement agencies' work with Bitcoin (Nosov, Manzhai, 2021) and Ethereum (Nosov, Manzhai, Panchenko, 2022). *Purpose*

This article analyzes certain technical and forensic aspects of working with traces related to Monero, as well as demonstrating a model for extracting the corresponding cryptoassets.

To achieve the goal, you need to complete the following *tasks:*

ÿ investigate the issue of using Monero for illegal purposes;

ÿ outline the features of the Monero cryptocurrency;

ÿ describe some aspects of forensic investigation of computer equipment used to work with Monero;

ÿ conduct a simulation of XMR atomic swaps to determine the subsequent picture;

ÿ demonstrate the XMR mining model.

The above study is one of the first attempts to study the Monero system in the context of the work of law enforcement agencies in Ukraine.

RESEARCH METHODOLOGY. The article uses a number of quantitative and qualitative methods, which together allow for a comprehensive
to study the relevant object. Historical and statistical methods were used when analyzing the use of Monero for illegal purposes in Ukraine and the world. In order to study the structural organization of Monero technology

The system analysis method was used. The modeling method was used to work out manipulations with the test cryptocurrency network, the skills of potential withdrawal of the corresponding virtual assets, as well as to determine the trace pattern that is formed by the results of atomic swaps of XMR.

RESEARCH RESULTS AND DISCUSSION. At the time of the study, crypto-

Monero (XMR) is in 33rd place by market capitalization, which is the product of the price of the XMR coin and the total number of coins in circulation (18.15 million)1 and is $2,796,919,510.

USA. According to Chainalysis2 's 2022 Cryptocrime Report, the number of darknet markets supporting Monero increased from 45% to 67% in 2021, with some markets exclusively supporting Monero, such as Archetyp

(Fig. 1) and the updated Alphabay (Fig. 2).

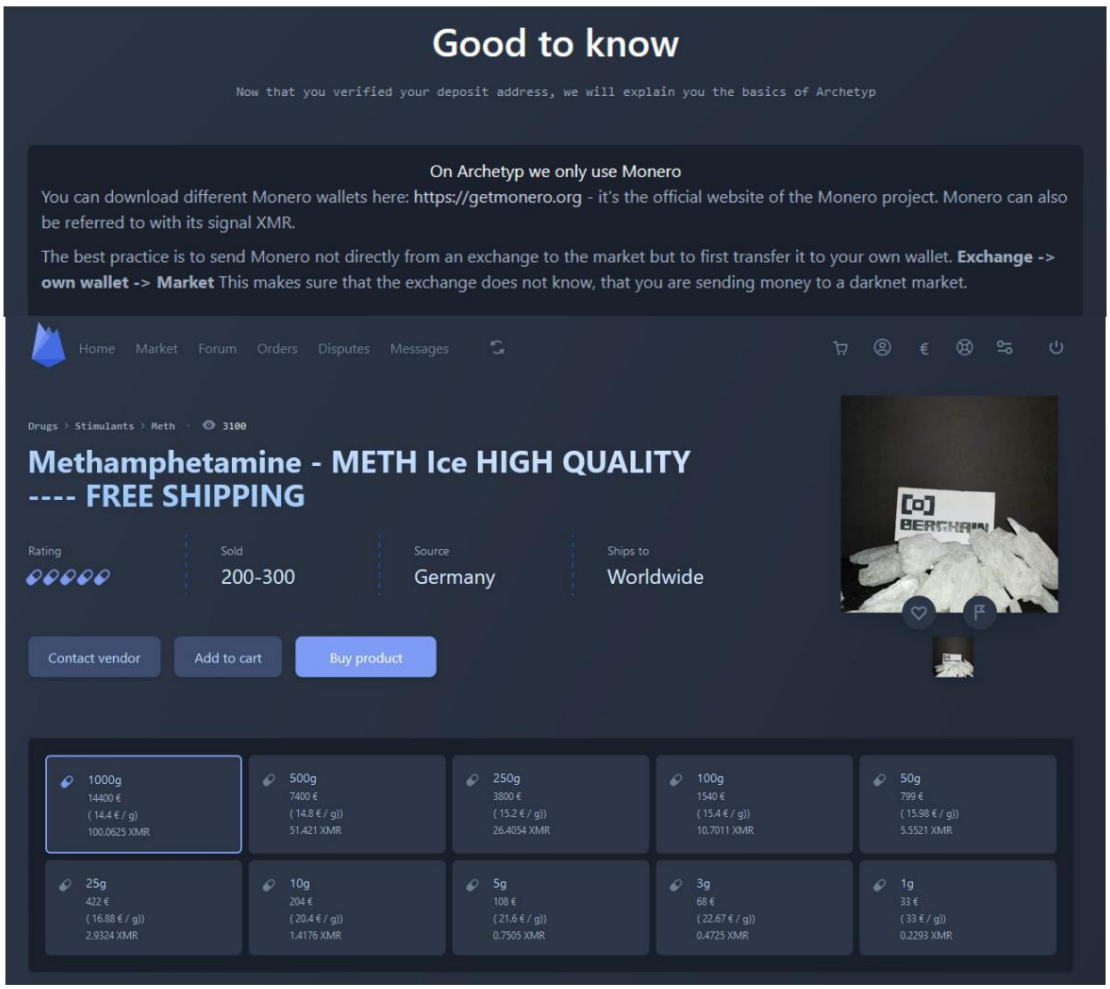

Fig. 1. Archetyp darknet marketplace payment2 exclusively in Monero (XMR)

1 Monero Price: XMR Live Price Chart // CoinGecko : site. URL: https://www.coingecko.com/en/coins/monero (access date: 01.07.2023).

2 The 2022 Crypto Crime Report // Chainalysis : website. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf (accessed: 01.07.2023).

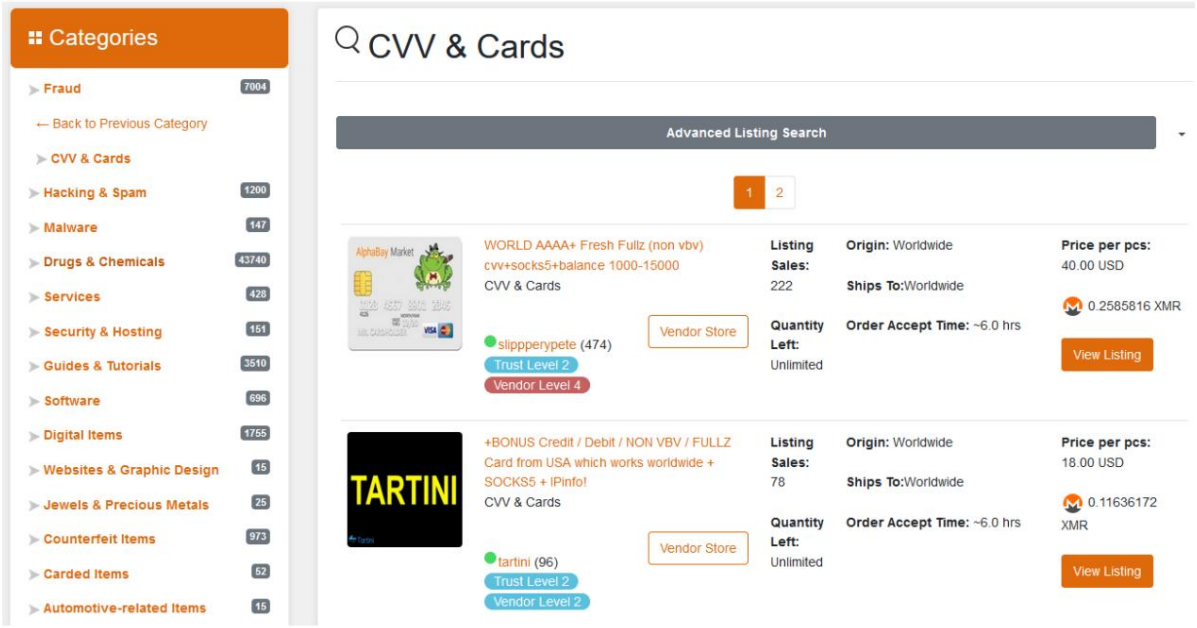

Fig. 2. Alphabay darknet marketplace with payment exclusively in Monero (XMR)

Chainalysis' 2023 Cryptocrime Report1 estimates that illicit cryptocurrency transactions are worth $20.6 billion. It is important to note that most cybercrime remains latent. For example, according to the US Department of Justice, only one in seven (or 15% of all) cybercrime cases is reported to law enforcement.2 Conservative estimates suggest that the true value of illicit cryptocurrency transactions, excluding money laundering transactions, is at least $144.2 billion.3

Monero (XMR) is a cryptocurrency that is popular with criminals because it is anonymous and untraceable. Monero is based on the CryptoNight hash proof-of-work algorithm, which is derived from the CryptoNote protocol. The CryptoNote protocol has significant algorithmic differences compared to Blockchain obfuscation. One-time ring signatures anonymize the sender address of a transaction. In addition, the Monero mining process does not depend on specialized architectures such as GPUs (Handaya, Yusoff, Jantan, 2020).

Monero is often used to pay for data decryption (Fig. 3) after a computer system has been infected with ransomware4.

1 The 2023 Crypto Crime Report // Chainalysis : website. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf (accessed: 01.07.2023).

2 Martin B. The Unseen Problem of Unreported Cybercrime // Anapaya: website. 09.12.2023. URL: https://www.anapaya.net/blog/the-unseen-problem-of-unreported-cybercrime (access date: 07/01/2023).

3 Crypto Money Laundering: How Criminals Cash Out Billions in Bitcoin and Other Cryptocurrencies // Chainalysis: website. 01/15/2020. URL: https://blog.chainalysis.com/reports/crypto-laundering (accessed: 07/01/2023).

4 Young M. Monero's crypto of choice as ransom-ware 'double extortion' attacks increase 500% // Cointelegraph: site. 20.04.2020. URL: https://cointelegraph.com/news/monero-crypto-of-choice-as-ransomware-double-extortion-attacks-increase-500 (access date: 01.07.2023).

Fig. 3. Monero (XMR) ransom demand for decryption of files

Russian fundraising campaigns to support aggression against Ukraine offer Monero as a transfer option (Fig. 4).

Fig. 4. An example of using Monero to raise funds for the needs of the Russian army

In 2019, the work “A First Look at the Crypto Mining Malware Ecosystem” (Pastrana, Suarez-Tangil, 2019) was published, in which authors from various sources attempted to analyze the relevant illegal cryptocurrency mining scheme using malware. According to their calculations from open sources, the largest number of campaigns implemented using malware for mining was focused on the use of Monero wallet addresses (2,449). The same is confirmed in other works of scientists (Zimba et al., 2018; Russo, Šrndic, Laskov, 2021; Musch et al al., 2019). Client-side browser mining is now also being considered as an alternative to monetizing services through advertising and is quite widely represented in the context of using Monero (Rüth et al., 2018).

As for the legal aspect of documenting criminal activity using Monero, in his work S. Ketineni and I. Cao (2020) analyzed 124 criminal proceedings from the PRC, South Korea and Japan. The analysis found that in at least two cases, Monero used in international criminal activity.

Features of the Monero payment system

The main differences between the Monero payment system and Bitcoin or Ethereum are the increased level of confidentiality (anonymity) of transactions and users. For this purpose, they use (Fig. 5):

– ring signatures, which hide the address from which the funds are spent among a group of other selected addresses;

– stealth addresses, which are random one-time addresses for each transaction and which the recipient of funds accesses through keys from the main address;

– ring confidential transactions (RingCT), which hide the amount of the transfer;

– garlic routing Kovri, which hides the IP addresses of the hosts of users of the Monero payment system (not yet implemented by default).

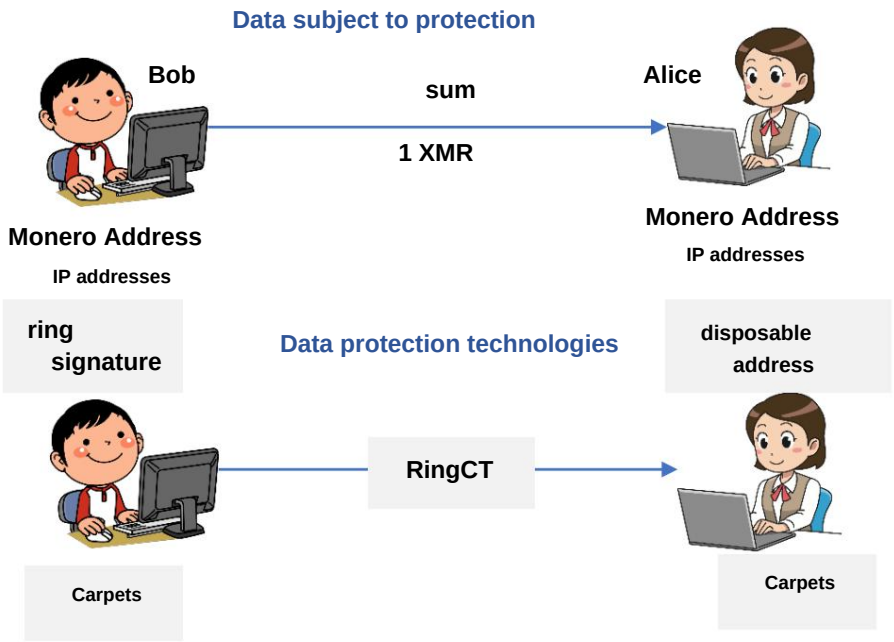

Fig. 5. Technologies for ensuring the confidentiality (anonymity) of Monero transactions and users

Ring signatures will only be traceable if the same user signs the same message twice with the same private key (Peili, Haixia, 2020). A characteristic of Monero is that the user has two key pairs – private/public spending keys *(ks, Ks)* and private/public viewing keys *(kv,* Kv). Private keys are typically created by generating a mnemonic phrase (seed) of 13 to 25 words in a language (English, Spanish, Portuguese, Japanese, Esperanto) etc.) Primary address

user is a pair of public keys *(Ks,* Kv), which is combined with the prefix 0x12, a checksum (4 bytes of Keccak256 hash from *0x12|Ks|Kv)* and represented in Base581 encoding:

Base58(0x12 | *Ks* | *Kv* | checksum) = "4 ……." [95 characters].

So, the main addresses start with the number 4 and can contain lowercase and uppercase Latin letters and numbers, except for 0 (zero), O (uppercase Latin o), I (uppercase Latin i), l (lowercase Latin L):

123456789ABCDEFGHJKLMNPQRSTUVWXY Zabcdefghijkmnopqrstuvwxyz.

Monero users can generate subaddresses from two pairs of primary address keys *(ks,* Ks)/ (kv, *Kv) ,* which are formed through the corresponding public subkeys *(Ks,i, Kv,i):*

Base58(0x2A | *Ks,i* | *Kv,i* | checksum) = "8 ……." [95 characters].

Subaddresses start with the number 8. Funds sent to subaddresses can be viewed and spent using the private viewing and spending keys of the main address. Examples of Monero addresses:

41uD5Tha7H3K2vtEhBWa7WddUiBgbjRLgT57x59 BaFF4GFTrFhkP2Z6ieif5XnVx26Tz2a7WNZSz8b7L mWy3txi7GUVfTgQ;
899iDfG5K4UFG8wQctki3sULRF28PvApthSb2xeHy M7PV2AXxyJs31LVUD3ZNyQU1cXSK9NjyRPxCbvh HG2ByCz3M59HL4C.

An alternative to subaddresses in Monero can be so-called integrated addresses, which contain a payment identifier (Payment ID) (a random string up to 8 bytes long) needed to link incoming payments to a specific sender or invoice. An integrated address is formed as follows:

Base58(0x13 | Ks | Kv | Payment ID | checksum) = "4 ……." [106 characters].

Moreover, the Payment ID in the address can be encrypted and accessible for decryption only by the recipient of the payment.

To simplify human use public main, sub- and integrated Monero addresses have introduced the ability (Open-Alias) to use an email address or domain name as an alias for a specific Monero address, for example donate@-getmonero.org or donate.getmonero.org. For this purpose, special accounts are created on the global network.

cial secure DNS servers containing matching records with the following syntax2:

oa1:xmr recipient_address=46BeWrHpwXmHDpDEUmZBW ZfoQpdc6HaERCNmx1pEYL2rAcuwufPN9rXHHtyU A4QVy66qeFQkn6sfK8aHYjA3jk3o1Bv16em; recipient_name=Monero Development.

The conversion of an email or domain name into a Monero address via a query to the appropriate DNS server is implemented by a crypto wallet.

Monero's public main, sub, and integrated addresses are not directly listed in transactions and are therefore not included in the Monero blockchain. From the recipient's public address, the sender of the payment creates a one-time (invisible) address (stealth address), the value and the possibility of spending funds from which are available to the owner of the key pairs of the corresponding public address. The recipient's private viewing key *ks* is used to determine the available one-time addresses in the blockchain to which the funds have been received, and the recipient's private spending key *kv is used* to further spend funds from these addresses.

Monero has group addresses (multisignature addresses), from which it is possible to spend funds only with the consent (signature) of m users out of n. For such addresses, the pairs of group review and spending keys are formed from the key pairs of the group members. The syntax of a group address is the same as a regular one.

Access to the Monero blockchain for transaction analysis can be obtained through the available global network resources, for example local-monero.co/ blocks, blockchair.com/monero, mo-nero.com/explorer, etc. According to known hash transactions (Fig. 6) from the point of view of investigations you can install:

– UTC time of entry of the transaction into the blockchain;

– the number of disposable addresses (Inputs (2)) from which funds were spent, but without the exact identification of the addresses themselves;

– disposable addresses to which funds are transferred came out (Outputs (2), Stealth address).

1 Monero Addresses Cheatsheet // Monero : site. URL: https://www.getmonero.org/library/MoneroAddressesCheatsheet20201206.pdf (access date: 01.07.2023).

2 OpenAlias. Simplifying the World. URL: https://openalias.org (accessed: 01.07.2023).

Transaction

Tx hash:	973f2d2130571e67a52d2b8a979a3a858ce043718d13212d8550bb3124c9983f
Tx prefix hash:	8b9c90509adf3065ccc65e4c7d950ed41668c748ebaadcd8da7b6f694054e486
Tx public key:	1fc448607d7ae2635b62a5fcf077a997734837f2d76b697e8025d8b4935d3db6
Block:	2584039
Payment ID (encrypted):	4b3ecd2a048e0e6d
Output total:	?
Timestamp [UTC]:	2022-03-20 21:53:00
Fee:	0.000008810000
Tx size:	1.9258 Kb
Tx version:	2
# of confirmations:	313195
RingCT/type:	yes/5
Extra:	011fc448607d7ae2635b62a5fcf077a997734837f2d76b697e8025d8b4935d3db60209014b3ecd2a048e0e6d

2 inputs(s) for total of ? xmr

#	Key image (click row to expand)	Amount
00	bf77537096e5a1f6547bcefb9aeb7c710fb0bdab2c1104204713ce7838d0d0fa	?
01	4ee0967119602f92cc662d112348597c9812308b99c5d907025100773494 4b88	?

2 output(s) for total of ? xmr

#	Stealth address	Amount	Amount Index
00	68a01aeaa9af0b5d4c8f5b685009237e727d0a799a70b5c64f4e52586f1ad687	?	50117695 of 74384866
01	b105d27544389547f4600472ad199f6257b8c3ed389c4839009c8a5fa3068b6a	?	50117696 of 74384866

Fig. 6. Basic information in a Monero transaction

Further analysis of a specific transaction shows that the stealth address from which the spending occurred is attached to 10 random blockchain addresses from the unknown with unspent outputs (Fig. 7). Today, the protocol involves joining up to 15 random blockchain addresses with unspent outputs.

2 inputs(s) for total of ? xmr

#	Key image (click row to expand)	Amount
00	bf77537096e5a1f6547bcefb9aeb7c710fb0bdab2c1104204713ce7838d0d0fa	?

Mixin	stealth address	blk	mixin	in/out	timestamp	age [y:d:h:m:s]
- 00:	1c00b32c5d3159c8625f2ec56a9ceb5b4d99428cec4dbc936b61562af3e31297	02338955	11	1/2	2021-04-14 06:45:53	02:046:07:53:45
- 01:	b655f7d7f8464593dd5b6a05dc60f7f9159f44d98de2e825cb9b65d1398cf53a	02537285	11	2/2	2022-01-14 21:54:04	01:135:16:45:34
- 02:	8917bb0c82fe5f439b685da98e11a31c25dfc15684c9c7c68463e69c1e356470	02542233	0	0/1	2022-01-21 19:12:14	01:128:19:27:24
- 03:	c6f1827fd6656f5590652c15c0a76703e9110d3ba380af28d63bedda7419776c	02581813	11	1/2	2022-03-17 21:00:25	01:073:17:39:13
- 04:	c2877eec9c5a8c04e2e37cab5e0de69665d8a6fc78a841cb23c1732e093f02b9	02582405	11	2/3	2022-03-18 16:46:37	01:072:21:53:01
- 05:	cbc2725988d95e29fe3c74b781bc74e76cc33bfbc8f13729995e0f0912f975f4	02583675	11	1/2	2022-03-20 10:29:29	01:071:04:10:09
- 06:	b0a7f86463d1f63e7d734fb312011c7618b2d4dfa28bab3a71c116627ac45c26	02583859	11	1/4	2022-03-20 16:38:55	01:070:22:00:43
- 07:	7ea9317ceb62ee2ddc08983773d839fd3552c152fbbd4aa28790a73df6669a8c	02583860	11	2/2	2022-03-20 16:42:37	01:070:21:57:01
- 08:	51deece5799b20e0c178c4fc51b27dfc245241a15a57c458bcce56992cb71268	02583914	11	2/2	2022-03-20 18:20:33	01:070:20:19:05
- 09:	78acfa585c8d1244e95894c2b583ea2e67c1e4bb95504c0841ccbbd3dd09ca5b	02583975	11	1/2	2022-03-20 19:48:28	01:070:18:51:10
- 10:	e9c88ea9df7185297eee78f51cab6a71ce723a5a51af92cbb5ec519f6330d8e2	02584018	11	2/2	2022-03-20 21:08:46	01:070:17:30:52

01	4ee0967119602f92cc662d112348597c9812308b99c5d907025100773494 4b88	?

Fig. 7. One-time transaction input address among 10 random blockchain addresses with unspent outputs

The transaction amount is encrypted and viewable only by the owner
private key view *kv* public address of the payee (Fig. 8) or vo-

the owner of the private key costs *ks* of the public address from which the funds are transferred to the recipient's public address (Fig. 9).

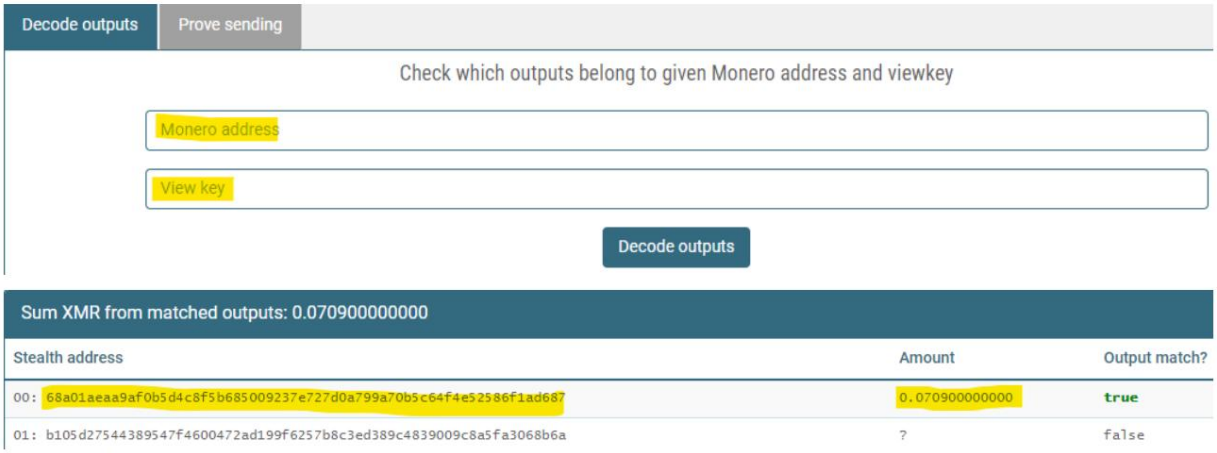

Fig. 8. Disclosure of the amount of the withdrawal to one of the one-time transaction addresses by entering the public address and the corresponding private key of viewing the public address of the recipient of the payment

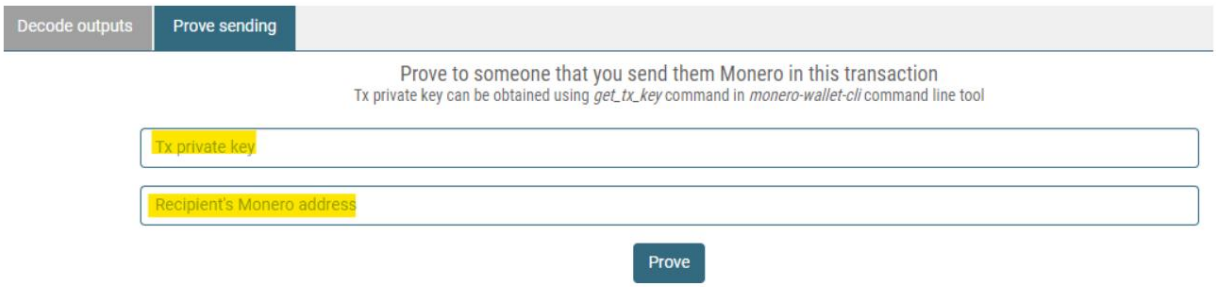

Fig. 9. The ability for the sender to receive confirmation of the transfer of funds to a specific the recipient's public Monero address

Thus, analysis of the Monero blockchain does not allow tracking the movement of funds related to illegal activity without knowing the public address and the corresponding keys. The details of a single transaction can be established if the criminal makes a transfer from his account to a legal cryptocurrency exchange (exchange service) through the appropriate request.

Features of forensic investigation of computer equipment used to work with Monero

Regarding privacy-oriented cryptocurrencies in general and Monero in particular, there are currently few scientific papers that cover methods for identifying participants in cryptocurrency transactions. Moreover, these are often methods are still at the stage of experimental research and may not always give the desired result (Biryukov, Tikho-mirov, 2019; Kumar et al., 2018; Wijaya et al.,
2018; Tramer, Boneh, Paterson, 2020). The same applies to works on forensic analysis of relevant computer technology tools, which were used to work with privacy-oriented cryptocurrencies. The work “Forensic Analysis of Privacy-Oriented Cryptocurrencies” (Koerhuis, Kechadi, Le-Khac,

2020), in which it was experimentally established that the following artifacts can be removed from the RAM of a computer:

– after creating a wallet – wallet passphrase (ASCII and UTF16 format), mnemonic keyphrase (stored only in UTF16 format);

– after opening the wallet using a passphrase – the wallet passphrase (ASCII and UTF16 format), the public address of your own wallet (ASCII format);

– after receiving a transaction from another wallet – the wallet passphrase (ASCII and UTF16 format), the public address of your own wallet, the ID of the incoming transaction with the received amount of XMR;

– after sending a transaction to another wallet – the wallet passphrase (format

ASCII and UTF16), the ID of the original transaction with the amount of XMR, the identifier of the previous transaction, the public address of the recipient, the public address of your own wallet;

– after sending a transaction with a full payment identifier – wallet passphrase (ASCII and UTF16 format), outgoing transaction ID with the XMR amount, recipient's public wallet address, own wallet public address, full payment transaction identifier, identifiers of previous transactions;

– after receiving a transaction with an integrated wallet address that contains the payment identifier within the public address, – the wallet passphrase (ASCII and UTF16 format),
Incoming transaction ID with the XMR amount, public wallet address of the previous recipient, public wallet address of your own wallet, short payment transaction ID, previous transaction IDs, full payment ID of the previous transaction;

– after executing the OpenAlias resolve action in wallet software when the Monero donation address is corrected, –
wallet passphrase (ASCII format and
UTF16), public address of your own wallet, public address of the previous recipient's wallet, short payment identifier of the previous transaction, identifiers of previous transactions, full payment identifier of the previous transaction, corrected public address with its description;

– after closing the wallet software – wallet passphrase (UTF16 format only), public address of your own wallet, all identifiers of previous transactions, full identifier of the previous transaction, short identifier of the previous transaction (belongs to the integrated address transaction).

Network traffic interception allows us to establish whether the installed Monero client is working. When analyzing the disk space in the two Monero client files of interest (monero-wallet-gui.log and

a file with the extension txt and a name containing wallet name), the public address of your own wallet, identifiers of all transactions, and the amounts of XMR received and sent were discovered.

When conducting criminal investigations, it is also of interest
identification of Monero wallets installed on the suspect's devices. The official Monero community website1 lists wallets for various devices and operating systems that are considered safe and recommended for use. Table 1 lists key artifacts that can be used to identify Monero wallets installed on the device being examined. For Android/iOS

Wallet directories and files are contained in a view-protected directory.

Table 1

Monero Wallet Artifacts1

Application name	*Main catalogs*	*Master file templates*
Monero GUI Wallet	extras, p2pool	monero-wallet-gui.exe
Monero CLI Wallet	extras	monero*, monero-wallet*, monero-gen*, monero-blockchain*
Cake Wallet	flutter_assets	cake_wallet
Monero.com	unavailable	unavailable
Feather	Monero\wallets, AppData\Roaming\FeatherWallet	feather*; wallet*, *.keys
Monero	unavailable	unavailable
MyMonero	locales, swiftshader, resources	MyMonero*,
Edge	unavailable	unavailable
ASB	wallets	seed.pem, asb.exe, sqlite, asb-wallet*
UnstoppableSwap	\AppData\Local\Programs\unstoppableswap-gui	UnstoppableSwap.exe

1 Downloads // Monero : website. URL: https://www.getmonero.org/downloads/ (access date: 01.07.2023).

Monero paper wallets, which can look like a text file or an image file, typically contain: a public address, mnemonic phrase and private keys of expenses/ view and can be presented in QR code format or hex string1 (Fig. 10).

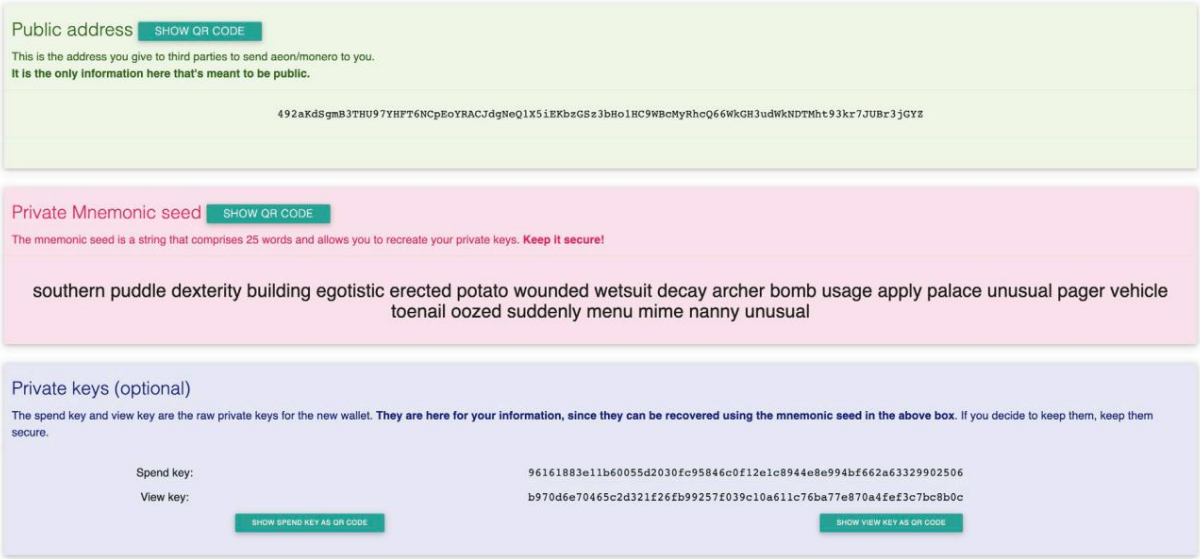

Fig. 10. Example of a Monero paper wallet

When conducting searches of persons involved in investigations where Monero is mentioned, attention should be paid to:

– all devices that may contain wallet data, such as mobile phones, tablets, computers, laptops, desktop hard drives, flash drives and other external storage media, SIM cards, etc.;

– hardware wallets Trezors and Ledgers (Fig. 11), which can be connected to the Monero GUI Wallet; – paper and

special media2 (Fig. 12) with private keys and key (seed) phrases, which are added to hardware wallets. For software wallets, the instructions usually indicate a recommendation to write down key phrases (and not take screenshots of them for cybersecurity reasons), but users often take screenshots of seed phrases;

– crypto wallet applications or browser bookmarks with links to crypto exchanges and online wallets3.

1 How to create a Monero paper wallet // Monero: site. URL: https://www.getmonero.org/resources/user-guides/securely_purchase.html (date of application: 01.07.2023).

2 Cryptosteel capsule solo // Ledger: site. URL: https://shop.ledger.com/products/cryptosteel-capsule-solo (access date: 01.07.2023).

3 Pamela C. Crypto Red Flags for Law Enforcement—How to know if your investigation involves cryptocurrency // Ciphertrace: site. 10/13/2020. URL: https://ciphertrace.com/crypto-red-flags-for-law-enforcement (access date: 07/01/2023).

Fig. 11. Hardware crypto wallets Trezor and Ledger

Fig. 12. Steel capsule for protecting the seed phrase Cryptosteel Capsule

Atomic exchange modeling (Atomic Swaps) XMR to determine the trailing pattern

Monero assets can be used to "clean" the history of the origin of other crypto assets (transition from one blockchain to another) through the use of automatic atomic exchange technology (Atomic Swaps), which does not require the disclosure of personal data of participants, trust in a third party and assumes the presence of:

– taker – has a certain crypto-tovaluta and wants to exchange it for XMR;

– maker – owns XMR and pro-intends to exchange them for a certain cryptocurrency;

– Swap Provider – provides peer-to-peer mutual discovery of takers and makers through a secure meeting point in p2p1, Tor2, Loki3 networks and can simultaneously be a maker.

In an atomic exchange, only two outcomes are possible: either the exchange is successfully completed and each participant receives the other's funds, or nothing happens and both participants keep the funds they had before the exchange. Protocol atomic swap forces both parties to follow the rules and it is impossible to take possession of the other party's coins outside of the specified
The rules therefore do not require the presence of a mediator who is trusted by both parties.

Today, Atomic Swaps is implemented for:

BTC<>XMR (unstoppableswap.net, – xmrswap.me, atomicwallet.io/xmr-to-btc-exchange, atomswap.net/btc-to-xmr, github.com/farcaster-project);

– ETH<>XMR (github.com/AthanorLabs/atomic-swap).

Atomic exchange can be performed by using a browser to connect to the exchange provider's website (Fig. 13) or through client modules that are installed on the taker's device.

Testing Atomic Swaps BTC<>XMR with the aim of studying the specifics of the procedure and the traces that are formed may look like this.

It is necessary to simulate a Service Provider Host with the function of a maker and a taker node (User Host) that are connected to public testnet servers.

Bitcoin and Monero stagenet (Fig. 14)4.

1 A modular network stack. URL: https://libp2p.io/ (access date: 01.07.2023).

2 Tor Project. URL: https://www.torproject.org/ (access date: 01.07.2023).

3 Lokinet. URL: https://lokinet.org/ (access date: 01.07.2023).

4 Automated Swap Backend (ASB) // GitHub: website. URL: https://github.com/comit-network/xmr-btc-swap/blob/master/docs/asb/README.md (last accessed: 01.07.2023).

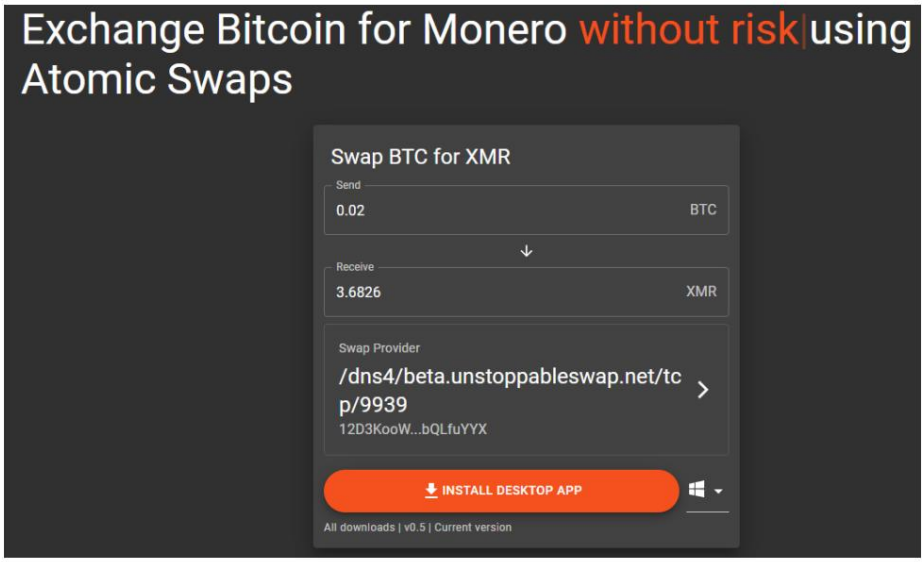

Fig. 13. Atomic online exchange via the website unstoppableswap.net

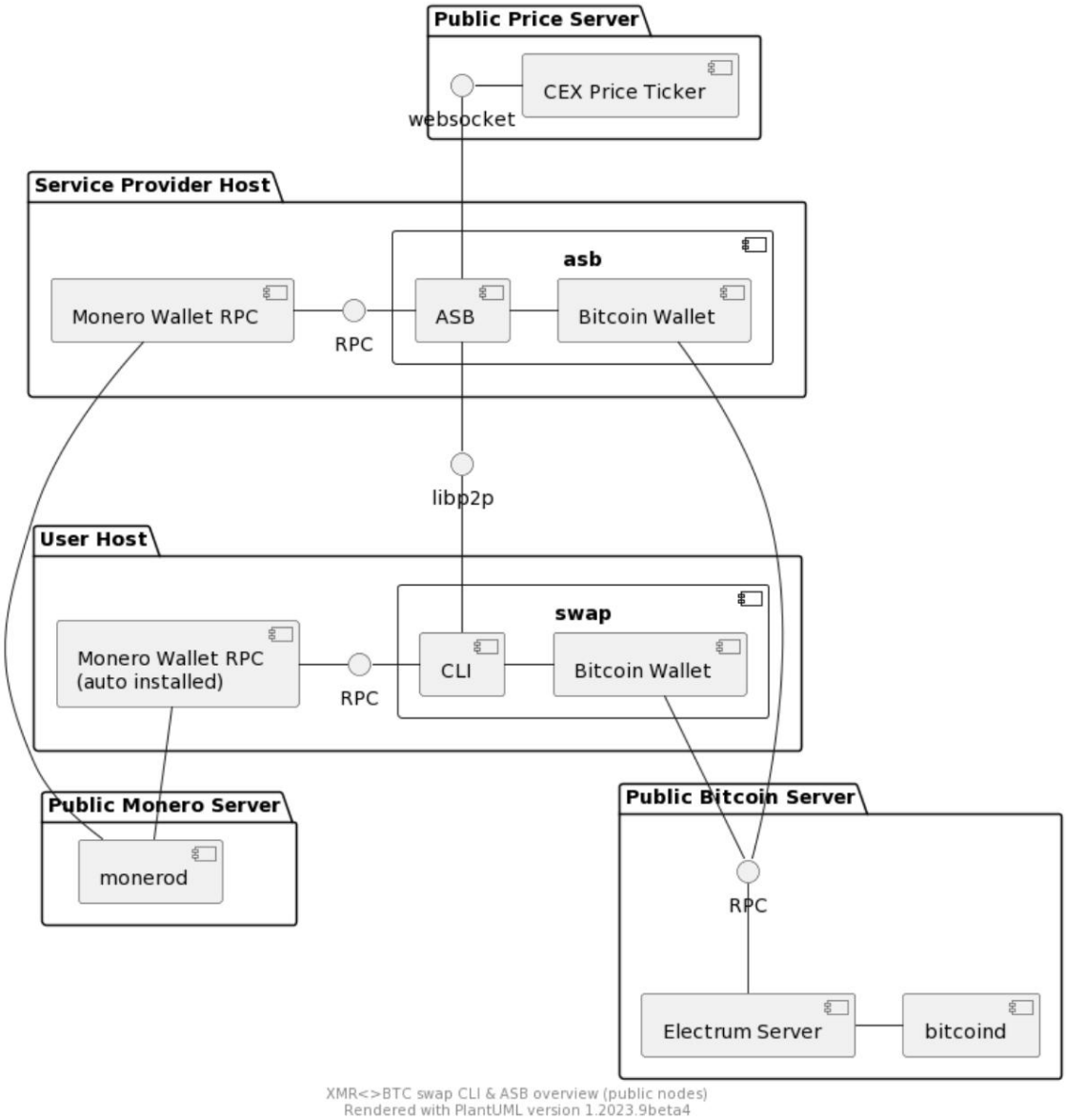

Fig. 14. Connection diagram of BTC<>XMR atomic exchange components using public Bitcoin and Monero servers

Accordingly, you need to install and configure two wallets:

– Electrum1 (BTC);

– Monero GUI (XMR).

When installing Electrum via Windows The Installer will additionally install Electrum Testnet (Fig. 15), which is already configured to connect to the BTC testnet. After installing the Monero GUI Wallet, it must be connected to the Stagenet network as described below (Fig. 15).

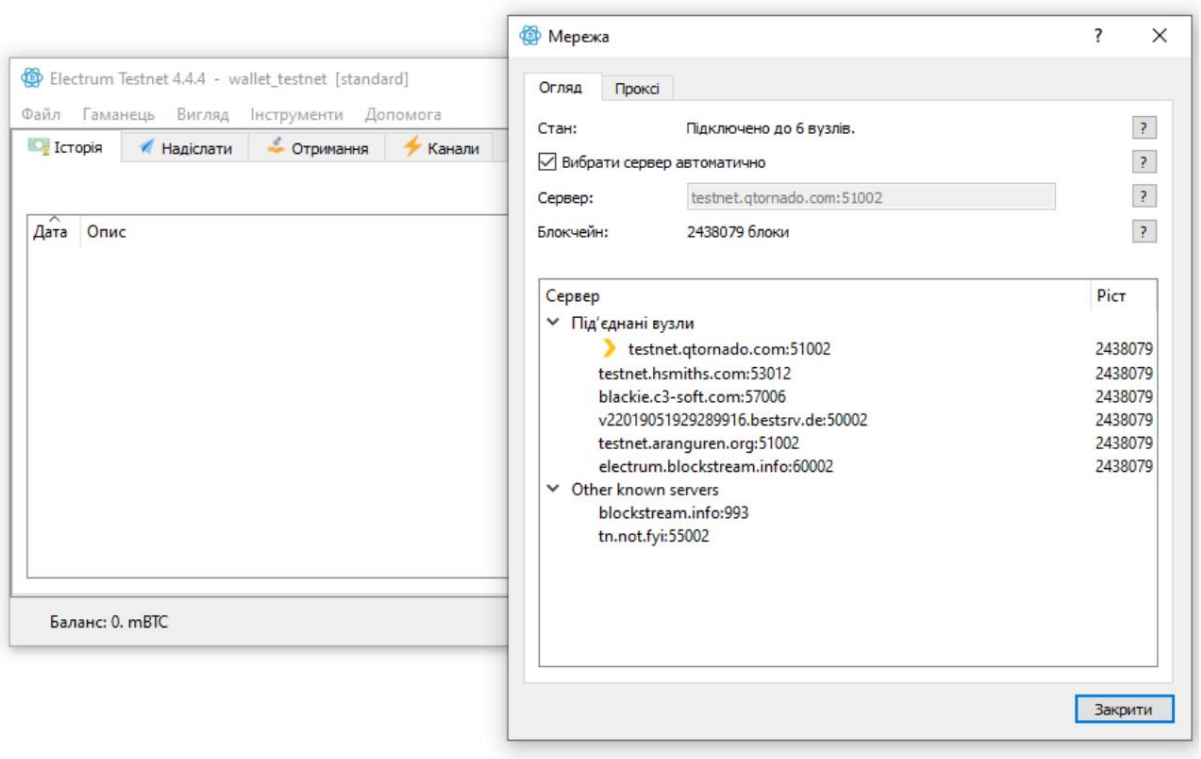

Fig. 15. Electrum Testnet Wallet

Through one of the available “faucets”, for example bitcoinfaucet.uo1.net, to the Electrum Testnet wallet address, receive test BTC (Fig. 16), via the website community.rino.io/faucet/stagenet to the Monero GUI Wallet address to receive test XMR.

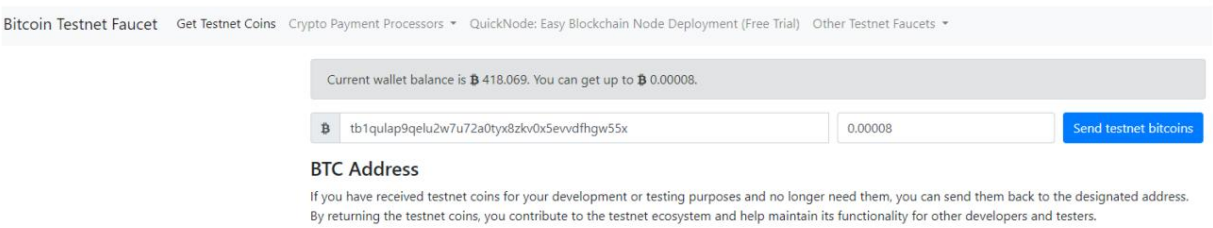

Fig. 16. Website-tap bitcoinfaucet.uo1.net for receiving test BTC

Initializing Service Provider Host services as an atomic exchange maker

Practical evaluation has shown that it is advisable to deploy the maker application on Linux OS. In a separate directory you need to have: monero-wallet-rpc2 (included in the Monero CLI Wallet archive) and asb3.

1Electrum Bitcoin Wallet. URL: https://electrum.org/#download accessed: 01.07.2023 (date).

2 Monero CLI Wallet // Monero : site. URL: https://www.getmonero.org/downloads/#cli (date application: 01.07.2023).

3 Release 0.12.1 commit-network/xmr-btc-swap // GitHub: website. URL: https://github.com/comit-network/xmr-btc-swap/releases/tag/0.12.1 (access date: 01.07.2023).

Run monero-wallet-rpc in the terminal with a connection to a public Monero node
Stagenet1 network and specifying the Bitcoin wallet directory of the exchange service (Fig. 17):

$ sudo ./monero-wallet-rpc --stagenet --daemon-host stagenet.community.rino.io:38081 --rpc-bind-port 38083 --disable-rpc-login --wallet-dir ~/Swap/SPH

```
└─$ sudo ./monero-wallet-rpc --stagenet --daemon-host stagenet.community.rino.io:38081 --rpc-bind-
port 38083 --disable-rpc-login --wallet-dir ~/Swap/SPH
This is the RPC monero wallet. It needs to connect to a monero
daemon to work correctly.

Monero 'Fluorine Fermi' (v0.18.2.2-release)
Logging to ./monero-wallet-rpc.log
2023-06-25 14:47:20.546 I Binding on 127.0.0.1 (IPv4):38083
2023-06-25 14:47:20.623 W Starting wallet RPC server
```

Fig. 17. Result of command execution

Run Automated Swap in Terminal
Backend (ASB):

>./asb --testnet start

and follow the instructions of the setup wizard (Fig. 18).

```
└─$ ./asb --testnet start
2023-06-25T15:06:39.965081896Z  INFO Initialized tracing level=debug
2023-06-25T15:06:39.965135814Z  INFO Reading config file path=/home/kali/.config/xmr-btc-swap/asb/testnet/config.toml
2023-06-25T15:06:39.965578796Z DEBUG Using existing sqlite database.
2023-06-25T15:06:39.966778644Z DEBUG Reading in seed from /home/kali/.local/share/xmr-btc-swap/asb/testnet/seed.pem
2023-06-25T15:06:39.966846996Z DEBUG Opening Monero wallet
2023-06-25T15:06:40.641466045Z DEBUG Opened Monero wallet monero_wallet_name=asb-wallet
2023-06-25T15:06:40.642078008Z  INFO Monero wallet address monero_address=58gyRFXAxUfE3vKP1CqZjC2aRrkjuEjkLjG1xvTRRuHY3gfexjtRxaYBXBD4
tfw8V2en8XNgP85ecZpdC4i4fgbvGQypjpr
2023-06-25T15:06:40.642861678Z  WARN The Monero balance is 0, make sure to deposit funds at monero_address=58gyRFXAxUfE3vKP1CqZjC2aRrk
juEjkLjG1xvTRRuHY3gfexjtRxaYBXBD4tfw8V2en8XNgP85ecZpdC4i4fgbvGQypjpr
2023-06-25T15:06:40.642885825Z DEBUG Opening Bitcoin wallet
2023-06-25T15:06:44.166333198Z  INFO Bitcoin wallet balance bitcoin_balance=0 BTC
2023-06-25T15:06:44.166969368Z  WARN Tor not found. Running on clear net
2023-06-25T15:06:44.167552292Z  INFO Network layer initialized peer_id=12D3KooWBdQGiVJuBoXXrKBExh9mCeUgwBeusWU8mnr9m55D7uTP
2023-06-25T15:06:44.168360524Z  INFO New listen address reported address=/ip4/10.0.2.8/tcp/9940/ws
2023-06-25T15:06:44.168604463Z  INFO New listen address reported address=/ip4/10.0.2.8/tcp/9939
2023-06-25T15:06:44.168633091Z  INFO New listen address reported address=/ip4/127.0.0.1/tcp/9940/ws
2023-06-25T15:06:44.168790234Z  INFO New listen address reported address=/ip4/127.0.0.1/tcp/9939
2023-06-25T15:06:45.498182044Z DEBUG Connected to Kraken websocket API
2023-06-25T15:06:45.804554207Z DEBUG Subscribed to updates for ticker
```

Fig. 18. Configuring Automated Swap Backend (ASB)

During ASB setup,1 will be created-
but:

– Monero maker wallet (asb-wallet) without a password with a new address, which is connected to monero-wallet-rpc and needs to be replenished with XMR test coins for further exchange for BTC;

– the Bitcoin wallet of the maker, connected to electrum.blockstream.info;

– identifier of a peer-to-peer maker node in a p2p network and multiaddress2
(multiaddr) its availability.

Through the faucet site community.rino.io/faucet/stagenet to the maker's wallet address (asb-wallet) to receive test XMR and verify-
to be replenished in the command line monero-wallet-rpc.

Initializing BTC<>XMR exchange from node
Download

the swap3 atomic exchange module to a separate directory *and* run it with the following parameters:

./swap buy-xmr --testnet --change-address <bitcoin-change-address> --receive-address <monero-receive-address> --seller <seller>,

where

<bitcoin-change-address> – Bitcoin address to which BTC will be returned in case of unsuccessful exchange (taken from installed Electrum
Testnet);

<monero-receive-address> – Monero address to which XMR will be transferred by the maker during the exchange (taken from the installed Monero GUI
Wallet);

1Public Monero nodes. URL: https://community.rino.io/nodes.html (access date: 01.07.2023).

2 Addressing in libp2p // GitHub: site. URL: https://github.com/libp2p/specs/blob/master/addressing/README.md accessed: 01.07.2023).

3 Release 0.12.1 commit-network/xmr-btc-swap // GitHub: website. URL: https://github.com/comit-network/xmr-btc-swap/releases/tag/0.12.1 (access date: 01.07.2023).

<seller> – the address and identifier of the maker node, which are specified in the command line of the launched ASB module (Fig. 19), for example:

/ip4/127.0.0.1/tcp/9939/p2p/12D3KooWB dQGiVJuBoXXrKBExh9mCeUgwBeusWU8mnr9m 55D7uTP.

As a result, monero-wallet-rpc will be additionally loaded, and a connection will be established. to the maker and a Bitcoin address (QR code) of the smart contract will be generated, to which it will be proposed to transfer BTC for exchange (Fig. 19).

Fig. 19. Initialization of BTC<>XMR exchange via swap module

Transfer BTC from the Electrum Testnet wallet to the generated address (Fig. 20).

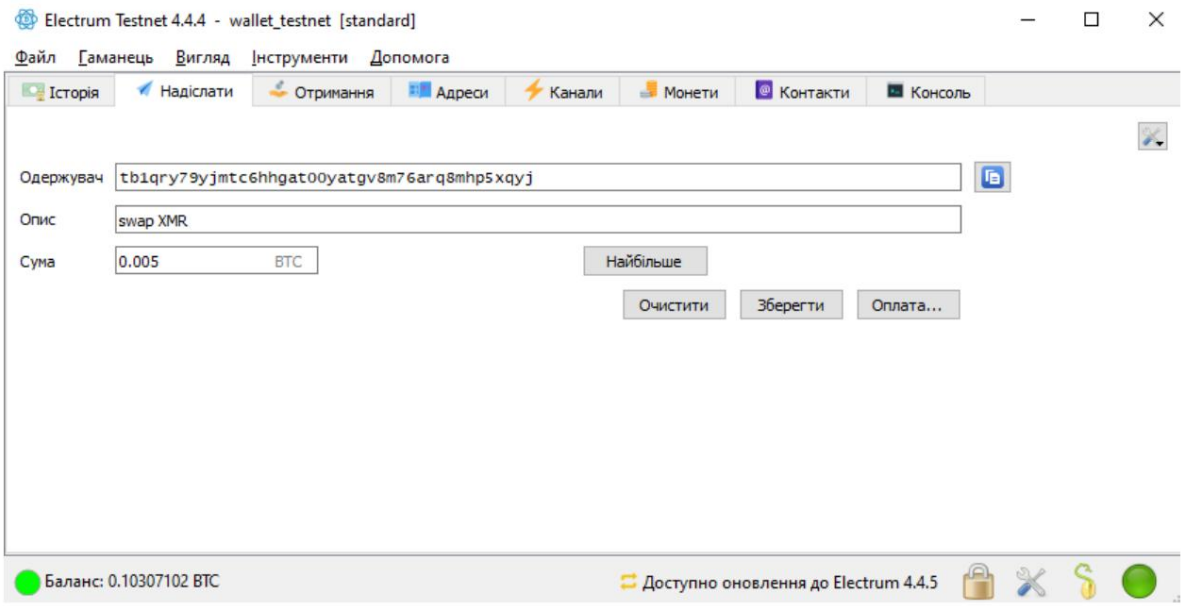

Fig. 20. Transfer BTC for exchange to XMR

Upon completion of the automatic mutual transfer procedures, the exchange will either be completed, or funds will be returned to the taker and maker in the event of interruption of individual phases of the protocol.

According to the results of the simulation, it was found that the devices of the participants in the atomic exchange will contain characteristic directories and files of the monero-wallet-rpc, swap (Table 1) and Bitcoin wallet implementations.

XMR mining simulation

Another important aspect of dealing with illegally obtained crypto assets is their seizure. Today, three separate Monero networks and blockchains have been implemented: mainnet, stagenet, and testnet. Each blockchain has its own genesis block, which is separate from the others. For law enforcement to practice the procedure for the controlled transfer of XMR during seizure

virtual assets, it is better to use the Stagenet network, which is technologically equivalent to the mainnet, rather than the Testnet, in which developers test new technologies before introducing them to the Mainnet network.

The official and most functional Monero wallet is the Monero GUI Wallet1, the process which connection to Stagenet can be modeled like this.

Download the latest official version of Monero GUI Wallet from the getmonero.org domain, for example, as an archive.

Check the integrity of the downloaded archive by calculating the hash and comparing it with the one specified on the site.

Unzip the archive and run the main wallet file monero-wallet-gui.exe, after which the setup wizard window will open, where you should select the appropriate interface language: “Advanced mode” ÿ “Additional settings” and in the drop-down list ÿ Stagenet (Fig. 21).

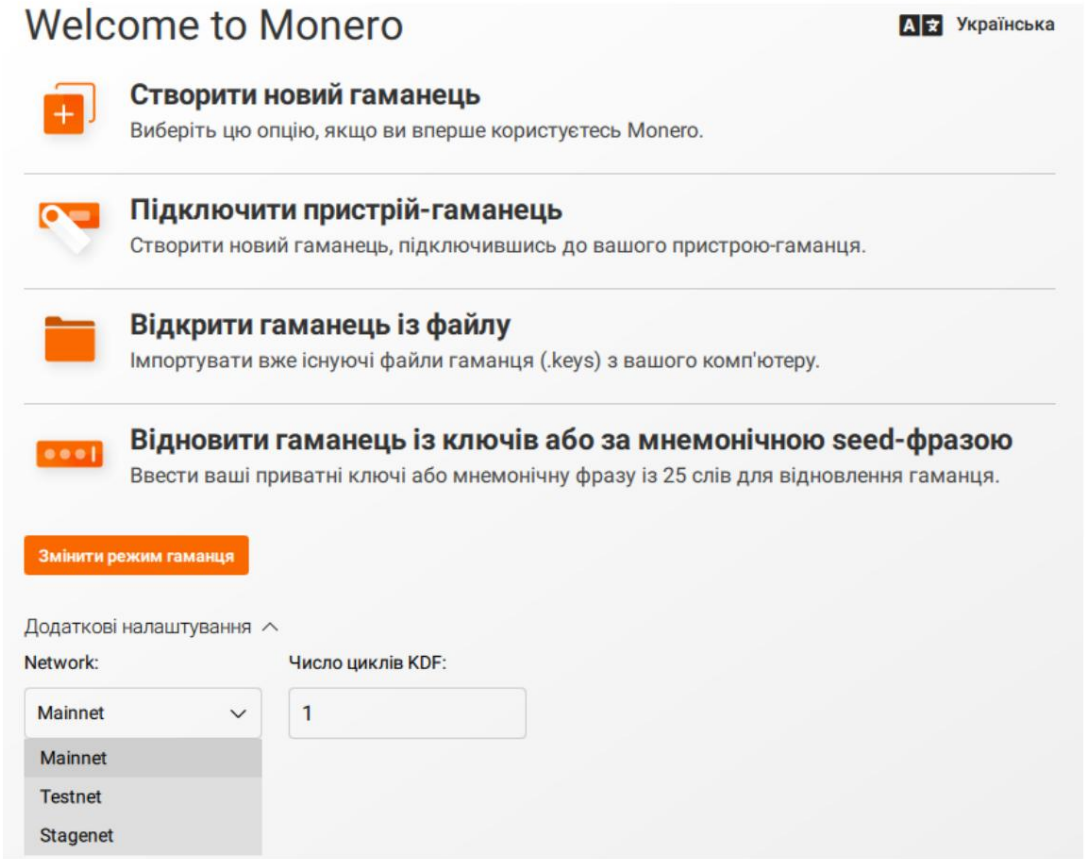

Fig. 21. Setting up a connection to the Stagenet network

Through master1 , create a new address (wallet), save a 25-word seed phrase, set a strong access password for using the wallet, in the Daemon settings (Fig. 22) select “Connect to remote node” ÿ “Add remote node”, where insert the node domain name and port, which are taken from the list of available nodes of the Stagenet network on monero.fail (Fig. 23).

1 Downloads // Monero: site. URL: (date https://www.getmonero.org/downloads/ accessed: 01.07.2023)

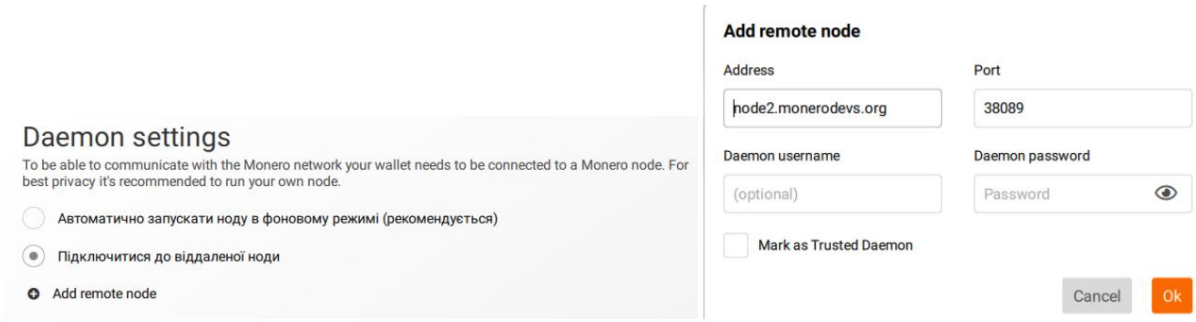

Fig. 22. Configuring access to a remote node with the Stagenet blockchain network

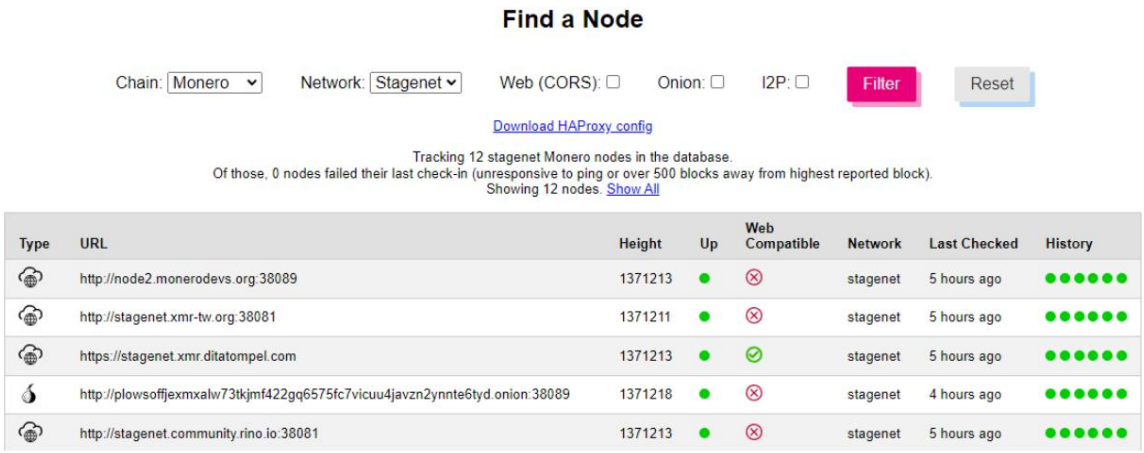

Fig. 23. List of available nodes with the Stagenet blockchain

The connection to Stagenet will be indicated by the inscription “Test network” (Fig. 24) on the start-your wallet page and an address that starts with "5".

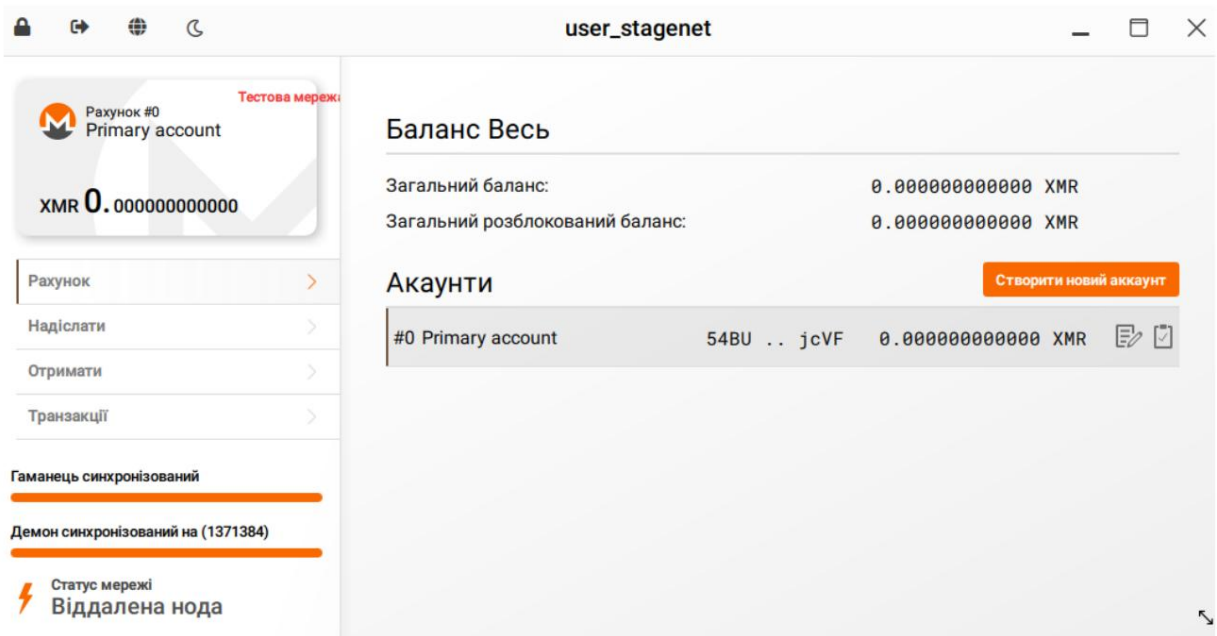

Fig. 24. Wallet connected to the Stagenet network

Via community.rino.io/faucet/ stagenet to the generated wallet address to receive test XMR (Fig. 25).

Fig. 25. Website-faucet community.rino.io/ faucet/ stagenet for obtaining test XMR

As a result, a Monero address will be created with a balance of test coins, allowing further transfer XMR from it to a special address as part of a simulated withdrawal of virtual assets.

Since there is currently no regulatory technology for withdrawing virtual assets, it is possible to propose using so-called multisig addresses as Monero addresses for storing withdrawn XMR, from which it is possible to withdraw funds only when applying digital signatures of several persons according to the m out of n rule. To create a multisig address, for example with the 2 out of 2 spending transaction signature rule, each person (let's say Person A and Person B) must first generate new separate addresses with their own keys. Working with multisig addresses is implemented only in the cmd Monero CLI Wallet command line, the files of which are located in the \extras directory of the Monero wallet GUI Wallet. First, you need to select the Stagenet node on monero.fail to which the Monero CLI Wallet will then connect, for example, stagenet.community.rino.io:380811.

Every person in dialogue mode with Monero CLI Wallet creates a wallet file:

extras\monero-wallet-cli.exe --stagenet --daemon-address stagenet.community.rino.io:38081.

In the created wallet, each person makes the remote node trusted and enables the data preparation option for the multisig address:

set_daemon stagenet.community.rino.io:38081 trusted,

set enable-multisig-experimental 1,

prepare_multisig.

After executing the prepare_multisig command, each person will receive a conditional data string <dataA> and <dataB>, which will be similar. to this:

MultisigxV2R1bFSuJcgPWh1EMiLo3DMaaEcN 9k6Y7p5BoRapCX5BD2T8PKC5Ls4MVVWG1QYwN fnY4ZTbzAD14S9FBWwU12Sr6riX7CDC62b7h3XX ZiuAHLmUJaTfCqvWjMbc4MtsSYkFkXPcBDSJd1esq PQbcgwUZS4g2xdhoNtStWu3ViFMKvdCNSyU.

These lines are exchanged between individuals and they perform further iteration with each other's received data:

Person A: make_multisig 2 <dataB>,

Person B: make_multisig 2 <dataA>.

After executing the make_multisig command, each person will receive a conditional string of data <infoA> and <infoB>, respectively, which the persons also exchange and complete the creation of a shared multisig wallet:

Person A: exchange_multisig_keys <infoB>,

Person B: exchange_multisig_keys <infoÿ>.

Each person will have a shared multisig address generated with a spending threshold of 2/2 and their own access passwords:

Multisig wallet has been successfully created. Current wallet type: 2/2,

Multisig address: 52MAkwb4q5YCK9vDNksygzGKnmnAs2ecujUuH ktip1MGMXmygKmYQgNhvRv64cfFZqaAgWQyy1 bWnK78GktnQqjJSEuNLNv.

To simulate a controlled transfer XMR on Monero GUI Wallet is required in

1 Public Monero nodes // Rino : site. URL: https://community.rino.io/nodes.html (access date: 07/01/2023).

in the "Send" section (Fig. 26) insert multisig address, specify the transfer amount and the confirm the transaction.

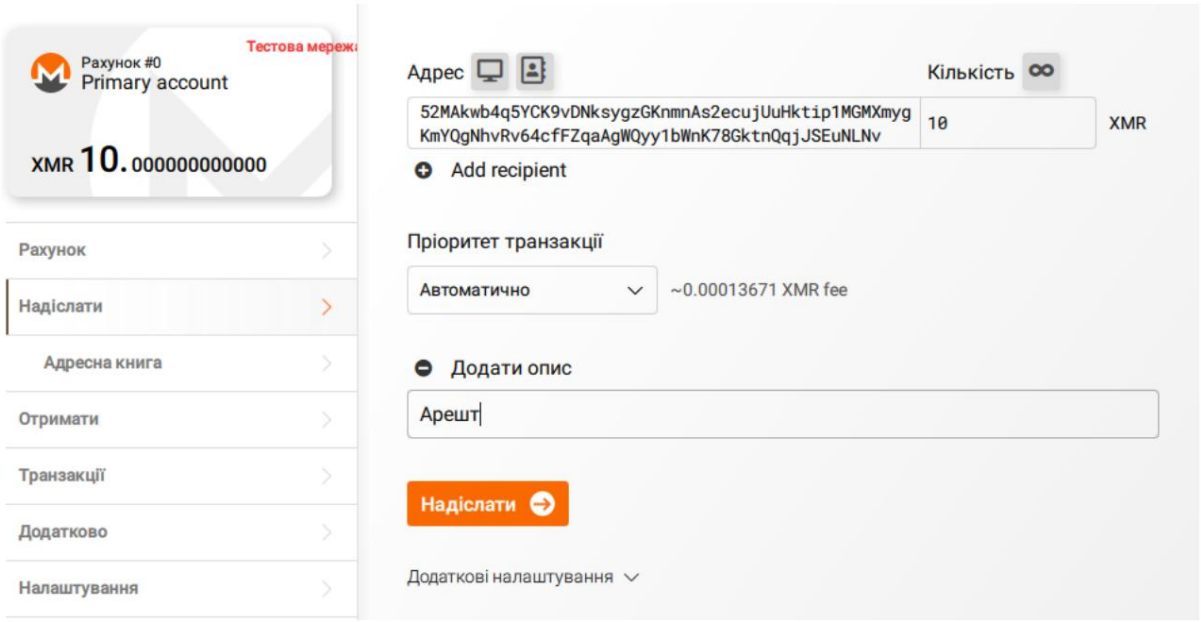

Fig. 26. Transferring XMR to a multisig address

The fact of XMR transfer will be reflected in the Monero GUI Wallet and in the Monero CLI Wallet multisig addresses via the commands: refresh, show_transfers. You can also see transaction details by its hash in the Stagenet blockchain, for example on the website community.rino.io/explorer/stagenet, by entering the address and private key to view the multisig address, which can be obtained in the Monero CLI

Wallet via the viewkey command.

Next, the general scenario for simulating a transfer from a multisig address according to the 2/2 rule consists of two stages:

– one of the multisig address owners exports a partial image of the multisig address private key from his wallet to a file and sends it to the transaction initiator, who in turn imports the file into his wallet;

– the initiator creates a transaction file, signs it and transfers it to the second owner for signature, after which the transaction with two signatures is sent to the Monero network for verification and inclusion in the blockchain. The specified stages are implemented as follows.

Export of partial images of the private key to the file imgkeyA(B):

Person A: export_multisig_info imgkeyA,
Person B: export_multisig_info imgkeyB.

Importing partial private images key:

Person A: import_multisig_info imgkeyB,
Person B: import_multisig_info imgkeyA.

Person A creates and signs the transaction file multisig_monero_tx transferring all funds to a specified address, for example like this:

[wallet 5AvBWc]: sweep_all 77yxUAG9nF43G5KWm93mk9QFiwvY9fSy3Bd9 CtzNoxPTYxVgUF7tqocAhdyJuxqqBhVN6X4Q4a2 2aiV7LSZaSu5H5Jjx8rX.

Person B, on his part, also signs the transaction file multisig_monero_tx and sends it to the Stagenet network:

[wallet 5AvBWc]: sign_multisig multisig_ monero_tx,

[wallet 5AvBWc]: submit_multisig multisig_ monero_tx.

The success of the transaction inclusion in the blockchain will be reflected in the Monero CLI wallet Wallet multisig addresses.

Performing Monero transactions on the Stagenet network showed that the main test addresses start with the number 5, and the subaddresses start with 7.

CONCLUSIONS. Cryptocurrencies are increasingly becoming a common tool for exchanging values in the field of criminal illegality, therefore, law enforcement agencies should already have the appropriate knowledge and skills to effectively document the relevant illegal activity. Given the growing interest in privately-oriented cryptocurrencies by offenders, law enforcement agencies should pay special attention to studying the technical and forensic aspects of working with the most common

currencies of this type, including Monero, Verge, Dash and Zcash.

Due to the difficulties of identifying participants in relevant transactions in such cryptocurrencies, law enforcement officers should at least understand some aspects of documenting their use. As for the Monero system, it is necessary to know the main aspects of organizing its work, to be guided by the methods of additional concealment of transactions, to understand the procedure for atomic exchange (swapping) and to be able to document traces of relevant activity. In addition, it is obvious that with the entry into force of legislation in the field of cryptocurrency circulation and the introduction of relevant amendments to the Criminal Procedure Code of Ukraine, one should be prepared for the correct organization of the seizure of relevant cryptocurrency assets.

Some aspects of the above are considered in this work. Among other things, based on the results of the conducted research, we conclude that today there is a steady trend of illegal transactions moving to privacy-oriented payment systems, in particular Monero. The advantage of this system for offenders is increased confidentiality, which is ensured by the use of ring signatures, invisible addresses, ring confidential transactions, garlic routing. Additional protection against identification may be the use of TOR networks and mixers by users. Currently, there are no stable algorithms for identifying Monero users, except for individual cases, such as using account records on crypto exchanges, analyzing transactions made before 2017, etc. Given the above, law enforcement agencies should focus on classic investigative and operational measures to identify Monero users of interest. At the same time, there are effective mechanisms for documenting traces of work with the Monero payment system and confirmed methods for extracting passphrases to crypto wallets and other sensitive information about the movement of funds in the Monero system from computer equipment. Some traces remain when using atomic exchange of one currency for another.

The article, among other things, proposes a step-by-step method for mining XMR using multisig addresses, from which withdrawals are only possible when multiple people sign the addresses. The described model has been successfully tested in the test network.

LIST OF BIBLIOGRAPHICAL REFERENCES

1. Nosov V. V., Manzhai I. A. Certain aspects of the analysis of cryptocurrency transactions during the prevention and investigation of crimes. *Law and Security.* 2021. No. 1 (80). P. 93–100. DOI: https://doi.org/10.32631/pb.2021.1.13.

2. Nosov V. V., Manzhai O. V., Panchenko E. V. Analysis of Ethereum transactions during the prevention and investigation of criminal offenses. *Law and Security.* 2022. No. 4 (87). P. 108–124. DOI: https://doi.org/10.32631/pb.2022.4.09.

3. Bahamazava K., Nanda R. The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. *Forensic Science International: Digital Investigation.* 2022. Vol. 4. DOI: https://doi.org/10.1016/j.fsidi.2022.301377.

4. Biryukov A., Tikhomirov S. Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis // 2019 IEEE European Symposium on Security and Privacy (Stockholm, Sweden, 17–19 June 2019) : Conference Proceedings. Stockholm, 2019. Pp. 172–184. DOI: https://doi.org/10.1109/eurosp.2019.00022.

5. Damgård I., Ganesh C., Khoshakhlagh H., Orlandi C., Siniscalchi L. Balancing Privacy and Accountability in Blockchain Identity Management // Topics in Cryptology – CT-RSA 2021 : Conference Proceedings (17–21 May 2021) / ed. by KG Paterson. Stockholm: Springer, 2021. Pp. 552–576. DOI: https://doi.org/10.1007/978-3-030-75539-3_23.

6. Handaya WBT, Yusoff MN, Jantan A. Machine learning approach for detection of fileless cryptocurrency mining malware. *Journal of Physics: Conference Series.* 2020. Vol. 1450. DOI: https://doi.org/10.1088/1742-6596/1450/1/012075.

7. Keller P., Florian M., Böhme R. Collaborative Deanonymization // Financial Cryptography and Data Security : FC 2021 International Workshops. Berlin, Germany : Springer, 2021. Pp. 39–46. DOI: https://doi.org/10.1007/978-3-662-63958-0_3.

8. Kethineni S., Cao Y. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review.* 2020. Vol. 30 (3). pp. 325–344. DOI: https://doi.org/10.1177/1057567719827051.

9. Koerhuis W., Kechadi T., Le-Khac N.-A. Forensic analysis of privacy-oriented cryptocurrencies. *Forensic Science International: Digital Investigation.* 2020. Vol. 33. DOI: https://doi.org/10.1016/j.fsidi.2019.200891.

10. Kumar A., Fischer C., Tople S., Saxena P. A Traceability Analysis of Monero's Blockchain // Computer Security – ESORICS 2017 : 22nd European Symposium (Oslo, Norway, September 11–15, 2017) / ed. by S. Foley, D. Gollmann, E. Snekkenes. Oslo, Norway : Springer, 2017. Pp. 153–173. DOI: https://doi.org/10.1007/978-3-319-66399-9_9.

11. Musch M., Wressnegger C., Johns M., Rieck K. Thieves in the Browser // Proceedings of the 14th International Conference on Availability, Reliability and Security (Canterbury, United Kingdom, August 26–29, 2019). New York, United States : Association For Computing Machinery, 2019. Pp. 1–10. DOI: https://doi.org/10.1145/3339252.3339261.

12. Pastrana S., Suarez-Tangil G. A First Look at the Crypto-Mining Malware Ecosystem // IMC'19: ACM Internet Measurement Conference (Amsterdam, Netherlands, October 21–23, 2019). New York, United States : Association For Computing Machinery, 2019. Pp. 73–86. DOI: https://doi.org/10.1145/3355369.3355576.

13. Peili, L., Haixia, X. Blockchain User Anonymity and Traceability Technology. *Journal of Electronics & Information Technology.* 2020. No. 42 (5). pp. 1061–1067. DOI: https://doi.org/10.11999/JEIT190813.

14. Russo M., Šrndiÿ N, Laskov P. Detection of illicit cryptomining using network metadata. *EURASIP Journal on Information Security.* 2021. No. 11. DOI: https://doi.org/10.1186/s13635-021-00126-1.

15. Rüth J., Zimmermann T., Wolsing K., Hohlfeld O. Digging into Browser-based Crypto Mining // IMC'18: Internet Measurement Conference (Boston, United States, 31 October – 2 November 2018). New York, United States : Association For Computing Machinery, 2018. Pp. 70–76. DOI: https://doi.org/10.1145/3278532.3278539.

16. Sampson J. Secret digital coin mining and trading is a threat to your business. *Computer Fraud & Security.* 2018. Vol. 4. pp. 8-10. DOI: https://doi.org/10.1016/s1361-3723(18)30032-0.

17. Tramer F., Boneh D., Paterson KG Remote Side-Channel Attacks on Anonymous Transactions // SEC'20: 29th USENIX Conference of Security Symposium (12–14 August 2020). Berkeley, United States, 2020. Pp. 2739–2756. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/tramer.

18. Wijaya DA, Liu J., Steinfeld R., Liu D. Monero Ring Attack: Recreating Zero Mixin Transaction Effect // 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference on Big Data Science and Engineering (New York, United States, August 1–3, 2018). New York, United States, 2018. Pp. 1196–1201. DOI: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00165.

19. Zhang Y., Xu H. Accountable Monero System with Privacy Protection. *Security and Communication Network.* 2022. Vol. 22. DOI: https://doi.org/10.1155/2022/7746341.

20. Zimba A., Wang Z., Mulenga M., Odongo NH Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. *Journal of Computer Information Systems.* 2018. No. 60 (4). DOI: https://doi.org/10.1080/08874417.2018.147.

Received by the editorial office: 04.07.2023

Accepted for publication: 10.08.2023

REFERENCES

1. Bahamazava, K., & Nanda, R. (2022). The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence, *Forensic Science International: Digital Investigation,* 4. https://doi.org/doi:10.1016/j.fsidi.2022.301377.

2. Biryukov, A., & Tikhomirov, S. (2019, June 17–19). *Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis* [Conference presentation abstract]. Conference Proceedings "2019 IEEE European Symposium on Security and Privacy", Stockholm, Sweden. https://doi.org/10.1109/eurosp.2019.00022.

3. Damgård, I., Ganesh, C., Khoshakhlagh, H., Orlandi, C., & Siniscalchi, L. (2021, May 17–21). *Balancing Privacy and Accountability in Blockchain Identity Management* [Conference presentation abstract]. Conference Proceedings "Topics in Cryptology - CT-RSA 2021". Stockholm, Sweden. https://doi.org/10.1007/978-3-030-75539-3_23.

4. Handaya, WBT, Yusoff, MN, & Jantan, A. (2020). Machine learning approach for detection of fileless cryptocurrency mining malware. *Journal of Physics: Conference Series, 1450.* https://doi.org/10.1088/1742-6596/1450/1/012075.

5. Keller, P., Florian, M., & Böhme, R. (2021). *Collaborative Deanonymization* [Conference presentation abstract]. Financial Cryptography and Data Security : FC 2021 International Workshops, Berlin, Germany. https://doi.org/10.1007/978-3-662-63958-0_3.

6. Kethineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review,* 30(3), 325–344. https://doi.org/10.1177/1057567719827051.

7. Koerhuis, W., Kechadi, T., & Le-Khac, N.-A. (2020). Forensic analysis of privacy-oriented cryptocurrencies. *Forensic Science International: Digital Investigation, 33.* https://doi.org/10.1016/j.fsidi.2019.200891.

8. Kumar, A., Fischer, C., Tople, S., & Saxena, P. A (2017, September 11–15). *Traceability Analysis of Monero's Blockchain* [Conference presentation abstract]. 22nd European Symposium "Computer Security - ESORICS 2017", Oslo, Norway. DOI: https://doi.org/10.1007/978-3-319-66399-9_9.

9. Musch, M., Wressnegger, C., Johns, M., & Rieck, K. (2019, August 26–29). *Thieves in the Browser* [Conference presentation abstract]. Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, United Kingdom. https://doi.org/10.1145/3339252.3339261.

10. Nosov, VV & Manzhai, IA (2021). Certain Aspects of the Analysis of Cryptocurrency Transactions during the Prevention and Investigation of Crimes. *Law and Safety,* 1(80), 93–100. https://doi.org/10.32631/pb.2021.1.13.

11. Nosov, VV, Manzhai, OV & Panchenko, Ye. V. (2022). Analysis of Ethereum transactions during the prevention and investigation of criminal offenses. *Law and Safety,* 4(87), 108–124. https://doi.org/10.32631/pb.2022.4.09.

12. Pastrana, S., & Suarez-Tangil, G. (2019, October 21–23). *A First Look at the Crypto-Mining Malware Ecosystem* [Conference presentation abstract]. IMC'19: ACM Internet Measurement Conference, Amsterdam, Netherlands. https://doi.org/10.1145/3355369.3355576.

13. Peili, L., & Haixia, X. (2020). Blockchain User Anonymity and Traceability Technology. *Journal of Electronics & Information Technology,* 42(5), 1061–1067. https://doi.org/10.11999/JEIT190813.

14. Russo, M., Šrndiÿ, N., & Laskov, P. (2021). Detection of illicit cryptomining using network metadata. *EURASIP Journal on Information Security, 11.* https://doi.org/10.1186/s13635-021-00126-1.

15. Rüth, J., Zimmermann, T., Wolsing, K., & Hohlfeld, O. (2018). *Digging into Browser-based Crypto Mining* [Conference presentation abstract]. IMC'18: Internet Measurement Conference, Boston, United States. https://doi.org/10.1145/3278532.3278539.

16. Sampson, J. (2018). Secret digital coin mining and trading is a threat to your business. *Computer Fraud & Security,* 4, 8–10. https://doi.org/10.1016/s1361-3723(18)30032-0.

17. Tramer, F., Boneh, D., & Paterson, KG (2020, August 12–14). *Remote Side-Channel Attacks on Anonymous Transactions* [Conference presentation abstract]. SEC'20: 29th USENIX Conference of Security Symposium, United States. https://www.usenix.org/conference/usenixsecurity20/presentation/tramer.

18. Wijaya, DA, Liu, J., Steinfeld, R., & Liu, D. (2018, August 1–3). *Monero Ring Attack: Recreating Zero Mixin Transaction Effect* [Conference presentation abstract]. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference on Big Data Science and Engineering, New York, United States. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00165.

19. Zhang, Y. & Xu, H. (2022). Accountable Monero System with Privacy Protection. *Security and Communication Networks, 22.* https://doi.org/10.1155/2022/7746341.

20. Zimba, A., Wang, Z., Mulenga, M., & Odongo, NH (2018). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. *Journal of Computer Information Systems,* 60(4). https://doi.org/10.1080/08874417.2018.147.

Received the editorial office: July 4, 2023

Accepted for publication: 10 August 2023

VITALIA VICTOROVYCH NOSOV,
Candidate of Technical Sciences, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Cybercrime Combating;
ORCID: https:// orcid.org/ 0000-0002-7848-6448,
email: vitnos.g@gmail.com;

OLEKSANDR VOLODYMYROVYCH MANZHAI,
Candidate of Law, Professor,
Kharkiv National University of Internal Affairs,
Department of Cybercrime Combating;
ORCID: https:// orcid.org/ 0000-0001-5435-5921,
e-mail: sofist@ukr.net;

VIKTORIIA OLEKSANDRIVNA KOVTUN,
Cyberpolice Department of the National Police of Ukraine,
2nd Unit (Analysis of Open Sources) of the 4th Department (Operational and Analytical Support and Analysis of Open Sources);
ORCID: https:// orcid.org/ 0000-0003-1263-5970,
email: cybercop322@gmail.com

TECHNICAL, FORENSIC AND ORGANIZATIONAL ASPECTS OF WORK WITH MONERO CRYPTOCURRENCY

The forensic, organizational and technical features of law enforcement agencies' work with the Monero cryptocurrency in the context of pre-trial investigation and operational search activities are analyzed. The development of the Monero system is described. The reasons and trends of Monero use by offenders are identified, and the scheme of operation of this payment system, which ensures its increased confidentiality, is shown. Examples of criminal offenses in which Monero is used are presented. The functionality of OpenAlias to facilitate the work with Monero addresses is disclosed. The possibility of identifying participants in Monero transactions is studied. It is stated that there are currently no effective ways of such identification without knowledge of the public address and the corresponding keys, especially if users use additional security mechanisms such as connection to the TOR network.

The features of forensic investigation of computer equipment used to work with Monero are revealed. It is established that the most effective is the study of traces of work with Monero, which are removed from the relevant computer equipment of the person of interest. Useful information can be stored in RAM, on a disc, and partially in network traffic. The article identifies artifacts that should be taken into account during inspection and search. Atomic Swaps of XMR are modeled to determine the trace pattern and identify artifacts of increased attention during forensic procedures. The fact that an atomic swap was carried out to obfuscate traces may be evidenced by the presence of specific software files on the disc used for this purpose.

The algorithm for XMR withdrawal using multisig addresses has been proposed, from which funds can be withdrawn only when digital signatures of several persons are superimposed. The work of this algorithm in the Stagenet test network is modeled. It has been concluded that law enforcement agencies should focus on classical investigative measures to identify Monero users of interest. At the same time, there are effective mechanisms for documenting traces of work with the Monero payment system and proven methods for extracting passphrases to crypto-wallets and other sensitive information on the movement of funds in the Monero system from computer equipment.

Key words: *cryptocurrency, Monero, law enforcement agencies, crime prevention, trace evidence.*

Citation (DSTU 8302:2015): Nosov V. V., Manzhai O. V., Kovtun V. O. Technical, forensic and organizational aspects of working with the Monero cryptocurrency. *Law and Security.* 2023. No. 3 (90). P. 102–125. DOI: https://doi.org/10.32631/pb.2023.3.9.

Citation (APA): Nosov, VV, Manzhai, OV, & Kovtun, VO (2023). Technical, forensic and organizational aspects of work with Monero cryptocurrency. *Law and Safety,* 3(90), 102–125. https://doi.org/10.32631/pb.2023.3.9.