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

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-7848-6448,
e-mail: vitnos.g@gmail.com;

ОЛЕКСАНДР ВОЛОДИМИРОВИЧ МАНЖАЙ,
кандидат юридичних наук, професор,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0001-5435-5921,
e-mail: sofist@ukr.net;

ВІКТОРІЯ ОЛЕКСАНДРІВНА КОВТУН,
Департамент кіберполіції Національної поліції України,
2-ий відділ (аналізу відкритих джерел)
4-го управління (оперативно-аналітичного
забезпечення та аналізу відкритих джерел);
https://orcid.org/0000-0003-1263-5970,
e-mail: cybercop322@gmail.com

ТЕХНІКО-КРИМІНАЛІСТИЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ РОБОТИ З КРИПТОВАЛЮТОЮ MONERO

Проаналізовано криміналістичні, організаційні і технічні особливості роботи правоохоронних органів із криптовалютою Monero в контексті проведення досудового слідства й оперативно-розшукової діяльності. Описано розвиток системи Monero. Окреслено причини і тенденції використання Monero правопорушниками, а також показано схему роботи цієї платіжної системи, яка забезпечує її підвищену конфіденційність. Наведено приклади кримінальних правопорушень, під час яких здійснюється використання Monero. Розкрито функціонал OpenAlias для полегшення роботи з адресами Monero. Вивчено можливість ідентифікації учасників трансакцій Monero. Констатовано відсутність на сьогодні дієвих способів такої ідентифікації без знання публічної адреси та відповідних ключів, особливо якщо користувачі використовують додаткові захисні механізми типу підключення до TOR-мережі.

Розкрито особливості криміналістичного дослідження засобів комп'ютерної техніки, які використовувалися для роботи з Monero. Встановлено, що найбільш результативним є вивчення слідів роботи з Monero, що вилучаються з відповідних засобів комп'ютерної техніки особи, яка становить інтерес. Корисна інформація може зберігатися в оперативній пам'яті, на диску, частково у мережному трафіку. Визначено артефакти, на які слід звертати увагу під час проведення огляду та обшуку. Змодельовано атомарний обмін (Atomic Swaps) XMR для визначення слідової картини та визначення артефактів підвищеної уваги під час здійснення криміналістичних процедур. Про факт здійснення атомарного обміну для заплутування слідів може свідчити наявність на диску специфічних файлів програмного забезпечення, яке використовувалося із цією метою.

Запропоновано алгоритм вилучення XMR за допомогою multisig-адрес, з яких виводити кошти можливо тільки при накладанні цифрових підписів декількох осіб. Змодельовано роботу цього алгоритму в тестовій мережі Stagenet. Зроблено висновок, що правоохоронним органам для ідентифікації користувачів Monero, які становлять інтерес, слід зосередитися на класичних слідчо-оперативних заходах розслідування. Водночас існують дієві механізми документування слідів роботи із платіжної системою Monero та підтверджені методики вилучення із засобів комп'ютерної техніки парольних фраз до криптогаманців та іншої чутливої інформації щодо руху коштів у системі Monero.

Ключові слова: *криптовалюта, Monero, правоохоронні органи, протидія злочинності, фіксація слідів.*

Оригінальна стаття

ВСТУП. Поява технологій, заснованих на блокчейні, відкрила нові можливості для осіб, які бажають проводити фінансові та інші трансакції дистанційно, анонімно та без допомоги третьої сторони, наприклад банку. На початковому етапі криптовалютні операції здебільшого були орієнтовані на роботу з Bitcoin чи Ethereum. Проте згодом ситуація змінилася і сьогодні вже можна побачити десятки й сотні нових проєктів щодо створення та підтримки криптовалютних активів.

Інтерес до криптовалютного ринку і технології часто виявляють не лише добропорядні користувачі, а й правопорушники. Віртуальні активи все частіше стають прийнятною формою оплати для забезпечення багатьох незаконних дій переважно через здатність окремих криптовалют виконувати анонімні трансакції дистанційно. Дж. Семпсон (2018) також звертає увагу, що робота із цифровими монетами може бути руйнівною та небезпечною через природу програмного забезпечення, яке використовується для цього. Користувачі криптовалют, які прагнуть конфіденційності, покладаються на методи анонімізації, такі як CoinJoin та кільцеві трансакції. Використовуючи такі технології, добропорядні користувачі потенційно забезпечують анонімність зловмисникам (Keller, Florian, Böhme, 2021).

Нині криптовалютні активи найчастіше використовують для отримання неправомірної вигоди, оплати наркоугод, у схемах, пов'язаних із торгівлею людьми, замовними вбивствами, вимаганням, шахрайством, відмиванням коштів. Наприклад, під час дослідження вмісту наркомайданчика Legalizer на початку 2022 року було встановлено, що найбільша кількість онлайн-наркомагазинів з можливістю оплати криптовалютою зосереджена в містах Харків, Київ, Одеса, Дніпро, Львів, Миколаїв, Запоріжжя.

Слід зауважити, що раніше основними валютами у злочинних схемах були Bitcoin чи Ethereum. Проте технологія їх роботи не повною мірою дозволяє зберегти анонімність. Щоб подолати цю проблему, було розроблено кілька нових криптовалют, які гарантують конфіденційність трансакцій та анонімність для своїх користувачів (зокрема ZCash, Monero тощо) (Damgård et al., 2021).

Із точки зору захисту приватності ключовою інновацією Monero є використання протоколу кільцевих конфіденційних трансакцій (RingCT) для приховування адреси відправника та суми трансакції, а також використання стелс-адреси для приховування адреси одержувача. Monero став засобом обміну на чорному ринку. Три з п'яти найбільших чорних ринків приймають Monero як платіжний засіб. Кіберзлочинці зрозуміли, що використання біткоїна дозволяє розкрити їхню особу через блокчейн-трансакції, тому вони все частіше вимагають викуп у монетах Monero (Zhang, Xu, 2022). Так, наприклад, у загальносвітовому контексті в наркоугодах використовували біткоїн, незважаючи на те, що його можна було відстежити, поки Monero стало неможливо відстежити у 2017 році через оновлення його конфіденційності (Bahamazava, Nanda, 2022).

Враховуючи викладене, для правоохоронних органів вкрай важливо опанувати методику ідентифікації учасників угод з Monero, правильного криміналістичного дослідження засобів комп'ютерної техніки, які використовувалися для трансакцій з Monero, а також вилучення відповідних криптоактивів.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. У попередніх роботах нами вже було опрацьовано деякі питання роботи правоохоронних органів з Bitcoin (Носов, Манжай, 2021) та Ethereum (Носов, Манжай, Панченко, 2022). *Мета* цієї статті – аналіз певних техніко-криміналістичних аспектів роботи зі слідами, пов'язаними з Monero, а також демонстрація моделі вилучення відповідних криптоактивів.

Для досягнення поставленої мети потрібно виконати такі *завдання*:

– дослідити питання щодо використання Monero в незаконних цілях;

– окреслити особливості криптовалюти Monero;

– описати деякі аспекти криміналістичного дослідження засобів комп'ютерної техніки, які використовувалися для роботи з Monero;

– провести моделювання атомарного обміну (Atomic Swaps) XMR для визначення слідової картини;

– продемонструвати модель вилучення XMR.

Наведене дослідження є однією з перших спроб вивчення системи Monero в контексті роботи правоохоронних органів в Україні.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. У статті застосовано низку кількісних та якісних методів, які в сукупності дозволяють комплексно вивчити відповідний об'єкт. Історичний і статистичний методи застосовувалися під час аналізу використання Monero в незаконних цілях в Україні та світі. З метою вивчення структурної організації Monero-технології

застосовувався метод системного аналізу. Метод моделювання був використаний для відпрацювання маніпуляцій із тестовою криптовалютною мережею, навичок потенційного вилучення відповідних віртуальних активів, а також для визначення слідової картини, яка утворюється за результатами атомарного обміну (Atomic Swaps) XMR.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. На момент дослідження криптовалюта Monero (XMR) перебуває на 33 місці за ринковою капіталізацією, яка є добутком ціни XMR-монети на загальну кількість монет в обігу (18,15 млн)[1] і становить 2 796 919 510 дол. США. Відповідно до звіту Chainalysis[2] про криптозлочинність за 2022 рік кількість ринків у даркнеті, які підтримують Monero, зросла у 2021 році з 45 до 67 %, а деякі ринки підтримують виключно Monero, наприклад Archetyp (рис. 1) та оновлений Alphabay (рис. 2).

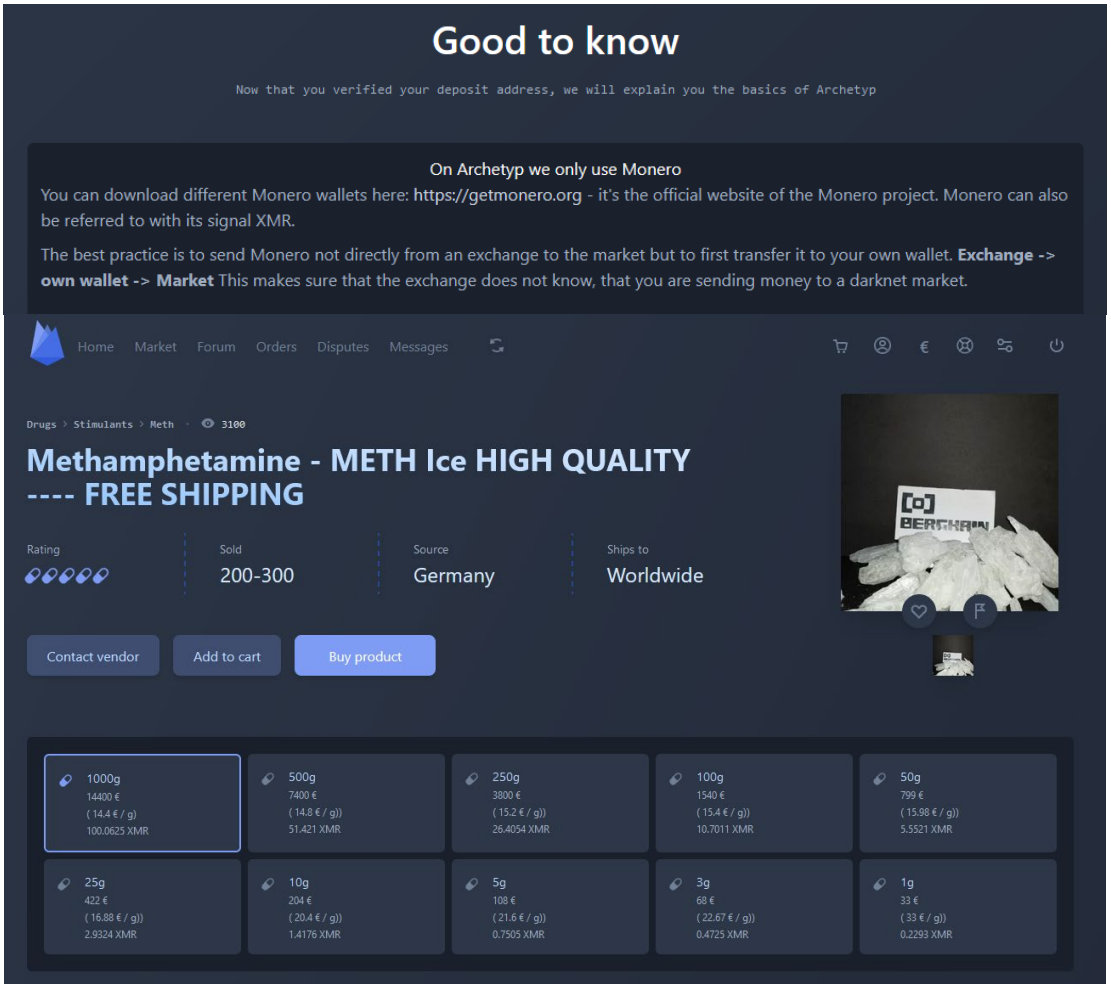

Рис. 1. Ринок Archetyp в даркнеті з оплатою виключно в Monero (XMR)

[1] Monero Price: XMR Live Price Chart // CoinGecko : сайт. URL: https://www.coingecko.com/en/coins/monero (дата звернення: 01.07.2023).

[2] The 2022 Crypto Crime Report // Chainalysis : сайт. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf (дата звернення: 01.07.2023).

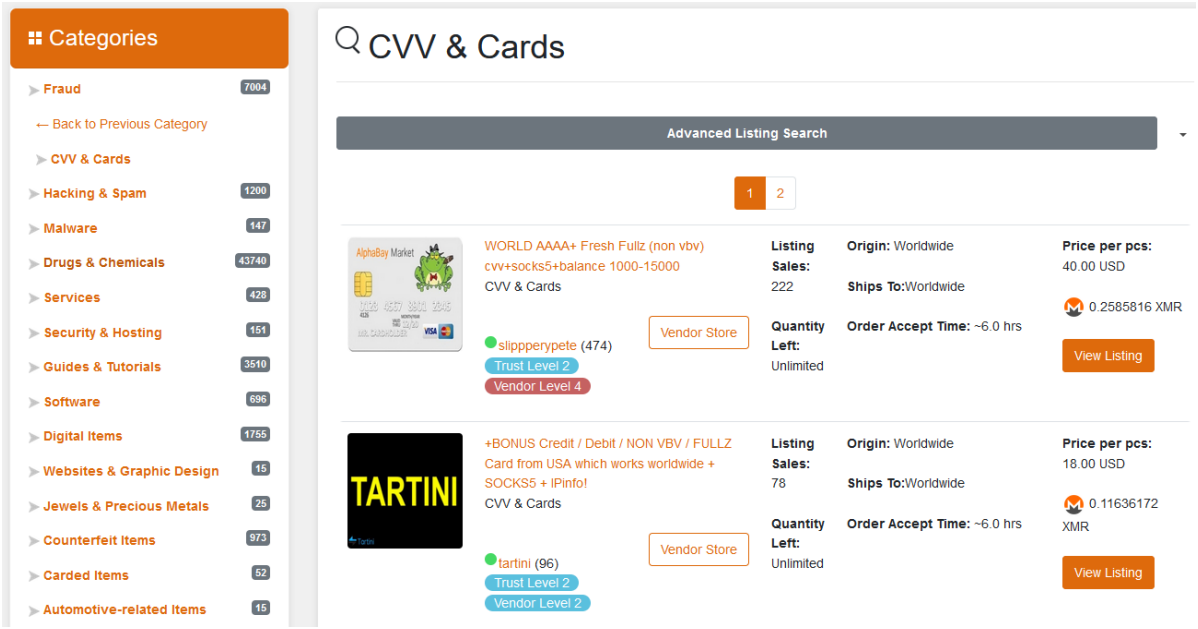

Рис. 2. Ринок Alphabay в даркнеті з оплатою виключно в Monero (XMR)

У звіті Chainalysis про криптозлочинність за 2023 рік[1] трансакції з криптовалютами, що пов'язані з незаконною діяльністю, оцінюються у 20,6 млрд дол. США. Важливо зауважити, що більшість кіберзлочинів залишаються латентними. Так, наприклад, за даними Міністерства юстиції США, лише про кожен сьомий (або 15 % від загальної кількості) випадок кіберзлочину повідомляється у правоохоронні органи[2]. За консервативною оцінкою справжній обсяг незаконних криптовалютних трансакцій, без урахування трансакцій, пов'язаних із відмиванням грошей, становить щонайменше 144,2 млрд дол. США[3].

Monero (XMR) як один із різновидів криптовалюти користується популярністю у злочинців, оскільки є анонімною і не відстежується. Monero базується на алгоритмі доказу роботи ґешу CryptoNight, який походить від протоколу CryptoNote. Протокол CryptoNote має значні алгоритмічні відмінності щодо обфускації Blockchain. Одноразові кільцеві підписи анонімізують адресу відправника трансакції. Крім того, процес майнінгу Monero не залежить від спеціалізованих архітектур, таких як GPU (Handaya, Yusoff, Jantan, 2020).

Нерідко Monero використовують для оплати розшифрування даних (рис. 3) після ураження комп'ютерної системи шкідливою програмою-вимагачем (ransomware)[4].

[1] The 2023 Crypto Crime Report // Chainalysis : сайт. URL: https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf (дата звернення: 01.07.2023).

[2] Martin B. The Unseen Problem of Unreported Cybercrime // Anapaya : сайт. 09.12.2023. URL: https://www.anapaya.net/blog/the-unseen-problem-of-unreported-cybercrime (дата звернення: 01.07.2023).

[3] Crypto Money Laundering: How Criminals Cash Out Billions in Bitcoin and Other Cryptocurrencies // Chainalysis : сайт. 15.01.2020. URL: https://blog.chainalysis.com/reports/crypto-laundering (дата звернення: 01.07.2023).

[4] Young M. Monero's crypto of choice as ransomware 'double extortion' attacks increase 500 % // Cointelegraph : сайт. 20.04.2020. URL: https://cointelegraph.com/news/monero-crypto-of-choice-as-ransomware-double-extortion-attacks-increase-500 (дата звернення: 01.07.2023).

Рис. 3. Вимагання викупу Monero (XMR) за розшифрування файлів

Російські кампанії зі збору коштів для підтримки агресії проти України пропонують Monero як варіант переказу (рис. 4).

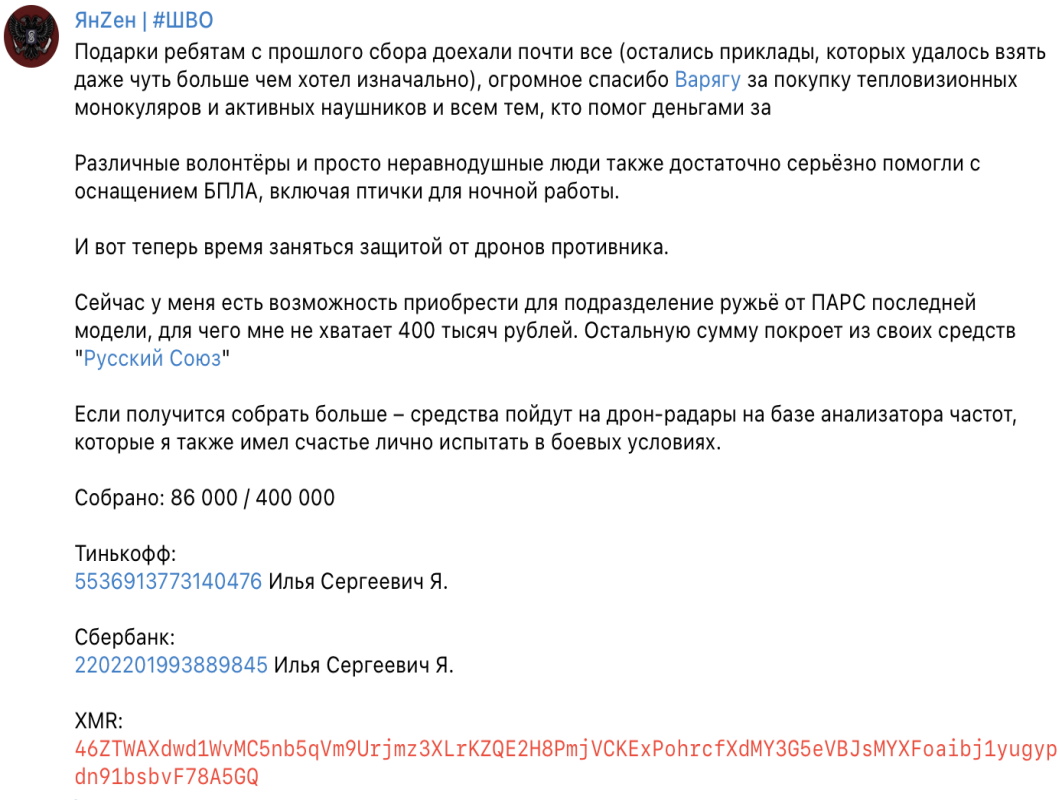

Рис. 4. Приклад використання Monero для збору коштів на потреби російської армії

У 2019 році була опублікована робота «Перший погляд на екосистему шкідливого програмного забезпечення для криптомайнінгу» (Pastrana, Suarez-Tangil, 2019), в якій автори з різноманітних джерел спробували проаналізувати відповідну протиправну схему майнінгу криптовалют за допомогою шкідливого програмного забезпечення. За їх підрахунками з відкритих джерел найбільша кількість кампаній, що реалізовувалися з використанням шкідливого програмного забезпечення для майнінгу, була орієнтована на використання адрес гаманців Monero (2 449). Те саме підтверджується і в інших роботах науковців (Zimba et al., 2018; Russo, Šrndić, Laskov, 2021; Musch et al., 2019). Браузерний майнінг на боці клієнта зараз також розглядається як альтернатива монетизації послуг за допомогою реклами і він доволі широко представлений саме в контексті використання Monero (Rüth et al., 2018).

Що стосується юридичного аспекту документування кримінальної активності з використанням Monero, то у своїй роботі С. Кетінені та І. Цао (2020) проаналізували 124 кримінальні провадження з КНР, Південної Кореї та Японії. За результатами аналізу було встановлено, що принаймні у двох випадках Monero використовувалася у кримінальній активності міжнародного рівня.

Особливості роботи платіжної системи Monero

Основними відмінностями платіжної системи Monero від Bitcoin або Ethereum є підвищений рівень конфіденційності (анонімності) трансакцій і користувачів. Для цього застосовують (рис. 5):

– кільцеві підписи (ring signatures), які приховують адресу, з якої витрачаються кошти, серед групи інших обраних адрес;

– невидимі адреси (stealth addresses), які є випадковими одноразовими адресами для кожної трансакції і до яких отримує доступ одержувач коштів через ключі від основної адреси;

– кільцеві конфіденційні трансакції (ring confidential transactions, RingCT), які приховують суму переказу;

– часникова маршрутизація (garlic routing) Kovri, яка приховує IP-адреси хостів користувачів платіжної системи Monero (поки не впроваджена за умовчанням).

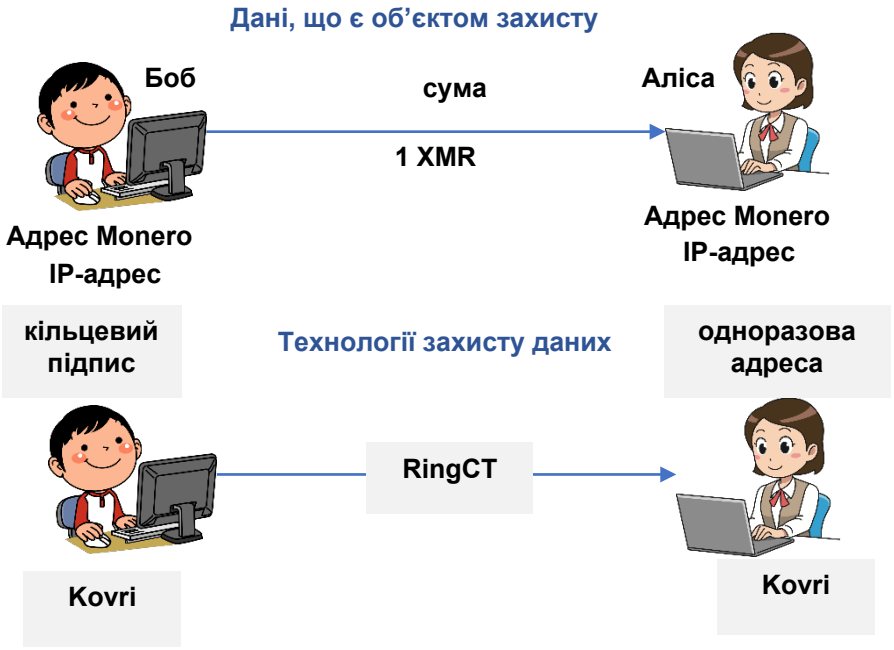

Рис. 5. Технології забезпечення конфіденційності (анонімності) трансакцій і користувачів Monero

Кільцеві підписи будуть відстежуватися тільки в разі, якщо один і той самий користувач двічі підписує одне й те саме повідомлення одним і тим самим закритим ключем (Peili, Haixia, 2020).

Характерним для Monero є наявність у користувача двох пар ключів – приватний/публічний ключі витрат (k^s, K^s) і приватний/публічний ключі перегляду (k^v, K^v). Приватні ключі переважно створюються через генерацію мнемонічної фрази (зерна) довжиною від 13 до 25 слів деякої мови (англійська, іспанська, португальська, японська, есперанто тощо). Основна адреса (primary address)

користувача – це пара публічних ключів (K^s, K^v), яка об'єднана з префіксом 0x12, контрольною сумою (4 байти ґеша Keccak256 від 0x12/K^s/K^v) і представлена в кодуванні Base58[1]:

Base58(0x12 | K^s | K^v | checksum) = "4 ……."
[95 символів].

Отже, основні адреси починаються з цифри 4 і можуть містити маленькі й великі латинські літери й цифри, окрім 0 (нуль), O (велика латинська о), I (велика латинська і), l (маленька латинська L):

123456789ABCDEFGHJKLMNPQRSTUVWXY Zabcdefghijkmnopqrstuvwxyz.

Користувачі Monero з двох пар ключів основної адреси (k^s, K^s)/(k^v, K^v) можуть генерувати субадреси (subaddresses), які формуються через відповідні публічні субключі ($K^{s,i}$, $K^{v,i}$):

Base58(0x2A | $K^{s,i}$ | $K^{v,i}$ | checksum) = "8 ……."
[95 символів].

Субадреси починаються з цифри 8. Кошти, надіслані на субадреси, можна переглядати і витрачати, використовуючи приватні ключі перегляду і витрачання основної адреси. Приклади адреси Monero:

41uD5Tha7H3K2vtEhBWa7WddUiBgbjRLgT57x59 BaFF4GFTrFhkP2Z6ieif5XnVx26Tz2a7WNZSz8b7L mWy3txi7GUVfTgQ;

899iDfG5K4UFG8wQctki3sULRF28PvApthSb2xeHy M7PV2AXxyJs31LVUD3ZNyQU1cXSK9NjyRPxCbvh HG2ByCz3M59HL4C.

Альтернативою субадресам у Monero можуть бути так звані інтегровані адреси (integrated addresses), які містять ідентифікатор платежу (Payment ID) (випадковий рядок довжиною 8 байтів), потрібний для зв'язування вхідних платежів із певним відправником або виставленим рахунком. Інтегрована адреса формується таким чином:

Base58(0x13 | K^s | K^v | Payment ID | checksum) = "4 ……." [106 символів].

Причому Payment ID в адресі може бути зашифрованим і доступним для розшифрування тільки отримувачем платежу.

Для спрощення використання людиною публічних основних, суб- та інтегрованих адрес Monero запроваджено можливість (OpenAlias) використовувати адресу електронної пошти або ім'я домену як псевдоніму конкретної адреси Monero, наприклад donate@getmonero.org або donate.getmonero.org. Для цього у глобальній мережі створюються спеціальні захищені DNS-сервери, що містять записи відповідності за таким синтаксисом[2]:

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

Перетворення електронної пошти або імені домену в адресу Monero через запит до відповідного DNS-серверу реалізується криптогаманцем.

Публічні основні, суб- та інтегровані адреси Monero безпосередньо не зазначаються у трансакції і відповідно не містяться в блокчейні Monero. З публічної адреси отримувача відправник платежу створює одноразову (невидиму) адресу (stealth address), значення і можливість витрати коштів з якої доступні володільцю пар ключів відповідної публічної адреси. Приватний ключ перегляду k^s отримувача платежу використовується для визначення доступних одноразових адрес у блокчейні, на які надійшли кошти, а приватний ключ витрат отримувача платежу k^v – для подальшої витрати коштів із цих адрес.

У Monero є групові адреси (multisignature addresses), витрачати кошти з яких можливо тільки за згодою (підписом) m користувачів з n. Для таких адрес пари групових ключів перегляду та витрати формуються з пар ключів учасників групи. Синтаксис групової адреси не відрізняється від звичайного.

Доступ до блокчейну Monero для аналізу трансакцій можна отримати через наявні у глобальній мережі ресурси, наприклад localmonero.co/blocks, blockchair.com/monero, monero.com/explorer та ін. За відомими ґешом трансакції (рис. 6) з точки зору розслідувань можна встановити:

– UTC час унесення в блокчейн трансакції;

– кількість одноразових адрес (Inputs (2)), з яких витрачалися кошти, але без точного встановлення самих адрес;

– одноразові адреси, на які кошти переказувались (Outputs (2), Stealth address).

[1] Monero Addresses Cheatsheet // Monero : сайт. URL: https://www.getmonero.org/library/MoneroAddressesCheatsheet20201206.pdf (дата звернення: 01.07.2023).

[2] OpenAlias. Simplifying the World. URL: https://openalias.org (дата звернення: 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	4ee0967119602f92cc662d112348597c9812308b99c5d9070251007734944b88	?

2 output(s) for total of ? xmr

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

Рис. 6. Базова інформація у трансакції Monero

Подальший аналіз визначеної трансакції показує, що одноразова адреса (stealth address), з якої відбувалася витрата, приєднана до 10 випадкових адрес блокчейну з невитраченими виходами (рис. 7). Сьогодні протокол передбачає приєднання до 15 випадкових адрес блокчейну з невитраченими виходами.

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	4ee0967119602f92cc662d112348597c9812308b99c5d9070251007734944b88	?

Рис. 7. Одноразова адреса входу трансакції серед 10 випадкових адрес блокчейну з невитраченими виходами

Сума (Amount) трансакції зашифрована й доступна для перегляду тільки володільцю приватного ключа перегляду k^v публічної адреси отримувача платежу (рис. 8) або володільцю приватного ключа витрати k^s публічної адреси, з якої переказуються кошти на публічну адресу отримувача (рис. 9).

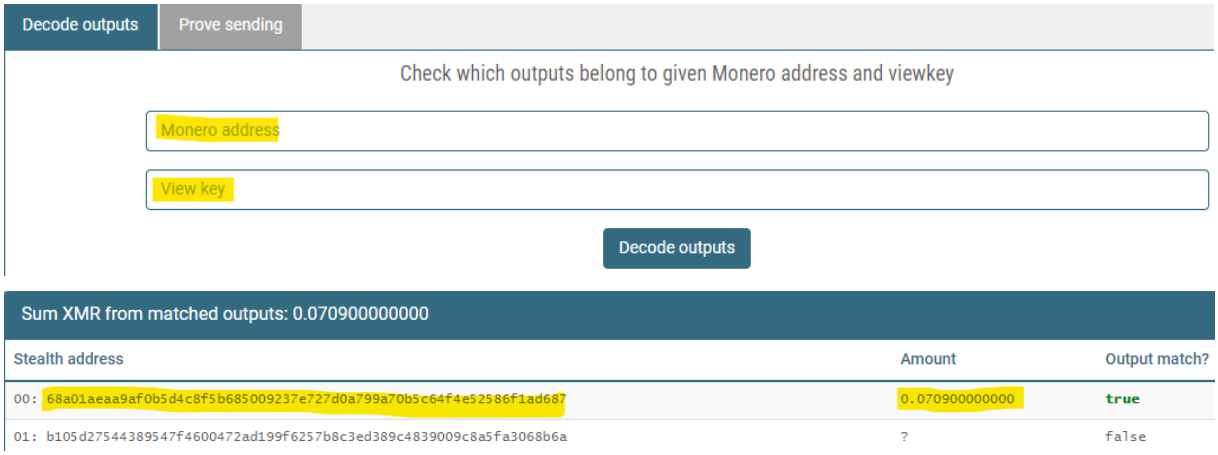

Рис. 8. Розкриття суми виходу на одну з одноразових адрес трансакції через уведення публічної адреси та відповідного приватного ключа перегляду публічної адреси отримувача платежу

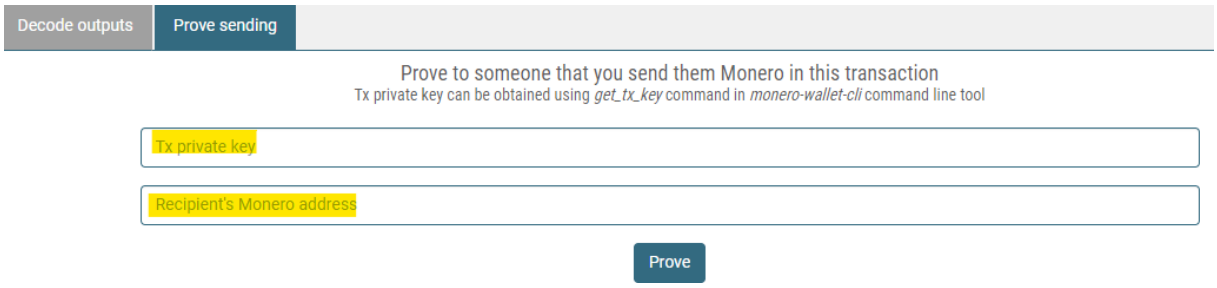

Рис. 9. Можливість для відправника отримати підтвердження переказу коштів на визначену публічну адресу Monero отримувача

Таким чином, аналіз блокчейну Monero не дозволяє відстежити рух коштів, що стосуються протиправної діяльності, без знання публічної адреси і відповідних ключів. Деталі однієї трансакції можна встановити, якщо злочинець здійснює переказ зі свого акаунту легальної криптовалютної біржі (сервісу обміну) через відповідний запит.

Особливості криміналістичного дослідження засобів комп'ютерної техніки, які використовувалися для роботи з Monero

Щодо приватно-орієнтованих криптовалют узагалі та Monero зокрема нині знайдено небагато наукових праць, у яких висвітлюються методи ідентифікації учасників криптовалютних трансакцій. До того ж нерідко ці методи перебувають ще на етапі експериментального дослідження та не завжди можуть дати бажаний результат (Biryukov, Tikhomirov, 2019; Kumar et al., 2018; Wijaya et al., 2018; Tramer, Boneh, Paterson, 2020). Те ж саме стосується робіт із криміналістичного аналізу відповідних засобів комп'ютерної техніки, які використовувалися для роботи з приватно-орієнтованими криптовалютами. Доволі ґрунтовною в цьому плані є робота «Криміналістичний аналіз криптовалют, орієнтованих на конфіденційність» (Koerhuis, Kechadi, Le-Khac, 2020), у якій шляхом експерименту було встановлено, що з оперативної пам'яті засобу комп'ютерної техніки можна вилучити такі артефакти:

– після створення гаманця – парольну фразу гаманця (формат ASCII та UTF16), мнемонічну ключову фразу (зберігається лише у форматі UTF16);

– після відкриття гаманця за допомогою парольної фрази – парольну фразу гаманця (формат ASCII та UTF16), публічну адресу власного гаманця (формат ASCII);

– після отримання трансакції з іншого гаманця – парольну фразу гаманця (формат ASCII та UTF16), публічну адресу власного гаманця, ID вхідної трансакції з отриманою сумою XMR;

– після надсилання трансакції на інший гаманець – парольну фразу гаманця (формат

ASCII та UTF16), ID вихідної трансакції із сумою XMR, ідентифікатор попередньої трансакції, публічну адресу отримувача, публічну адресу власного гаманця;

– після відправлення трансакції з повним ідентифікатором платежу – парольну фразу гаманця (формат ASCII та UTF16), ID вихідної трансакції із сумою XMR, публічну адресу гаманця отримувача, публічну адресу власного гаманця, повний платіжний ідентифікатор трансакції, ідентифікатори попередніх трансакцій;

– після отримання трансакції з інтегрованою адресою гаманця, яка містить ідентифікатор платежу в межах публічної адреси, – парольну фразу гаманця (формат ASCII та UTF16), ID вхідної трансакції із сумою XMR, публічну адресу гаманця попереднього отримувача, публічну адресу власного гаманця, короткий платіжний ідентифікатор трансакції, ідентифікатори попередніх трансакцій, повний ідентифікатор платежу попередньої трансакції;

– після виконання дії OpenAlias resolve у програмному забезпеченні гаманця, коли адресу пожертвування Monero виправлено, – парольну фразу гаманця (формат ASCII та UTF16), публічну адресу власного гаманця, публічну адресу гаманця попереднього отримувача, короткий платіжний ідентифікатор попередньої трансакції, ідентифікатори попередніх трансакцій, повний ідентифікатор платежу попередньої трансакції, виправлену публічну адресу з її описом;

– після закриття програмного забезпечення гаманця – парольну фразу гаманця (тільки формат UTF16), публічну адресу власного гаманця, всі ідентифікатори попередніх трансакцій, повний ідентифікатор попередньої трансакції, короткий ідентифікатор попередньої трансакції (належить до інтегрованої адресної трансакції).

Перехоплення мережного трафіку дозволяє встановити наявність роботи встановленого клієнту Monero. Під час аналізу дискового простору у двох файлах клієнту Monero, які становили інтерес (monero-wallet-gui.log та файл з розширенням txt та іменем, що містить назву гаманця), було виявлено публічну адресу власного гаманця, ідентифікатори всіх трансакцій, суми отриманих та відправлених XMR.

При проведенні розслідувань кримінальних правопорушень також становить інтерес ідентифікація на пристроях підозрюваного інстальованих гаманців Monero. На офіційному сайті спільноти Monero[1] наведені гаманці для різних пристроїв і операційних систем, які вважаються безпечними і рекомендовані для використання. У таблиці 1 наведено ключові артефакти, за допомогою яких можна ідентифікувати на пристрої, що оглядається, встановлені гаманці Monero. Для ОС Android/iOS каталоги та файли гаманців містяться в захищеному від перегляду каталозі.

Таблиця 1

Артефакти гаманців Monero

Назва застосунку	*Основні каталоги*	*Шаблони основних файлів*
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	недоступні	недоступні
Feather	Monero\wallets, AppData\Roaming\FeatherWallet	feather*; wallet*, *.keys
Monerujo	недоступні	недоступні
MyMonero	locales, swiftshader, resources	MyMonero*,
Edge	недоступні	недоступні
ASB	wallet	seed.pem, asb.exe, sqlite, asb-wallet*
UnstoppableSwap	\AppData\Local\Programs\unstoppableswap-gui	UnstoppableSwap.exe

[1] Downloads // Monero : сайт. URL: https://www.getmonero.org/downloads/ (дата звернення: 01.07.2023).

Паперові гаманці Monero, які можуть виглядати як текстовий файл або файл зображення, зазвичай містять: публічну адресу, мнемонічну фразу та приватні ключі витрат/перегляду і можуть бути представлені у форматі QR-коду або hex-рядка[1] (рис. 10).

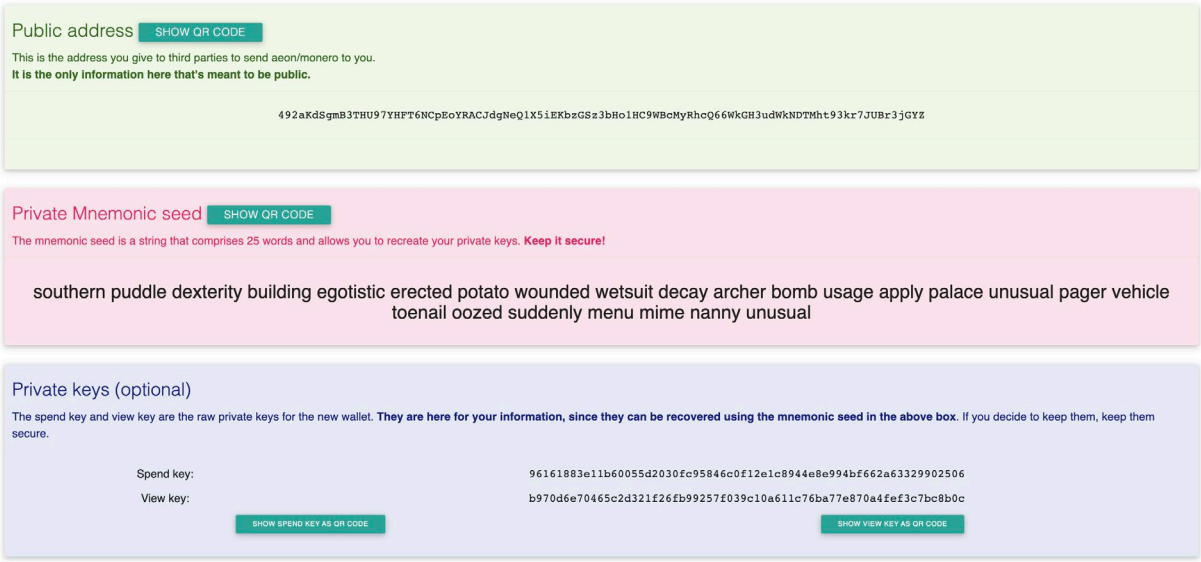

Рис. 10. Приклад паперового гаманця Monero

При проведенні обшуків у фігурантів розслідувань, де згадується Monero, слід звертати увагу на:

– всі пристрої, які можуть містити дані гаманців, наприклад мобільні телефони, планшети, комп'ютери, ноутбуки, жорсткі диски настільних комп'ютерів, флеш-накопичувачі та інші зовнішні носії інформації, SIM-карти тощо;

– апаратні гаманці Trezors та Ledgers (рис. 11), які можуть бути підключені до Monero GUI Wallet;

– паперові та спеціальні носії[2] (рис. 12) з приватними ключами та ключовими (seed) фразами, що додаються до апаратних гаманців. Для програмних гаманців в інструкціях зазвичай вказується рекомендація записувати ключові фрази (а не робити їхні скріншоти з міркувань кібербезпеки), однак часто користувачі роблять скріншоти seed-фраз;

– застосунки криптогаманців або закладок у браузерах із покликаннями на криптобіржі та онлайн-гаманці[3].

[1] How to create a Monero paper wallet // Monero : сайт. URL: https://www.getmonero.org/resources/user-guides/securely_purchase.html (дата звернення: 01.07.2023).

[2] Cryptosteel capsule solo // Ledger : сайт. URL: https://shop.ledger.com/products/cryptosteel-capsule-solo (дата звернення: 01.07.2023).

[3] Pamela C. Crypto Red Flags for Law Enforcement—How to know if your investigation involves cryptocurrency // Ciphertrace : сайт. 13.10.2020. URL: https://ciphertrace.com/crypto-red-flags-for-law-enforcement (дата звернення: 01.07.2023).

Рис. 11. Апаратні криптогаманці Trezor та Ledger

Рис. 12. Сталева капсула захисту seed-фрази Cryptosteel Capsule

Моделювання атомарного обміну (Atomic Swaps) XMR для визначення слідової картини

Активи Monero можуть бути використані для «очищення» історії походження інших криптоактивів (перехід з одного блокчейну в інший) через застосування технології автоматичного атомарного обміну (Atomic Swaps), який не потребує розкриття персональних даних учасників, довіри до третьої сторони і передбачає наявність:

– тейкера (taker) – володіє певною криптовалютою та хоче її обміняти на XMR;

– мейкера (maker) – володіє XMR та пропонує їх обміняти на певну криптовалюту;

– провайдера обміну (Swap Provider) – забезпечує однорангове взаємне виявлення тейкера і мейкера через безпечну точку зустрічі в мережах p2p[1], Tor[2], Loki[3] і одночасно може бути мейкером.

При атомарному обміні можливі лише два результати: або обмін успішно завершений і кожен учасник отримує кошти іншого, або нічого не відбувається і обидва учасники зберігають кошти, які мали до обміну. Протокол атомарного обміну змушує обидві сторони дотримуватися правил і неможливо заволодіти монетами іншої сторони поза визначеними правилами, отже, не вимагається наявність посередника, якому довіряють обидві сторони.

Сьогодні Atomic Swaps реалізований для:

– 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).

Атомарний обмін може бути здійснений через використання браузеру для підключення до сайту провайдера обміну (рис. 13) або через клієнтські модулі, які встановлюються на пристрій тейкера.

Тестування Atomic Swaps BTC<>XMR з метою вивчення особливостей процедури і слідів, які утворюються, може виглядати таким чином.

Потрібно здійснити симуляцію вузла провайдеру обміну (Service Provider Host) з функцією мейкера та вузла тейкера (User Host), які підключені до публічних серверів testnet Bitcoin і stagenet Monero (рис. 14)[4].

[1] A modular network stack. URL: https://libp2p.io/ (дата звернення: 01.07.2023).

[2] Tor Projec. URL: https://www.torproject.org/ (дата звернення: 01.07.2023).

[3] Lokinet. URL: https://lokinet.org/ (дата звернення: 01.07.2023).

[4] Automated Swap Backend (ASB) // GitHub : сайт. URL: https://github.com/comit-network/xmr-btc-swap/blob/master/docs/asb/README.md (дата звернення: 01.07.2023).

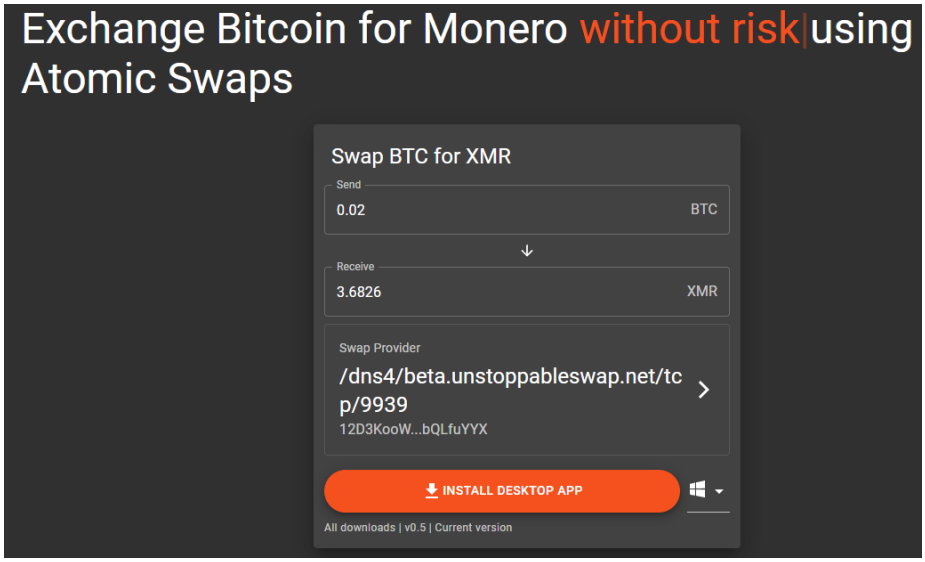

Рис. 13. Атомарний онлайн-обмін через сайт unstoppableswap.net

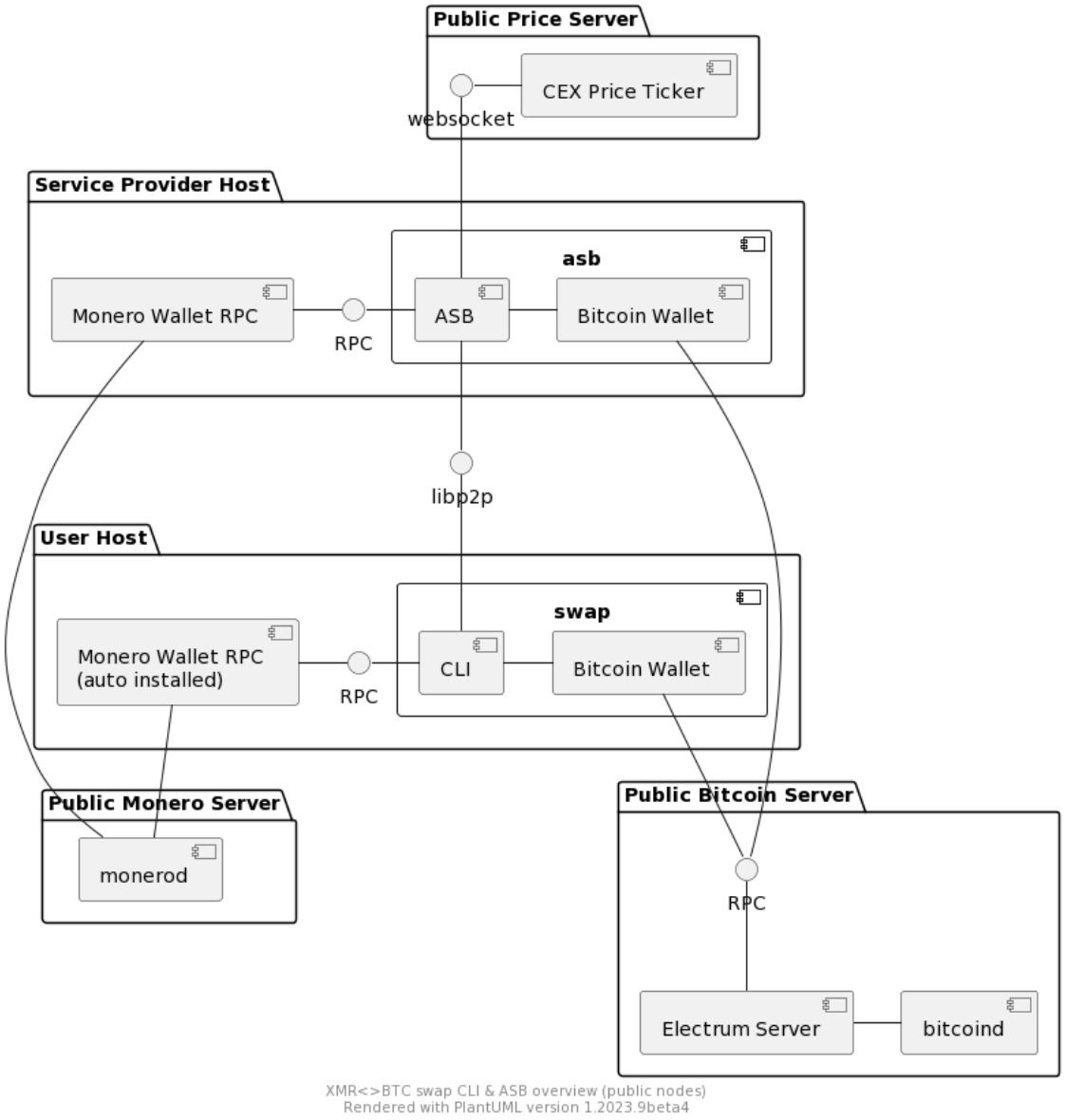

Рис. 14. Схема з'єднань компонентів атомарного обміну BTC<>XMR із використанням публічних серверів Bitcoin і Monero

Відповідно потрібно встановити і налаштувати два гаманці:

– Electrum[1] (BTC);

– Monero GUI (XMR).

При встановленні Electrum через Windows Installer буде додатково інстальований Electrum Testnet (рис. 15), який вже налаштований для підключення до testnet BTC. Після встановлення Monero GUI Wallet його необхідно підключити до мережі Stagenet так, як буде описано нижче (рис. 15).

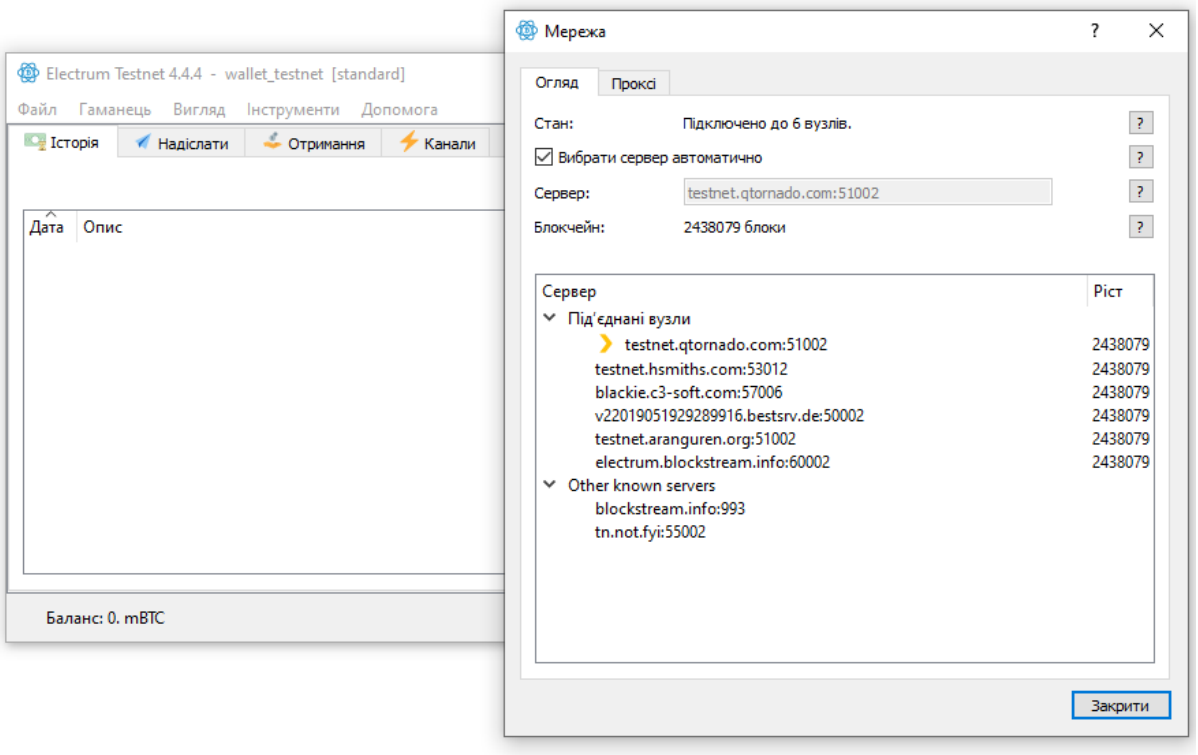

Рис. 15. Гаманець Electrum Testnet

Через один із доступних «кранів», наприклад bitcoinfaucet.uo1.net, на адресу гаманця Electrum Testnet отримати тестові BTC (рис. 16), через сайт community.rino.io/faucet/stagenet на адресу гаманця Monero GUI Wallet отримати тестові XMR.

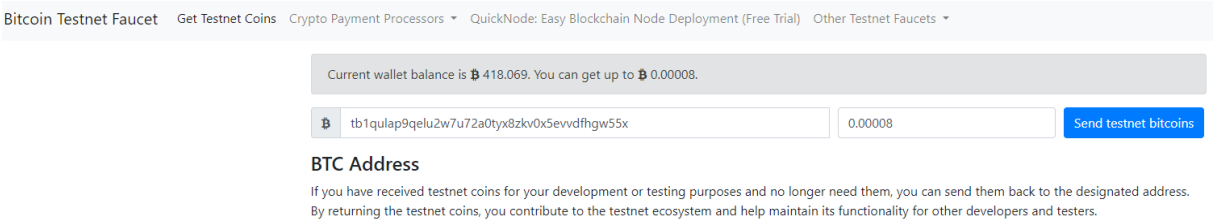

Рис. 16. Сайт-кран bitcoinfaucet.uo1.net з отримання тестових BTC

Ініціалізація сервісів Service Provider Host як мейкера атомарного обміну

Практична оцінка показала, що застосунки мейкера доцільно розгортати в ОС Linux. В окремому каталозі потрібно мати: monero-wallet-rpc[2] (входить до архіву Monero CLI Wallet) і asb[3].

[1] Electrum Bitcoin Wallet. URL: https://electrum.org/#download (дата звернення: 01.07.2023).

[2] Monero CLI Wallet // Monero : сайт. URL: https://www.getmonero.org/downloads/#cli (дата звернення: 01.07.2023).

[3] Release 0.12.1 comit-network/xmr-btc-swap // GitHub : сайт. URL: https://github.com/comit-network/xmr-btc-swap/releases/tag/0.12.1 (дата звернення: 01.07.2023).

Запустити в терміналі monero-wallet-rpc із підключенням до публічного вузла Monero мережі Stagenet[1] і зазначенням каталогу гаманця Bitcoin сервісу обміну (рис. 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
```

Рис. 17. Результат виконання команд

Запустити в терміналі Automated Swap Backend (ASB):

>./asb --testnet start

і дотримуватись вказівок майстра налаштувань (рис. 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
```

Рис. 18. Налаштування Automated Swap Backend (ASB)

Під час налаштування ASB буде створено:

– гаманець Monero мейкера (asb-wallet) без паролю із новим адресом, який підключений до monero-wallet-rpc і потребує поповнення тестовими монетами XMR для подальшого обміну на BTC;

– гаманець Bitcoin мейкера, що підключений до electrum.blockstream.info;

– ідентифікатор однорангового вузла-мейкера в мережі p2p і мультиадресу[2] (multiaddr) його доступності.

Через сайт-кран community.rino.io/faucet/stagenet на адресу гаманця мейкера (asb-wallet) отримати тестові XMR та пересвідчитися в поповнені в командному рядку monero-wallet-rpc.

Ініціалізація обміну BTC<>XMR з вузла тейкера

Завантажити в окремий каталог модуль атомарного обміну swap[3] і запустити його з такими параметрами:

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

де

<bitcoin-change-address> – адреса Bitcoin, на яку будуть повернуті BTC у разі неуспішності обміну (взяти зі встановленого Electrum Testnet);

<monero-receive-address> – адреса Monero, на яку при обміні будуть перераховані мейкером XMR (взяти зі встановленого Monero GUI Wallet);

[1] Public Monero nodes. URL: https://community.rino.io/nodes.html (дата звернення: 01.07.2023).

[2] Addressing in libp2p // GitHub : сайт. URL: https://github.com/libp2p/specs/blob/master/addressing/README.md (дата звернення: 01.07.2023).

[3] Release 0.12.1 comit-network/xmr-btc-swap // GitHub : сайт. URL: https://github.com/comit-network/xmr-btc-swap/releases/tag/0.12.1 (дата звернення: 01.07.2023).

<seller> – адреса та ідентифікатор вузла мейкера, які вказані в командному рядку запущеного модулю ASB (рис. 19), наприклад:

/ip4/127.0.0.1/tcp/9939/p2p/12D3KooWBdQGiVJuBoXXrKBExh9mCeUgwBeusWU8mnr9m55D7uTP.

У результаті додатково завантажиться monero-wallet-rpc, відбудеться підключення до мейкера і згенерується адреса Bitcoin (QR-код) смарт-контракту, на яку буде запропоновано перерахувати BTC для обміну (рис. 19).

```
└─$ ./swap buy-xmr --testnet --change-address tb1q6khtw5mxghlccrhd5k9zzcvlzpx2apvqqvq22c --receive-address 7554Ds3uU9
gf3qCdLcxQYZ6EGtdjb6ALYbF82JwKeA4WQ4tXqAzbGeChMwjtRQcArLeeff3PK6PoZeW9F6SwDgFB4vTPPsk --seller /ip4/127.0.0.1/tcp/993
9/p2p/12D3KooWBdQGiVJuBoXXrKBExh9mCeUgwBeusWU8mnr9m55D7uTP
Logging initialized to /home/kali/.local/share/xmr-btc-swap/cli/testnet/logs
Connected to Alice at /ip4/127.0.0.1/tcp/9939/p2p/12D3KooWBdQGiVJuBoXXrKBExh9mCeUgwBeusWU8mnr9m55D7uTP
Received quote price=0.00537744 BTC minimum_amount=0.0002 BTC maximum_amount=0.02 BTC
```

```
Estimated fee of 121.25 is smaller than the min relay fee, defaulting to min relay fee 1000
Deposit at least 0.00021 BTC to cover the min quantity with fee!
Waiting for Bitcoin deposit deposit_address=tb1qhdcnc9nyzlh3c3hvjcc5zuz702j7c4rxltywuc min_deposit=0.00021 BTC max_gi
veable=0 BTC minimum_amount=0.0002 BTC maximum_amount=0.02 BTC
```

Рис. 19. Ініціалізація обміну BTC<>XMR через модуль swap

З гаманця Electrum Testnet переказати BTC на згенеровану адресу (рис. 20).

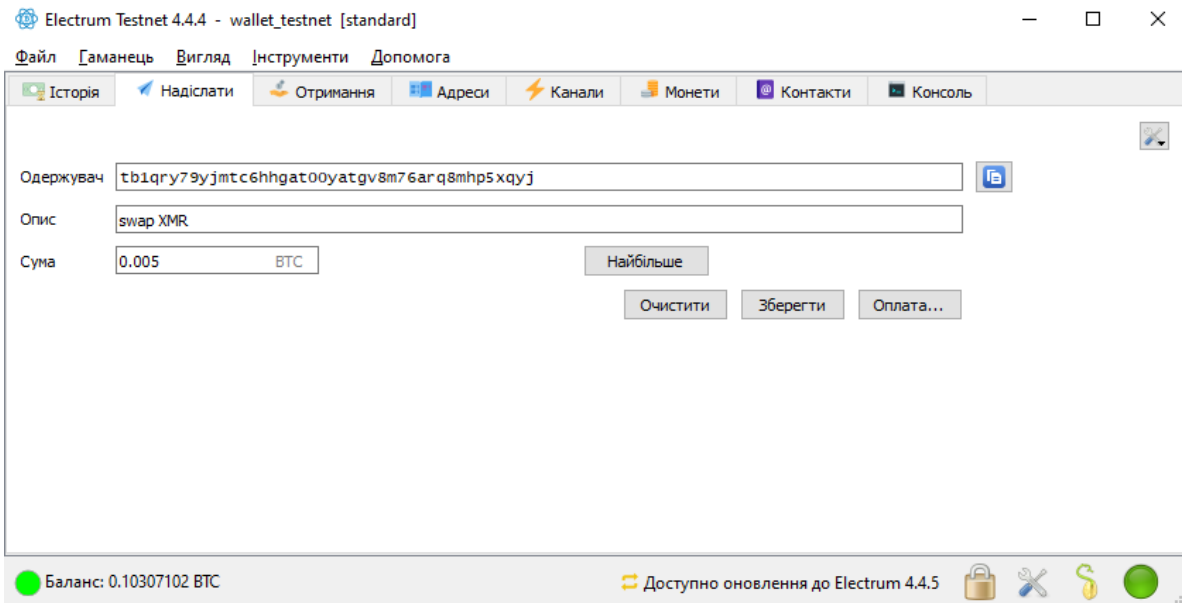

Рис. 20. Переказ BTC для обміну на XMR

По завершенню автоматичних процедур взаємних переказів обмін або буде завершений, або кошти будуть повернені тейкеру і мейкеру в разі переривання окремих фаз протоколу.

За результатами проведеного моделювання встановлено, що на пристроях учасників атомарного обміну залишаться характерні каталоги і файли застосувань monero-wallet-rpc, swap (табл. 1) та реалізації Bitcoin wallet.

Моделювання вилучення XMR

Ще одним важливим аспектом роботи із протиправно одержаними криптоактивами є їх вилучення. Сьогодні реалізовано три окремі мережі та блокчейни Monero: основна (mainnet), налагоджувальна (stagenet) і тестова (testnet). Кожен блокчейн має власний відокремлений від інших генезис-блок. Для відпрацювання правоохоронцями процедури контрольованого переказу XMR при вилученні віртуальних активів краще використовувати мережу Stagenet, яка технологічно еквівалентна основній, а не Testnet, у якій розробники перевіряють нові технології перед їх впровадженням у мережу Mainnet.

Офіційним і найбільш функціональним гаманцем Monero є Monero GUI Wallet[1], процес підключення якого до Stagenet може бути змодельовано так.

Завантажити останню офіційну версію Monero GUI Wallet з домену getmonero.org, наприклад у вигляді архіву.

Перевірити цілісність завантаженого архіву через обчислення ґешу і порівняння його із зазначеним на сайті.

Розпакувати архів і запустити основний файл гаманця monero-wallet-gui.exe, після чого відкриється вікно майстра налаштування, де слід обрати відповідну мову інтерфейсу: «Розширений режим» → «Додаткові налаштування» і у спадному списку → Stagenet (рис. 21).

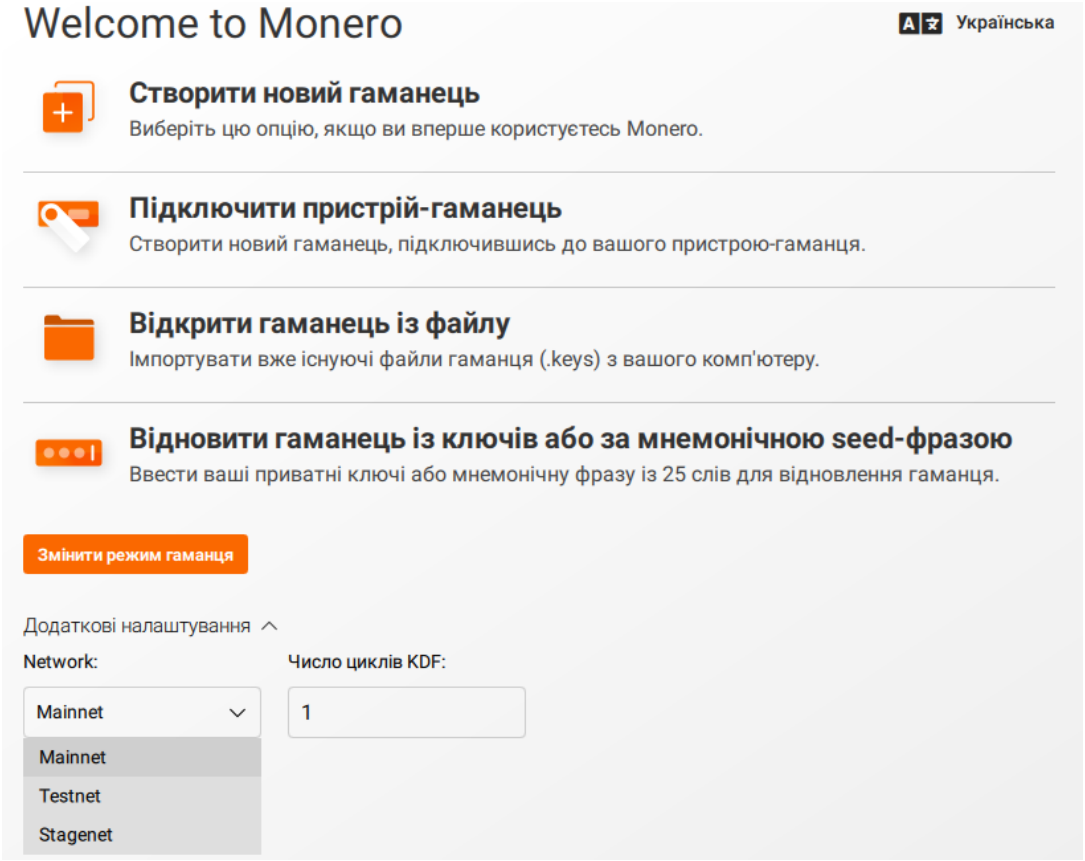

Рис. 21. Налаштування підключення до мережі Stagenet

Через майстер створити нову адресу (гаманець), зберегти seed-фразу з 25 слів, встановити надійний пароль доступу для користування гаманцем, у налаштуваннях Daemon settings (рис. 22) обрати «Підключитися до віддаленої ноди» → «Add remote node», де вставити доменне ім'я ноди та порт, які взяти зі списку доступних нод мережі Stagenet на monero.fail (рис. 23).

[1] Downloads // Monero : сайт. URL: https://www.getmonero.org/downloads/ (дата звернення: 01.07.2023)

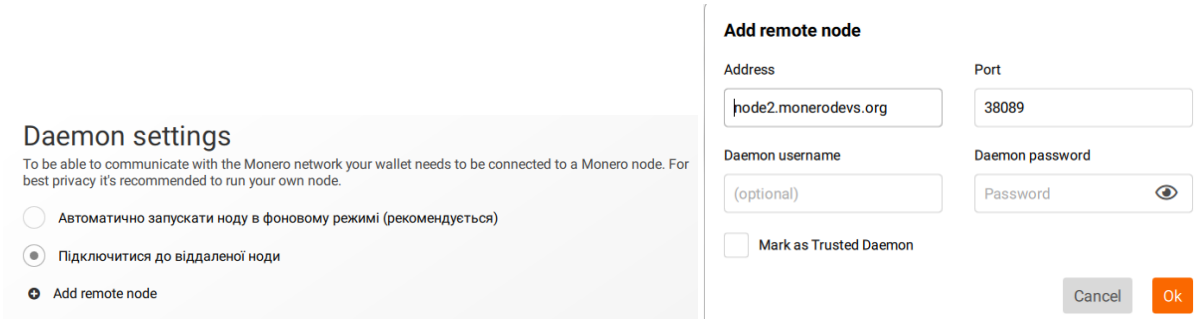

Рис. 22. Налаштування доступу до віддаленої ноди з блокчейном мережі Stagenet

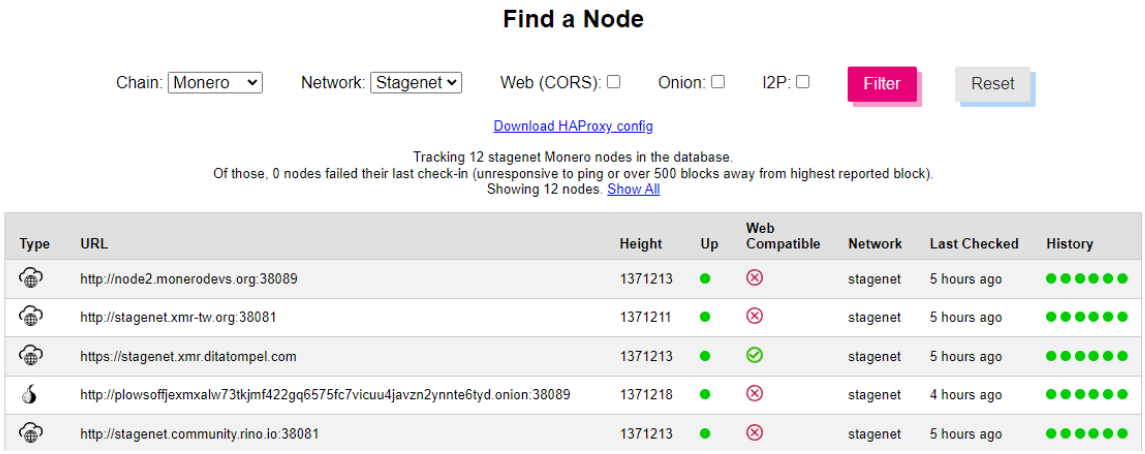

Рис. 23. Список доступних нод із блокчейном мережі Stagenet

Про підключення до Stagenet буде свідчити напис «Тестова мережа» (рис. 24) на стартовій сторінці гаманця і адреса, що починається з «5».

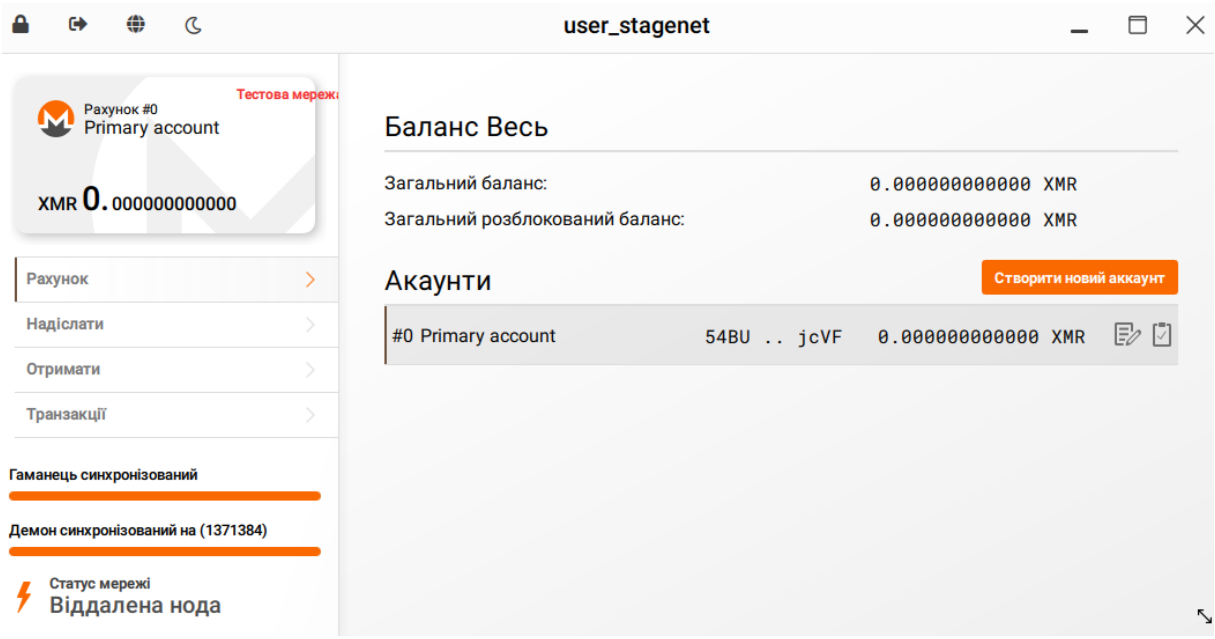

Рис. 24. Підключений до мережі Stagenet гаманець

Через сайт community.rino.io/faucet/stagenet на згенеровану адресу гаманця слід отримати тестові XMR (рис. 25).

Рис. 25. Сайт-кран community.rino.io/faucet/stagenet з отримання тестових XMR

У підсумку буде створена адреса Monero з балансом тестових монет, що дозволяє далі здійснити з неї переказ XMR на спеціальну адресу в межах імітації вилучення віртуальних активів.

Оскільки сьогодні відсутня нормативно визначена технологія вилучення віртуальних активів, то можна запропонувати як адресу Monero зберігання вилучених XMR використовувати так звані multisig-адреси, з яких виводити кошти можливо тільки при накладанні цифрових підписів декількох осіб за правилом m з n.

Для створення multisig-адреси, наприклад із правилом підпису трансакції витрати 2 із 2, необхідно спочатку кожній особі (нехай Person A і Person B) згенерувати нові окремі адреси зі своїми ключами. Робота з multisig-адресами реалізована тільки в командному рядку cmd Monero CLI Wallet, файли якого розташовані у каталогу \extras гаманця Monero GUI Wallet. Попередньо потрібно обрати на monero.fail ноду Stagenet, до якої далі буде підключатися Monero CLI Wallet, наприклад, stagenet.community.rino.io:38081[1].

Кожна особа в режимі діалогу з Monero CLI Wallet створює файл гаманця:

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

У створеному гаманці кожна особа робить довіреною віддалену ноду і вмикає опцію підготовки даних для multisig-адреси:

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

set enable-multisig-experimental 1,

prepare_multisig.

Після виконання команди prepare_multisig кожна особа отримає відповідно умовний рядок даних <dataA> і <dataB>, які будуть схожі на таке:

MultisigxV2R1bFSuJcgPWh1EMiLo3DMaaEcN9k6Y7p5BoRapCX5BD2T8PKC5Ls4MVVWG1QYwNfnY4ZTbzAD14S9FBWwU12Sr6riX7CDC62b7h3XXZiuAHLmUJaTfCqvWjMbc4MtsSYkFkXPcBDSJd1esqPQbcgwUZS4g2xdhoNtStWu3ViFMKvdCNSyU.

Цими рядками особи обмінюються і роблять подальшу ітерацію з отриманими даними один одного:

Person A: make_multisig 2 <dataB>,

Person B: make_multisig 2 <dataA>.

Після виконання команди make_multisig кожна особа отримає відповідно умовний рядок даних <infoA> і <infoB>, якими також особи обмінюються і завершують створення спільного гаманця multisig:

Person A: exchange_multisig_keys <infoB>,

Person B: exchange_multisig_keys <infoA>.

У кожної особи буде згенерована спільна multisig-адреса з порогом витрати 2/2 та своїми паролями доступу:

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

Multisig address: 52MAkwb4q5YCK9vDNksygzGKnmnAs2ecujUuHktip1MGMXmygKmYQgNhvRv64cfFZqaAgWQyy1bWnK78GktnQqjJSEuNLNv.

Для імітації контрольованого переказу XMR на гаманці Monero GUI Wallet необхідно в

[1] Public Monero nodes // Rino : сайт. URL: https://community.rino.io/nodes.html (дата звернення: 01.07.2023).

розділі «Надіслати» (рис. 26) вставити multisig-адресу, вказати суму переказу та підтвердити трансакцію.

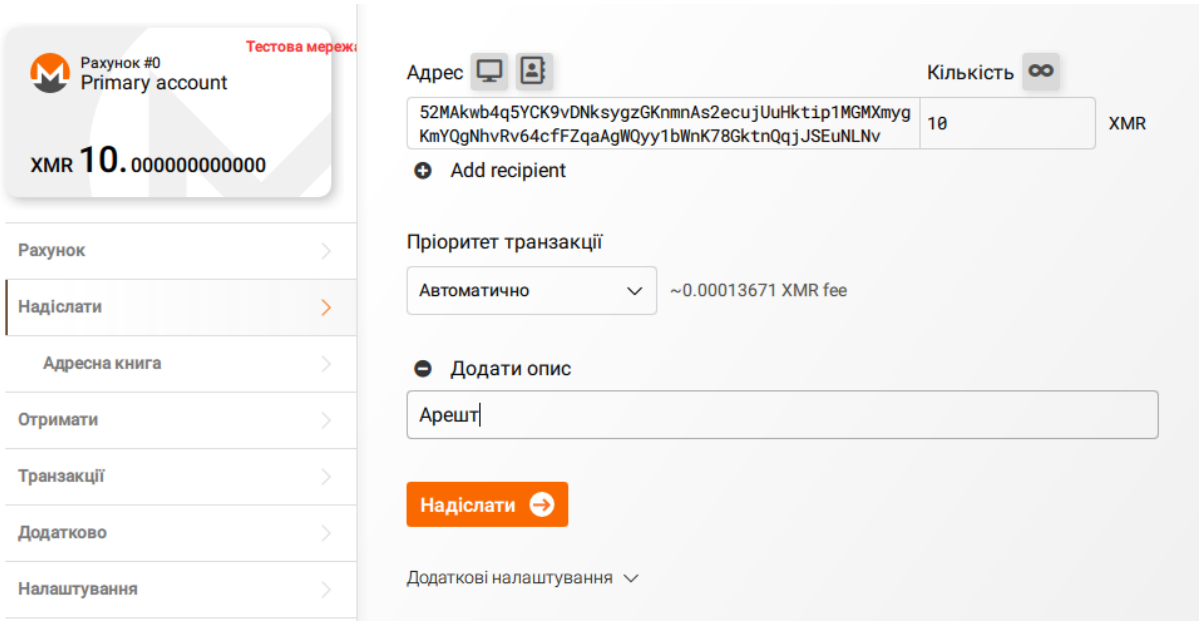

Рис. 26. Переказ XMR на multisig-адресу

Факт переказу XMR через певний час буде відображений у гаманці Monero GUI Wallet та в гаманці Monero CLI Wallet multisig-адреси через команди: refresh, show_transfers. Також деталі трансакції за її ґешем можна побачити в блокчейні Stagenet, наприклад на сайті community.rino.io/explorer/stagenet, увівши адресу та приватний ключ перегляду multisig-адреси, який можна отримати в Monero CLI Wallet через команду viewkey.

Далі загальний сценарій імітації переказу з multisig-адреси за правилом 2/2 складається з двох етапів:

– один із володільців multisig-адреси зі свого гаманця експортує у файл часткове зображення приватного ключа multisig-адреси та відправляє його ініціатору трансакції, який зі свого боку імпортує файл до свого гаманця;

– ініціатор створює файл трансакції, підписує й передає на підпис другому володільцю, після чого трансакція з двома підписами відправляється в мережу Monero для перевірки та включення в блокчейн.

Зазначені етапи реалізуються таким чином. Експорт часткових зображень приватного ключа у файл imgkeyA(B):

Person A: export_multisig_info imgkeyA,

Person B: export_multisig_info imgkeyB.

Імпорт часткових зображень приватного ключа:

Person A: import_multisig_info imgkeyB,

Person B: import_multisig_info imgkeyA.

Person A створює і підписує файл трансакції multisig_monero_tx переказу всіх коштів на визначену адресу, наприклад так:

[wallet 5AvBWc]: sweep_all 77yxUAG9nF43G5KWm93mk9QFiwvY9fSy3Bd9CtzNoxPTYxVgUF7tqocAhdyJuxqqBhVN6X4Q4a22aiV7LSZaSu5H5Jjx8rX.

Person B зі свого боку також підписує файл трансакції multisig_monero_tx та відправляє в мережу Stagenet:

[wallet 5AvBWc]: sign_multisig multisig_monero_tx,

[wallet 5AvBWc]: submit_multisig multisig_monero_tx.

Успішність включення трансакції у блокчейн буде відображена у гаманці Monero CLI Wallet multisig-адреси.

Здійснення Monero трансакцій у мережі Stagenet показала, що основні тестові адреси починаються з цифри 5, а субадреси – із 7.

ВИСНОВКИ. Криптовалюти все більше стають звичайним інструментом обміну цінностей у сфері кримінальної протиправності, тому правоохоронні органи вже сьогодні повинні мати належні знання й навички, достатні для ефективного документування відповідної протиправної діяльності. Зважаючи на все більший інтерес до приватно-орієнтованих криптовалют з боку правопорушників, правоохоронним органам слід приділити особливу увагу вивченню техніко-криміналістичних аспектів роботи з найбільш поширеними

валютами такого виду, зокрема Monero, Verge, Dash та Zcash.

Через складнощі ідентифікації учасників відповідних трансакцій у таких криптовалютах правоохоронцям слід принаймні розуміти окремі аспекти документування їх використання. Щодо системи Monero, то потрібно знати головні аспекти організації її роботи, орієнтуватися у способах додаткового приховування трансакцій, розуміти порядок атомарного обміну (свопінгу) та вміти документувати сліди відповідної діяльності. Крім того, очевидно, що з набуттям чинності законодавства у сфері обігу криптовалют та внесення відповідних змін до Кримінального процесуального кодексу України слід бути готовим до правильної організації вилучення відповідних криптовалютних активів.

Окремі аспекти наведеного розглянуто в цій роботі. Серед іншого за результатами проведеного дослідження доходимо висновків, що сьогодні спостерігається стійкий тренд переходу протиправних угод на приватно-орієнтовані платіжні системи, зокрема Monero. Перевагою цієї системи для правопорушників є підвищена конфіденційність, яка забезпечується використанням кільцевих підписів, невидимих адрес, кільцевих конфіденційних трансакцій, часниковою маршрутизацією. Додатковим захистом від ідентифікації може бути застосування користувачами TOR-мереж та мікшерів. Натепер не існує сталих алгоритмів ідентифікації користувачів Monero, крім окремих випадків, наприклад користування обліковими записами на криптобіржах, аналіз трансакцій, зроблених до 2017 року, тощо. Зважаючи на викладене, правоохоронним органам для ідентифікації користувачів Monero, які становлять інтерес, слід зосередитися на класичних слідчо-оперативних заходах розслідування. Водночас існують дієві механізми документування слідів роботи із платіжної системою Monero та підтверджені методики вилучення із засобів комп'ютерної техніки парольних фраз до криптогаманців та іншої чутливої інформації щодо руху коштів у системі Monero. Окремі сліди залишаються під час застосування атомарного обміну однієї валюти на іншу.

У статті, серед іншого, запропоновано порядок вилучення XMR за допомогою multisig-адрес, з яких виводити кошти можливо тільки при накладанні цифрових підписів декількох осіб. Описана модель успішно апробована в тестовій мережі.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Носов В. В., Манжай І. А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1 (80). С. 93–100. DOI: https://doi.org/10.32631/pb.2021.1.13.

2. Носов В. В., Манжай О. В., Панченко Є. В. Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень. *Право і безпека*. 2022. № 4 (87). С. 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 Net-work 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 K. G. Paterson. Stockholm : Springer, 2021. Pp. 552–576. DOI: https://doi.org/10.1007/978-3-030-75539-3_23.

6. Handaya W. B. T., Yusoff M. N., 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, 11–15 September 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, 26–29 August 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, Netherland, 21–23 October 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., Šrndić 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 K. G. 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 D. A., 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, 1–3 August 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 N. H. 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.

Надійшла до редакції: 04.07.2023

Прийнята до опублікування: 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 Net-work 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, W. B. T., Yusoff, M. N., & 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, V. V. & Manzhai, I. A. (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, V. V., Manzhai, O. V. & 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, Netherland. 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., Šrndić, 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, K. G. (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, D. A., 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, N. H. (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: 4 July 2023

Accepted for publication: 10 August 2023

VITALII 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,
e-mail: 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,
e-mail: cybercop322@gmail.com

TECHNICAL, FORENSIC AND ORGANISATIONAL ASPECTS OF WORK WITH MONERO CRYPTOCURRENCY

The forensic, organisational and technical features of law enforcement agencies' work with the Monero cryptocurrency in the context of pre-trial investigation and operational search activities are analysed. 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 offences 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 artefacts that should be taken into account during inspection and search. Atomic Swaps of XMR are modelled to determine the trace pattern and identify artefacts 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 test network Stagenet is modelled. 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.*

Цитування (ДСТУ 8302:2015): Носов В. В., Манжай О. В., Ковтун В. О. Технікокриміналістичні та організаційні аспекти роботи з криптовалютою Monero. *Право і безпека*. 2023. № 3 (90). С. 102–125. DOI: https://doi.org/10.32631/pb.2023.3.9.

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