УДК 343.1:65.012.8+004 DOI: https://doi.org/10.32631/pb.2022.4.09

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, доцент,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0001-5435-5921,
e-mail: sofist@ukr.net;

ЄВГЕНІЙ ВІКТОРОВИЧ ПАНЧЕНКО,
Національна поліція України,
Департамент кіберполіції,
4-те управління (оперативно-аналітичного забезпечення
та аналізу відкритих джерел);
https://orcid.org/0000-0001-5755-7457,
e-mail: panch.evg@gmail.com

АНАЛІЗ ЕТЕРІУМ-ТРАНСАКЦІЙ ПІД ЧАС ПОПЕРЕДЖЕННЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Запропоновано механізм аналізу етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень на основі вивчення сучасного досвіду в цій сфері. Вивчено стан нормативно-правового урегулювання криптовалют в Україні. Порушено питання неможливості накладання арешту на криптовалютні активи під час кримінального розслідування. Окреслено проблемні моменти, з якими стикаються правоохоронні органи в інших країнах під час накладання арешту на криптовалюти. Розкрито структуру та особливості обігу криптовалюти етер. Шляхом експерименту проведено оцінку деяких програмних інструментів, що використовуються для аналізу етеріум-трансакцій. Продемонстровано автоматизацію пошуку та побудову схеми відношень різних ідентифікаторів етер-трансакцій на прикладі Maltego Community Edition та Crystal Expert. Описано значення ефективного аналізу криптовалют для проведення розслідування. Розкрито технічний бік навчання правоохоронців щодо вилучення криптовалютних активів. Запропоновано механізм контрольованого переказу криптовалютних активів для кастодіальних і некастодіальних гаманців.

Ключові слова: *криптовалюта, етер, ethereum, криптовалютні трансакції, блокчейн, правоохоронні органи, протидія злочинності.*

Оригінальна стаття

ВСТУП. Використання криптовалюти як частини злочинних схем зростає, а поширення цього платіжного засобу прискорюється. Криптовалюта залишається привабливою для злочинців, насамперед через її псевдоанонімну природу та легкість і швидкість, з якою кошти можуть бути відправлені в будь-яку точку світу. Правопорушники стали також більш досвідченими у використанні криптовалют. Незаконне їх використання сьогодні переважно пов'язане з відмиванням грошей, торгівлею (онлайн) незаконними товарами, послугами та шахрайством.

Загальна кількість і вартість криптовалютних операцій, пов'язаних із злочинною діяльністю, все ще становить лише обмежену частку кримінальної економіки порівняно з готівкою та іншими формами операцій. Разом із тим, як свідчать окремі дослідження, намагання державних органів обмежити обіг готівкових коштів також спонукає перенесення оплати протиправних схем у криптовалютну площину (Hendrickson, Luther, 2022).

Отже, для працівників правоохоронних органів досить актуальним питанням є розробка алгоритму дій для автоматизації пошуку

та побудови схеми відношень різних ідентифікаторів криптовалютних трансакцій.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. Метою статті є запропонувати механізм аналізу етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень на основі вивчення сучасного досвіду в цій сфері. Для досягнення поставленої мети потрібно виконати такі *завдання*:

– провести аналіз стану нормативно-правового регулювання криптовалют в Україні, а також їх перспективи;

– дослідити проблемні моменти поводження з криптовалютами на різних стадіях кримінального процесу;

– розкрити структуру й особливості обігу криптовалюти етер;

– вивчити прикладні аспекти застосування інструментів поводження з криптовалютою етер в діяльності правоохоронних органів.

Дослідження є однією з перших спроб вивчення інструментів для аналізу етеріум-трансакцій у контексті автоматизації роботи правоохоронних органів.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. У статті застосовано низку кількісних та якісних методів, які в сукупності дозволяють комплексно вивчити відповідний об'єкт. Історичний метод використано під час аналізу нормативно-правової бази, яка регулює обіг криптовалют в Україні. З метою вивчення структурної організації етер-технології та методів аналізу відповідних трансакцій застосовано метод системного аналізу. Порівняльно-правовий метод дав змогу вивчити стан роботи з криптовалютами правоохоронними органами в Україні та за її межами. Метод моделювання використано для того, щоб показати маніпуляції з тестовою криптовалютною мережею для відпрацювання навичок потенційного накладання арешту на відповідні віртуальні активи.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Для врегулювання обігу криптовалют в Україні 17 лютого 2022 р. було ухвалено Закон України «Про віртуальні активи»[1], відповідно до якого віртуальний актив вважається нематеріальним благом, що є об'єктом цивільних прав, має вартість і виражений сукупністю даних в електронній формі. Проте цей Закон набуває чинності з дня набрання чинності Законом України «Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами»[2]. Це, по-перше, одразу обмежує його застосування в часі, а по-друге, викладена в Законі концепція вкрай опосередковано торкається кримінально-правових і кримінальних процесуальних правовідносин.

Більш слушною уявляється позиція, що регулювання таких криптовалют має відбуватися таким чином, щоб правоохоронні органи могли найбільш ефективно притягувати до відповідальності осіб і за цивільні та кримінальні порушення із найменшими затратами. При цьому посилення тиску на користувачів у довгостроковій перспективі призведе лише до збільшення вартості притягнення до відповідальності (Bryans, 2014, p. 471).

Враховуючи те, що питання обігу криптовалют в Україні досі недостатньо врегульоване, підприємці та правоохоронці керуються загальними нормами законодавчих актів, що не описують специфіку криптовалют. Згідно з нормами Кримінального процесуального кодексу України[3] практично неможливо накласти арешт на такі активи, що і є однією з найгостріших проблем під час розслідування кримінальних правопорушень. Водночас у провідних країнах уже вирішують це питання[4], а в наукових колах обговорюють удосконалення

[1] Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2074-20 (дата звернення: 13.11.2022).

[2] Проект Закону про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами : від 13.03.2022 № 7150 / ініціатор М. В. Крячко // БД «Законодавство України» / ВР України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=73963 (дата звернення: 13.11.2022).

[3] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 13.11.2022).

[4] Guidelines for the Seizure and Sale of Virtual Assets. Interpol Innovation Centre. Singapore, 2020. 29 p.; Virtual Asset Seizure Best Practices. Federal Bureau Investigation (FBI). 2020. 45 p.; Guidance on Financial Investigations Involving Virtual Assets, 2019. Financial Action Task Force (FATF); Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets. December 2021 // GAFILAT : сайт. URL: https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/traducciones/4338-guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets/file (дата звернення: 13.11.2022).

механізму збереження арештованих криптовалютних активів.

Серед проблемних моментів щодо арешту віртуальних активів науковці називають:

– неможливість швидкого від'єднання пристрою з даними криптогаманця від мережі Інтернет через необхідність переказу коштів на контрольований правоохоронними органами гаманець;

– необхідність належного захисту контрольованого правоохоронцями криптогаманця від злому;

– потребу виплати комісійних коштів за кожну трансакцію з криптовалютами, причому розмір такої комісії не є фіксованим;

– використання зловмисниками спеціальних застосунків із прихованими витонченими захисними механізмами для уникнення втрати коштів;

– необхідність взаємодії з криптообмінниками та біржами, які можуть перебувати за межами національної юрисдикції;

– вимоги до кваліфікації правоохоронців і процедури виконання контрольованого переказу криптовалют;

– належність запису в blockchain до доказової інформації;

– уникнення помилок при фіксуванні складних та довгих рядків даних, які потрібно використати для опису гаманців, трансакцій та ключів (Taylor et al., 2021; Taylor et al., 2022).

Важливим аспектом, який ускладнює представлення доказової інформації щодо криптовалют у суді, є також недостатня обізнаність суддів із механізмом роботи криптовалют. Тому часто судді відмовляються брати до уваги незрозумілі для них відомості. Ця проблема є характерною не тільки для національного сегмента, але й для зарубіжних країн (Trozze, Davies, Kleinberg, 2022; Marchant, 2019).

На сьогодні в Україні та за її межами відсутні сталі процедури криміналістичного дослідження криптовалют. У цьому контексті зарубіжні дослідники пропонують досить непогану чотирьохступеневу процедуру: 1) ідентифікація та профілювання; 2) вивчення; 3) отримання та збереження; 4) аналіз і звітування (Paschal Mgembe, Ladislaus Msongaleli, Chaundhary, 2022).

Крім наведених аспектів поглянути на технологію блокчейн, яка використовується у криптовалютах, можна і під іншим кутом. Так, деякі науковці пропонують розглядати цю технологію як інструмент для генерації та зберігання електронних доказів (Wu, Zheng, 2020). Блокчейн компенсує недоліки чинних правил доказування та збільшує достовірність у роботі судів, судово-медичних установ та експертів. Інші дослідники пішли ще далі та розробили на основі технології блокчейн систему, яка підвищує захист мереж від кібератак (Yadav et al., 2022). Таких прикладів можна навести багато, що підтверджує актуальність описаної технології для суспільства зараз і в майбутньому. Водночас блокчейн-технологія здебільшого асоціюється саме з функціонуванням киптовалют.

На сьогодні серед криптовалют другою за ринковою капіталізацією після біткоїну (Bitcoin, BTC) є етер (Ether, ETH)[1], який являє собою нативну валюту децентралізованої платформи Ethereum[2], що призначена для виконання запрограмованих смарт-контрактів (smart contracts) або застосунків. Під смарт-контрактами розуміють угоди у вигляді програмного коду про перерозподіл цінностей між її учасниками-підписантами, в яких заданні однозначні умови, автоматизовані процеси їх виконання та мінімізовано залучення довірених сторін. Комісія за трансакції та обчислення в мережі Ethereum сплачується в етерах (ETH).

Основними відмінностями платформи Ethereum є наявність:

– віртуальних машин (Ethereum virtual machine, EVM) у кожному вузлі мережі Ethereum, які відповідають за обробку стану мережі;

– двох типів аккаунтів: користувача і контракту;

– можливості за допомогою смарт-контрактів емітувати користувацькі токени.

Таким чином, у мережі Ethereum користувачами створюються токени, які можуть бути оцифрованим правом власності на будь-який актив або платіжним засобом (валютою). Для уніфікації застосування різних токенів в Ethereum прийняті стандарти програмування смарт-контрактів, що емітують токени, наприклад для взаємозамінних токенів (Fungible Tokens, FT) – це ERC-20[3] для невзаємозамінних (Non-Fungible Token, NFT) – ERC-721[4]. Всі токени асоційовані з етер-аккаунтом (адресою).

[1] Cryptocurrency Prices // Blockchain.com : сайт. URL: https://www.blockchain.com/explorer/prices (дата звернення: 13.11.2022).

[2] Welcome to Ethereum. URL: https://ethereum.org/ (дата звернення: 13.11.2022).

[3] EIP-20: Token Standard // Ethereum Improvement Proposals : сайт. URL: https://eips.ethereum.org/EIPS/eip-20 (дата звернення: 13.11.2022).

[4] EIP-721: Non-Fungible Token Standard // Ethereum Improvement Proposals : сайт. URL: https://eips.ethereum.org/EIPS/eip-721 (дата звернення: 13.11.2022).

При розслідуванні кримінальних правопорушень, де фігурує етер або етер-токени, вхідним для аналізу є етер-адреси – унікальні публічні ідентифікатори в розподіленій базі даних (блокчейні) Ethereum, з якими асоційовані баланси етер-монет або токенів.

Для створення етер-адреси аккаунту користувача спочатку генерується приватний ключ (private key) у вигляді 64 шістнадцятиричних (hex) символів (0,1,2,…9,a,b,c,d,e,f), за яким з використанням криптографічного алгоритму ECDSA[1] знаходиться публічний ключ (public key). Публічний ключ гешується за алгоритмом Keccak-256[2], і молодші 20 байт отриманого дайджесту стають адресою етер-аккаунту, до якої ще додається hex-префікс «0x». У підсумку адреса представляється рядком із 42 символів, наприклад:

0x06012c8cf97bead5deae237070f9587f8e7a266d,

які в свою чергу можуть бути перетворені у QR-код (рис. 1).

Рис. 1. QR-код етер-аккаунту

Адреса аккаунту контракту зазвичай утворюється під час розгортання контракту в блокчейні Ethereum з адреси автора контракту та кількості трансакцій, надісланих із цієї адреси. Адреса аккаунту контракту також представляється рядком із 42 символів.

В Ethereum одночасно діють головна (mainnet) і тестова (testnet) мережі, для яких формати етер-адрес, на відміну від біткоїн-адрес[3], однакові, що ускладнює їх аналіз щодо належності до відповідної мережі.

Сама етер-адреса нечутлива до регістру, проте зустрічається запис, де літери в адресі записані в різних регістрах після обчислення умовної контрольної суми. Таке представлення було запропоновано у стандарті EIP55[4] (Ethereum Improvement Protocol) для виявлення можливих помилок в адресі при її передачі.

Аккаунт користувача є анонімним і не містить інформації про власника. Один користувач може мати необмежену кількість етер-аккаунтів, створюючи їх кожний раз для отримання коштів. Програмне забезпечення етер-гаманця може оперувати будь-якою кількістю аккаунтів або кожен аккаунт може керуватися окремим гаманцем.

Ethereum трансакції в блокчейні містять такі суттєві для аналізу дані: геш трансакції; статус трансакції; номер блоку, в якому була записана трансакція; кількість блоків із моменту здійснення трансакції; дата і час здійснення трансакції; адреси відправника і отримувача; кількість етерів, що пересилаються; кількість токенів (якщо вони є), що пересилаються; комісія за проведення трансакції тощо. Доступ до блокчейну Ethereum-трансакцій можна отримати через різні вебресурси (etherscan.io, etherchain.org, ethplorer.io тощо), що дозволяє проводити їх аналіз (рис. 2).

На рисунку 2 можна побачити унікальний ідентифікатор трансакції, адресу, з якої були переведені етери, та адресу, на яку вони надійшли. Таким чином можна відслідкувати ланцюг руху коштів від виходу з певної адреси до входу на іншу (інші).

Для ускладнення аналізу в мережі Ethereum руху коштів існують ресурси «етер-мікшування» (наприклад, eth-mixer.com), що за додаткову плату приймають на свою адресу платежі, а потім у довільному порядку відправляють їх за призначенням. Деякі дослідники додатково виділяють серед методів підвищення приватності трансакцій:

– Coinjoin (спільне використання однієї трансакції декількома користувачами, що породжує велику кількість вхідних і вихідних адрес та знижує точність їх кластеризації). Водночас ті ж науковці демонструють методологію виявлення механізму Coinjoin на прикладі клієнту Wasabi Wallet (Tironsakkul et al., 2022b).

– трансакції поза мережею (механізм, який дозволяє користувачам обмінювати криптовалюту поза блокчейном; прикладом такого механізму є застосування протоколу Lightning Network, який дозволяє користувачам створювати

[1] Elliptic Curve Digital Signature Algorithm // Wikipedia : сайт. URL: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm (дата звернення: 13.11.2022).

[2] Team Keccak. URL: https://keccak.team/index.html (дата звернення: 13.11.2022).

[3] What is testnet? How do I avoid testnet Bitcoin scams? // bitpay : сайт. URL: https://support.bitpay.com/hc/en-us/articles/360004102011-What-is-testnet-How-do-I-avoid-testnet-Bitcoin-scams- (дата звернення: 13.11.2022).

[4] EIP-55: Mixed-case checksum address encoding // Ethereum Improvement Proposals : сайт. URL: https://eips.ethereum.org/EIPS/eip-55 (дата звернення: 13.11.2022).

канали та обмінюватися в них криптовалютою з іншими користувачами. Після закриття каналу з його адреси будуть внесені зміни до блокчейну відповідно до кінцевого балансу) (Tironsakkul et al., 2022a).

Вказані інструменти покликані збільшити анонімність користувача відповідної адреси. Для багатьох криптовалютних адрес, зокрема етеру, анонімність втрачається, якщо: в розрахунках криптовалютою зазначаються дійсні ідентифікатори особи; здійснюється купівля криптовалюти за допомогою банківської картки; криптовалюта виводиться з криптобіржі на банківську картку тощо.

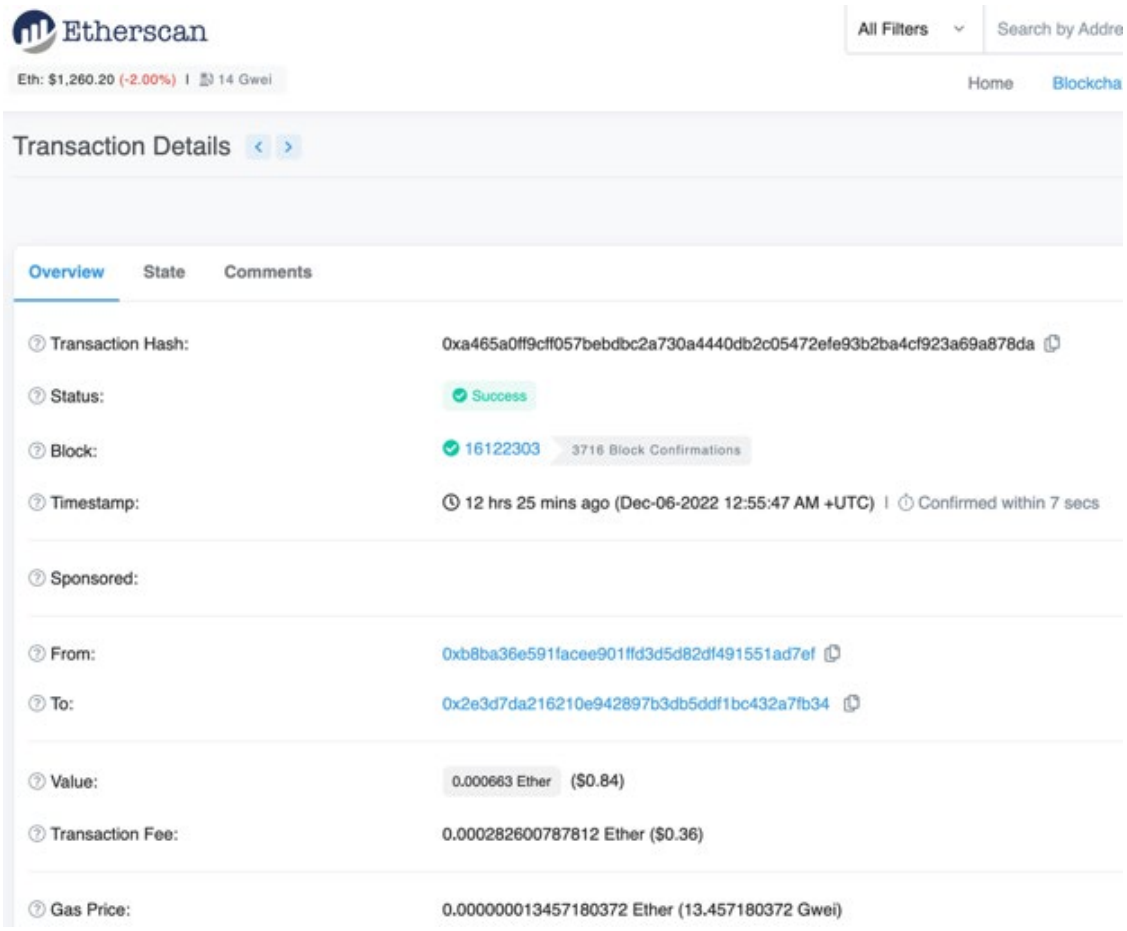

Рис. 2. Вигляд етер-трансакції

Для автоматизації побудови схеми відношень різних ідентифікаторів різних трансакцій можна використати кросплатформенний застосунок Maltego Community Edition (maltego.com) зі встановленим додатково перетворювачем Social Links і отриманим API key з сервісу bloxy.info (рис. 3).

На рисунку 3 видно схему, де облікові записи Ethereum представлені як вузли мережі у мультидіграфі (Lin et al., 2022). Вони пов'язані між собою у випадку наявності відповідних трансакцій, що представлені зваженими ребрами та мітками часу. Однак наведена схема не містить додаткової інформації, яка б допомогла встановити володільця тих або інших етерів та оцінити ризик протиправності конкретних трансакцій і коштів, які в них використовувалися. Враховуючи викладене, для більш глибокого аналізу потрібно застосовувати інструменти для доступу до банків даних, які містять додаткову інформацію про криптогаманці та відповідні трансакції.

Як було нами зазначено в інших роботах (Носов, Манжай, 2021), одним із потужних інструментів аналізу, в тому числі етеріум-трансакцій, є платформа Crystal Expert (crystalblockchain.com), у якій за введеною етер-адресою надається інформація про категорію володільця адреси (сервіс мікшування), поточний баланс, кількість трансакцій, поточний стан, дати першої і останньої активності, величину ризику (Risk Score) щодо ймовірної участі у кримінальній діяльності і кримінального походження коштів (рис. 4).

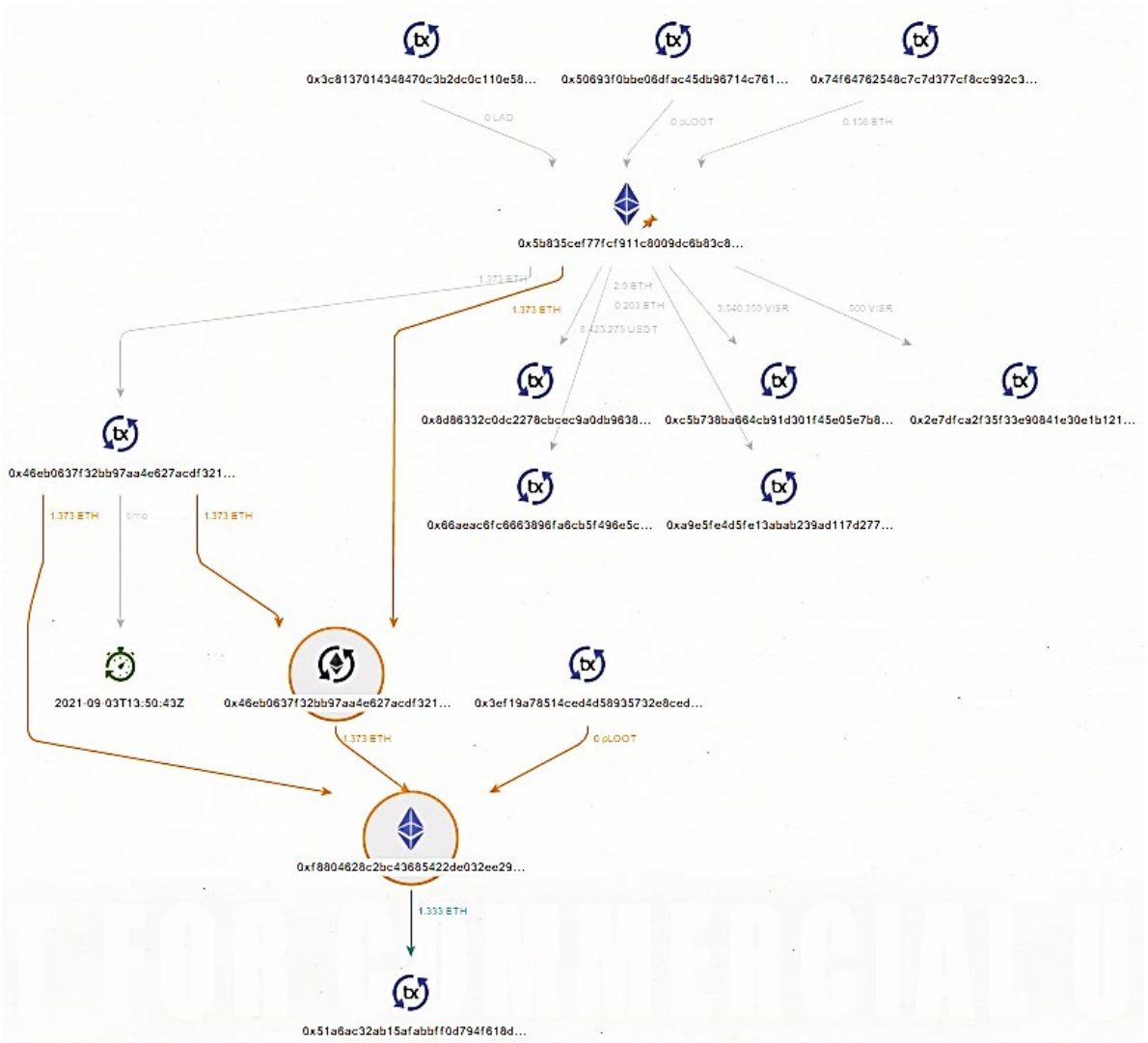

Рис. 3. Приклад побудови логічної схеми трансакцій між етер-адресами в Maltego Community Edition

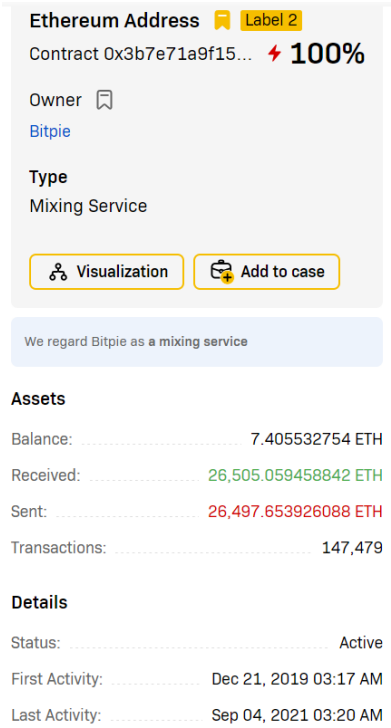

Рис. 4. Інформація про етер-адресу

Також для володільця етер-адреси відображається загальна якісно-кількісна діаграма взаємодії (отримання і відправлення коштів) з іншими ідентифікованими сервісом володільцями етер-адрес із зазначенням величини ризику (рис. 5). Для детального аналізу трансакції виводяться у вигляді переліку (рис. 6).

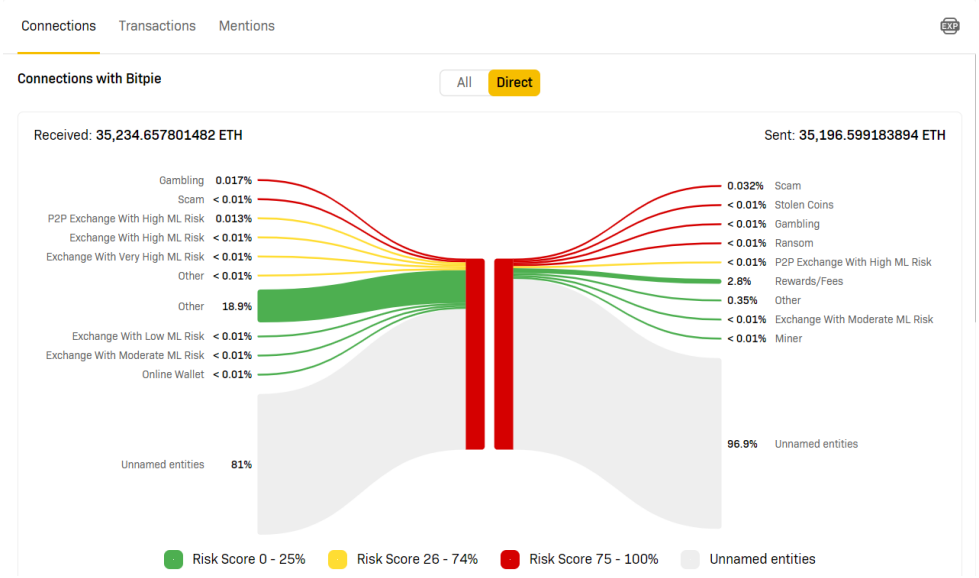

Рис. 5. Якісно-кількісна діаграма взаємодії (отримання і відправлення коштів) етер-адреси з іншими ідентифікованими володільцями етер-адрес

ENTITY	TYPE	RECEIVED, ETH ↓	SENT, ETH ↓	TRANSACTIONS ↓	FIRST INTERACTION ↓	LAST INTERACTION ↓	
Roobet		5.68610484	0	22	Jul 29, 2019 12:31:04 pm	Jul 21, 2020 02:23:43 am	⇄
OKEx		0.503	0	3	Aug 17, 2019 10:08:16 pm	Jul 31, 2020 11:12:22 pm	⇄
Binance		0.2975006	0	10	Jul 22, 2020 08:37:57 am	Aug 13, 2021 11:49:32 am	⇄
Quidax		0.23	0	1	Apr 03, 2020 02:22:57 pm	Apr 03, 2020 02:22:57 pm	⇄
BetHash		0.22286284	0	3	Aug 24, 2020 04:27:54 am	Oct 07, 2020 10:22:55 pm	⇄

Рис. 6. Фрагмент списку трансакцій володільця етер-адреси, що досліджується

Усі трансакції з етер-адресою, що досліджується, можна вивести у вигляді графа (рис. 7). Цільову етер-адресу також можна додати до так званої справи (cases) для подальшого управління розслідуванням у вигляді справи (рис. 8). Сторінка справи містить основні деталі, адреси, візуалізації та відстеження, що додані до справи. В подальшому через розділ «Відстеження (Tracking)» можна відстежувати в часі рух коштів за визначеною трансакцією або групою трансакцій (рис. 9).

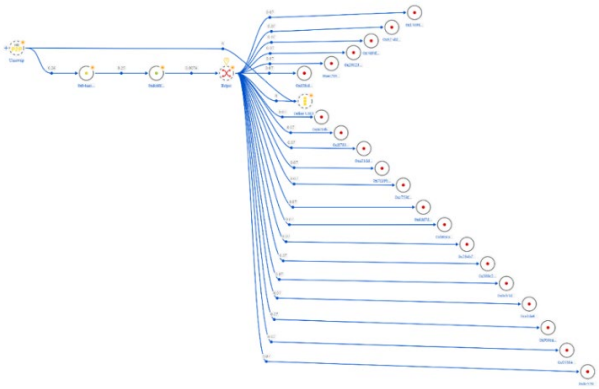

Рис. 7. Візуалізація трансакцій з етер-адресою, що досліджується

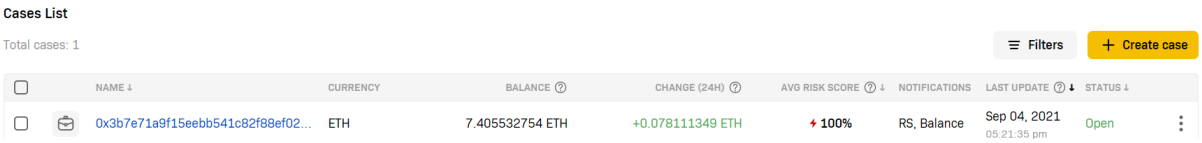

Рис. 8. Поточні записи інструменту «Справи (Cases)»

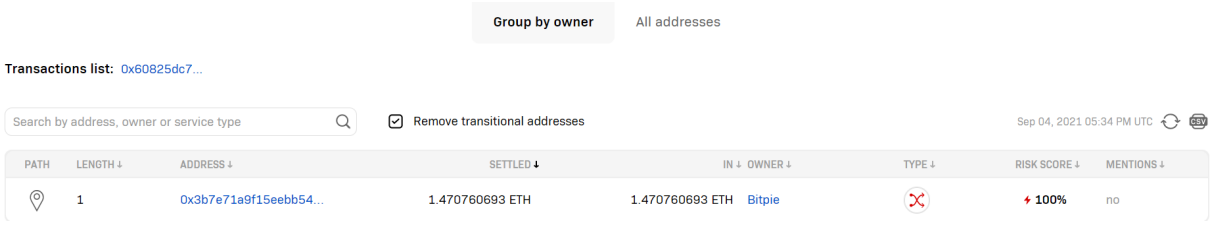

Рис. 9. Фрагмент результатів відстеження визначених трансакцій інструменту «Відстеження (Tracking)»

Аналіз руху етер-токенів інструментами платформи Crystal Expert можна продемонструвати на прикладі етер-адреси: 0x40c02b60db263fca0c8ea59cc35467e5c2c35be2

За наданою адресою інструмент «Дослідник (Explorer)» в розділі «Assets» дає змогу побачити, що у володільця адреси два активи: етер ETH і етер-токен USDT (Tether USD, ERC-20 token), де також можна встановити етер-адресу смарт-контракту (0xdac17f958d2ee523a2206206994597c13d831ec7), який емітував токен USDT (рис. 10).

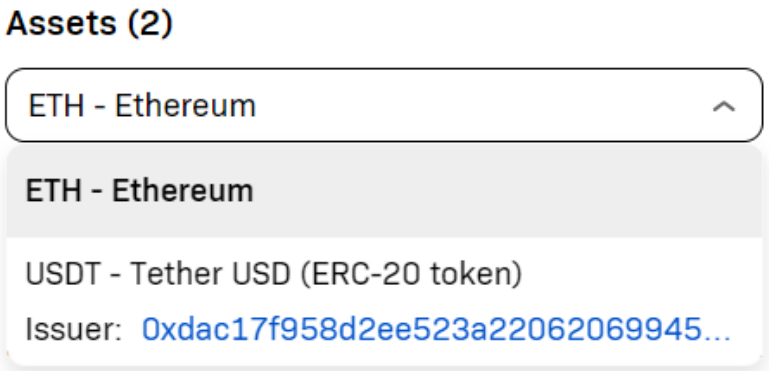

Рис. 10. Фрагмент оцінки інструментом «Дослідник (Explorer)» активів за етер-адресою

Вибір для аналізу етер-токену USDT дозволяє встановити: кількість USDT-трансакцій – 153, отримано – 28395032,992604 USDT, відправлено – 28395032,992604 USDT, поточний баланс – 0 USDT (рис. 11).

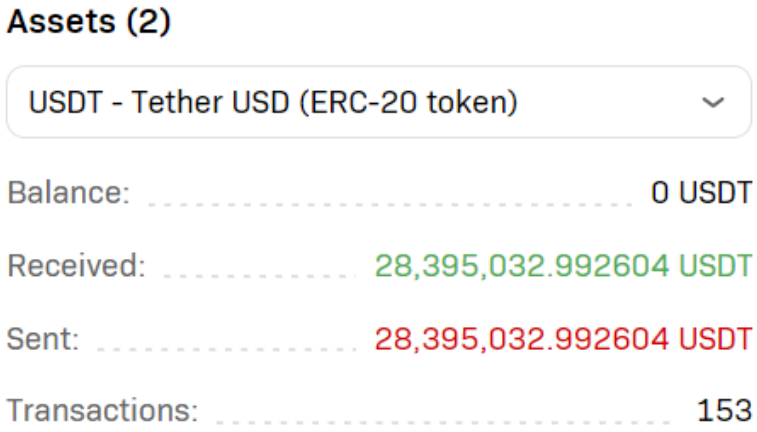

Рис. 11. Фрагмент оцінки інструментом «Дослідник (Explorer)» параметрів USDT-трансакції

Для володільця відповідної адреси відображається загальна якісно-кількісна діаграма взаємодії (отримання і відправлення USDT) з іншими ідентифікованими володільцями адрес із зазначенням величини ризику (рис. 12).

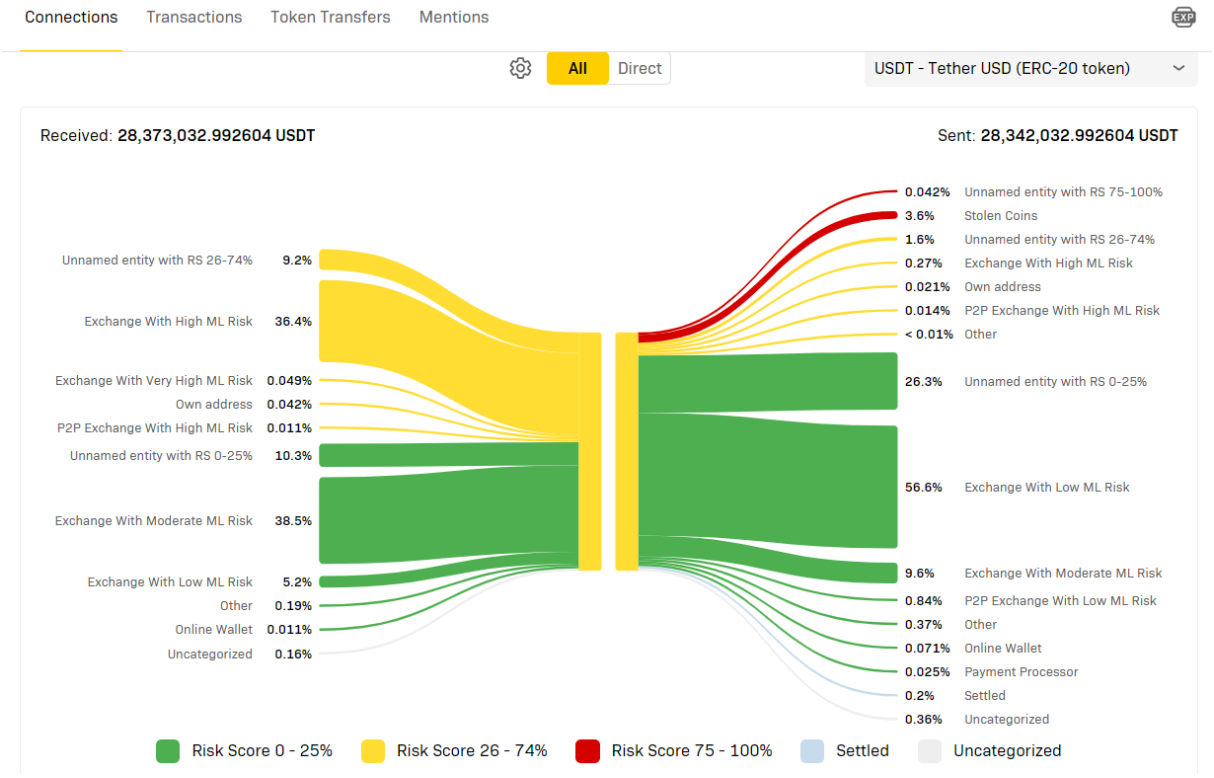

Рис. 12. Якісно-кількісна діаграма взаємодії (отримання і відправлення USDT) вхідної адреси з іншими ідентифікованими володільцями адрес

Також трансакції з діаграми наводяться у вигляді переліку (рис. 13), який дозволяє дослідити детально кожну USDT-трансакцію та вивести ланцюг руху токенів у вигляді графа.

ENTITY	TYPE	RECEIVED, USDT	SENT, USDT	TRANSACTIONS	FIRST INTERACTION	LAST INTERACTION
Huobi		9,743,000	0	16	Feb 26, 2021 02:22:59 pm	Mar 30, 2021 10:30:37 am
WhiteBIT		8,800,100	0	15	Mar 04, 2021 02:57:58 pm	Apr 21, 2021 08:22:07 am
0xc1fcfc24a3e83eac55c...		4,553,712.298072	0	2	Feb 23, 2021 01:21:50 pm	Feb 23, 2021 01:28:19 pm
0x1b8620cea26b408914...		1,982,814	0	7	Feb 26, 2021 12:54:14 pm	Mar 12, 2021 02:46:39 pm
0x56b217cc582e19b3ca...		1,578,175.28932	0	8	Feb 23, 2021 01:22:36 pm	Mar 25, 2021 04:03:25 pm
0xec0a05ef13249a51dc...		630,930	0	4	Apr 13, 2021 08:23:29 am	Apr 13, 2021 02:22:09 pm
0x5cc536b8aa76ea1b14...		456,498	273,882	17	Feb 27, 2021 03:46:20 pm	Apr 09, 2021 10:43:14 am
Binance		316,976.405212	0	6	Mar 01, 2021 08:50:13 am	Apr 19, 2021 02:34:06 pm
0xf7b3fbf66cb8607de0d...		155,750	0	2	Apr 13, 2021 10:37:48 am	Apr 13, 2021 12:15:18 pm
0x9ac79b974446ba0782...		70,000	1,003,018	3	Mar 09, 2021 09:57:26 am	Apr 19, 2021 04:14:10 pm

Рис. 13. Фрагмент переліку USDT-трансакцій володільця адреси, яка досліджується

Таким чином, платформа Crystal Blockchain є доволі ефективним інструментом підтримки аналізу не тільки біткоїн-трансакцій, але й етеріум-трансакцій у розслідуваннях кримінальних правопорушень.

Потенційно під час виконання процедури контрольованого переказу криптовалют для збереження арештованих криптовалютних активів може виникати хибна уява, що криптогаманці містять безпосередньо криптовалюти. Вони містять лише зашифровані приватні і публічні ключі, які дозволяють володільцю витрачати баланси, що асоційовані з відповідними адресами в блокчейні, шляхом формування підписаних приватними ключами трансакцій, в яких також зазначається публічні ключі володільця.

Суттєвим для контрольованого переказу є тип криптогаманця – кастодіальний або некастодіальний. У кастодіальних криптогаманців ключі зберігаються у третьої сторони, у некастодіальних – на носіях володільця. Це означає, що зашифровані ключі кастодіальних криптогаманців можна отримати також у третьої сторони, яка забезпечує роботу криптогаманця. Криптогаманці також можуть бути десктопними, мобільними, апаратними, онлайновими, паперовими. Тобто вид криптогаманця також впливає на методику контрольованого переказу криптовалют.

Для підвищення кваліфікації правоохоронців та відпрацювання процедури контрольованого переказу, наприклад, етеру і етер-токенів доцільно використовувати тестові мережі (testnet). Монети тестових мереж не мають цінності і не можуть використовуватися в реальних трансакціях, їх можна отримати безкоштовно за запитом на так званих сайтах-кранах (faucet), які створюються майнерами або іншими користувачами з надлишком монет у тестовій мережі. Підключення до тестової мережі відповідної криптовалюти здійснюється через звичайний криптогаманець з додатковим параметром –testnet.

Навчальний контрольований переказ на прикладі етер-гаманця MetaMask[1] може виглядати так.

1. Встановлення, підключення до тестової мережі етер-гаманця і отримання етер-токенів

Metamask доступний як розширення для браузера, що діє як етер-гаманець. Користувачі можуть зберігати в ньому ETH і токени ETH, як у будь-якому іншому етер-гаманці. Для встановлення розширення у браузері Chrome і підключення MetaMask до тестової мережі необхідно здійснити такі кроки.

У вебмагазині Chrome знайти MetaMask і встановити розширення від metamask.io (рис. 14).

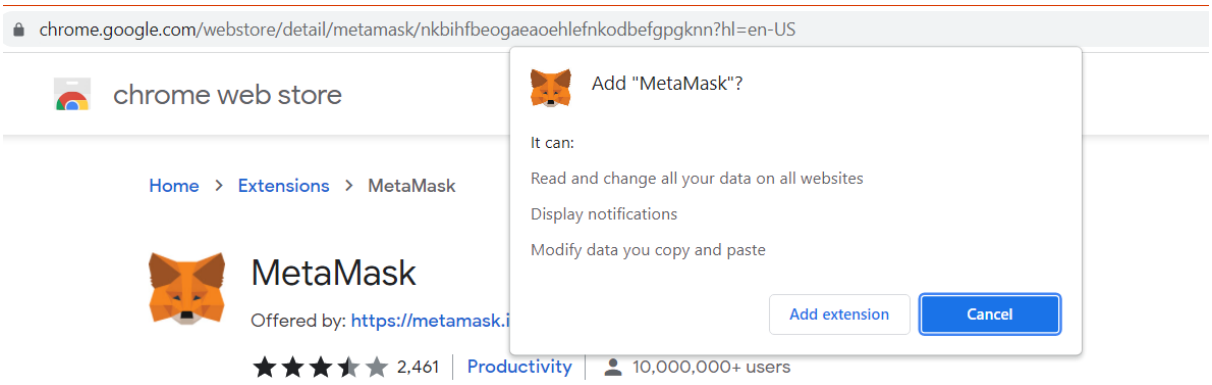

Рис. 14. Встановлення розширення Metamask у Chrome

Після завершення установки відкриється вікно майстра налаштування MetaMask, де слід натиснути «Get Started».

У подальшій роботі з програмою існує два варіанти дій: відновлення ключів доступу «Import wallet» або створення нового гаманця «Create a Wallet» з новими ключами. Відновлення ключів доступу до етер-адрес відбувається через введення seed-фрази, яка може бути написана на папері і зберігатись у будь-якому місці, і паролю, що використовується для шифрування ключів.

У випадку створення нового гаманця слід створити пароль, що використовуватиметься для обмеження доступу до ключів та іншої інформації у MetaMask, та seed-фразу з 12 слів. Seed-фраза дозволить за потреби відновити гаманець на іншому пристрої. Якщо seed-фраза загубиться, отримати доступ буде неможливо.

[1] A crypto wallet & gateway to blockchain apps // METAMASK : сайт. URL: https://metamask.io/ (дата звернення: 13.11.2022).

Створений гаманець MetaMask необхідно приєднати до тестової мережі. MetaMask пропонує декілька тестових мереж за замовчуванням і можливість підключення до будь-яких інших. Для здійснення відповідного вибору у розділі «Settings» – «Advanced» слід увімкнути відображення доступних тестових мереж «Show test networks». Доступні тестові мережі відобразяться під час натискання кнопки «Ethereum Mainnet» (рис. 15).

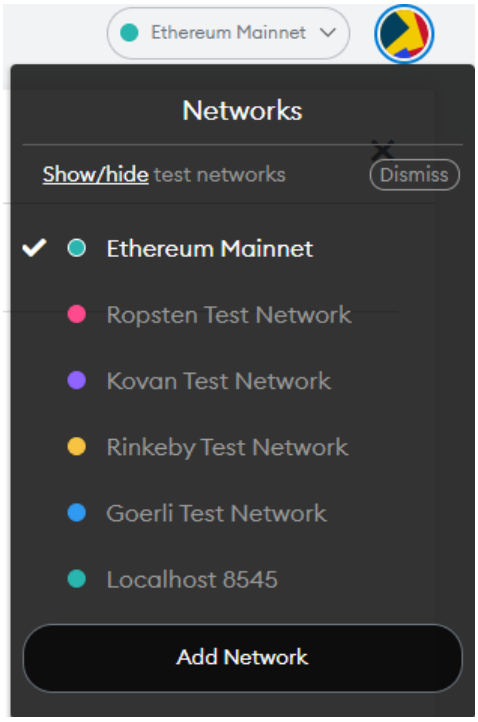

Рис. 15. Доступні тестові мережі в MetaMask

Далі необхідно вручну підключитися до тестової мережі криптобіржі Binance, натиснувши «Add Network» і ввівши:

– Network Name: Binance Smart Chain Testnet або довільне ім'я;

– RPC URL: https://data-seed-prebsc-1-s1.binance.org:8545;

– Chain ID: 97;

– Currency Symbol (не обов'язково): BNB або TBNB;

– Block Explorer URL (не обов'язково): https://testnet.bscscan.com.

Підключення до тестової мережі криптобіржі Binance дозволить отримати етер-токени BNB. Для цього потрібно скопіювати етер-адресу гаманця, натиснувши на адресу або ім'я облікового запису, перейти до крану testnet.binance.org/faucet-smart, вставити у відповідне поле назву етер-адреси гаманця та запитати етер-токени BNB, натиснувши «Give me BNB».

Також можна запитати отримання так званих Peggy tokens, які імітують інші криптовалюти, але попередньо в гаманці MetaMask необхідно на основній сторінці через опцію «Import tokens» ввести адресу смарт-контракту, який емітує відповідний токен. Адресу смарт-контракту можна дізнатися на сторінці крану testnet.binance.org/faucet-smart через відповідний запит у розділі «How does this work?».

Після отримання токенів їх баланс буде відображений на основній сторінці MetaMask.

2. Імітація контрольованого переказу етер-токенів

Через розділ My accounts в MetaMask потрібно створити ще один обліковий запис – Account 2 та скопіювати його етер-адресу.

В Account 1 кликнути на етер-токен, що буде переказуватись, і далі на значок «Send», після чого вставити у відповідне поле етер-адресу Account 2, ввести суму переказу і підтвердити переказ.

Оскільки в MetaMask відповідним налаштуванням можна приховати відображення визначених токенів, то доцільно перевірити, що всі токени із цієї цільової етер-адреси були переказані на контрольовану етер-адресу через огляд цільової етер-адреси у блокчейні. Для цього потрібно натиснути на значок меню поруч з назвою облікового запису (три вертикальні крапки) на головній сторінці MetaMask і обрати «View Account in Explorer», після чого на сайті https://testnet.bscscan.com/ переконатися, що всі токени цільової етер-адреси були переказані (рис. 16).

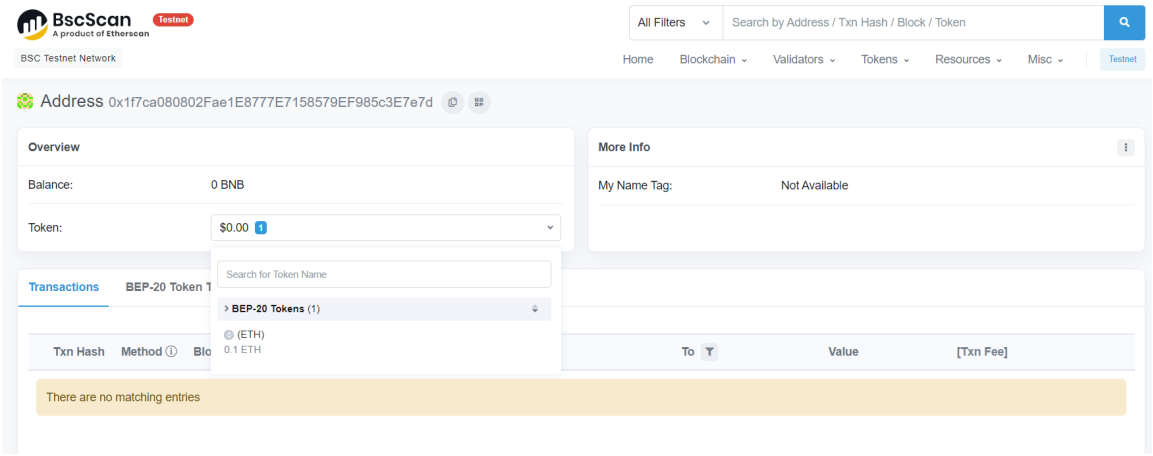

Рис. 16. Перегляд інформації у блокчейні про баланс по всіх токенах етер-адреси

Кожний токен, знайдений у цільовому гаманці, необхідно переказувати окремо на контрольовану етер-адресу.

Контрольований переказ криптовалюти і токенів із мобільних гаманців відбувається приблизно таким же чином, як і з десктопних, але є деякі нюанси. По-перше, зазвичай може знадобитися або пароль, або seed-фраза. По-друге, введення контрольованої адреси краще робити через сканування смартфоном, де встановлений мобільний гаманець, QR-коду цієї адреси. Представлення адреси у вигляді QR-коду є стандартною функцією більшості гаманців, якщо ж вона відсутня, то в мережі є велика кількість онлайн-ресурсів кодування довільного рядка у QR-код (наприклад, https://www.qr-code-generator.com/).

Контрольований переказ криптовалюти і токенів з апаратних гаманців залежить від його моделі, але принцип залишається тим самим. Як правило, апаратні гаманці підключаються через USB-інтерфейс до десктопних гаманців, які лише зчитують відповідні приватні ключі для формування трансакцій.

Паперові етер-гаманці у найпростішому варіанті являють собою надруковані на папері відомості про етер-адресу і приватний ключ для підпису трансакцій, які додатково представлені у вигляді QR-кодів для полегшення їх зчитування (рис. 17). Генерація етер-адреси і приватного ключа здійснюється будь-яким призначеним для цього застосунком.

Рис. 17 Приклад паперового етер-гаманця

Використання такого паперового етер-гаманця відбувається таким чином. Для отримання переказів коштів етер-адреса зчитується сканером QR-кодів і поширюється. Для витрати коштів приватний ключ зчитується сканером QR-кодів та імпортується в будь-який етер-гаманець, який підтримує функцію імпорту етер-аккаунту з іншого гаманця через приватний

ключ. Наприклад, таку функцію підтримує мультивалютний криптогаманець enkrypt[1].

У більш складному варіанті (рис. 18) застосунок генерації паперового етер-гаманця може друкувати на папері: етер-адресу; парольну фразу; зміст файлу у форматі «json», який містить шифртекст приватного ключа і параметри шифрування; назву файлу json. Додатково етер-адреса і зміст файлу у форматі «json» представлені QR-кодами.

Рис. 18. Приклад паперового етер-гаманця із зашифрованим приватним ключем

У цьому випадку для витрати коштів сканером QR-кодів зчитується зміст файлу у форматі «json» і зберігається. Далі в тому ж застосунку в середовищі Java використовується зчитаний json-файл і введена парольна фраза для розшифрування приватного ключа. Потім відбувається формування трансакції переказу на зазначену етер-адресу. З огляду на це методика контрольованого переказу з паперового етер-гаманця залежить від виду подання приватного ключа на папері.

Якщо є підстави вважати, що гаманець – кастодіальний, то правоохоронним органам слід заздалегідь спланувати контрольований переказ, оскільки вилучення токенів безпосередньо з гаманця може виявитися непростим завданням. Для цього слід звернутися до адміністрації платформи, яка підтримує кастодіальний гаманець, щоб заморозити обліковий запис і отримати максимальну інформацію про користувача гаманця (адреса електронної пошти, IP-адреси підключень тощо). Слід взяти до уваги, що практично всі кастодіальні гаманці (особливо на криптовалютних платформах) містять особисту інформацію про своїх користувачів. Принаймні вони зможуть поділитися адресами електронної пошти та журналами IP-адрес.

Описані інструменти аналізу та навчання не є вичерпними, проте за їх допомогою можна зрозуміти загальні підходи до проведення відповідного аналізу й арешту криптовалют. Також варто наголосити на необхідності врахування сучасних наукових розробок щодо аналізу криптовалютних трансакцій, які можуть допомогти в розслідуванні злочинів. У цьому контексті слід згадати методи: виявлення ключових злочинних угруповань та гаманців, запропонований М. Паке-Клустоном, Б. Хаслгофером та Б. Дюпоном (2019), ідентифікації випадків відмивання коштів з використанням криптовалют (Zhong et al., 2022; Alotibi et al., 2022), додаткового профілювання адреси (Tironsakkul et al., 2022b), попередження протиправної поведінки на торговій етер-платформі (Zhou, Yan, Zhang, 2022) тощо.

ВИСНОВКИ. Оскільки криптовалюта продовжує розвиватися, вкрай важливо, щоб працівники правоохоронних органів України були обізнані у сфері технології блокчейн, знали,

[1] A multichain crypto wallet // encrypt : сайт. URL: https://www.enkrypt.com (дата звернення: 13.11.2022).

що це таке, та які засади використання та функціонування криптовалют. На сьогодні національне законодавство у сфері криптовалютного регулювання перебуває в процесі становлення. Базовим законом, на підставі якого відбуватиметься розвиток відповідної нормативно-правової бази, ймовірно стане Закон України «Про віртуальні активи», який, утім, не набуде чинності до внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами.

Серед ключових проблемних моментів поводження з криптовалютами варто виділити проблеми, пов'язані з арештом криптовалютних активів у кримінальному процесі, недостатність знань і навичок у правоохоронних органів і судового корпусу щодо роботи з криптовалюними активами, відсутність сталих процедур криміналістичного дослідження криптовалют.

Другою за капіталізацією криптовалютою є етер, що визначає її популярність серед користувачів. Тому в роботі розкриті структура й особливості обігу криптовалюти етер та проаналізовані окремі інструменти, які дозволяють візуалізувати й аналізувати криптовалютні трансакції в мережі Ethereum. З метою навчання правоохоронців проведенню потенційного арешту криптовалюних активів запропоновано використовувати так звані тестові мережі. На прикладі криптовалюти етер пропонується процедура контрольованого переказу криптовалютних активів для кастодіальних і некастодіальних гаманців.

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. Alotibi J., Almutanni B., Alsubait T., Alhakami H., Baz A. Money Laundering Detection using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*. 2022. Vol. 13, Iss. 10. Pp. 732–738. DOI: https://doi.org/10.14569/IJACSA.2022.0131087.
3. Bryans D. Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*. 2014. No. 89 (1). Pp. 441–472.
4. Hendrickson J. R., Luther W. J. Cash, crime, and cryptocurrencies. *The Quarterly Review of Economics and Finance*. 2022. Vol. 85. Pp. 200–207. DOI: https://doi.org/10.1016/j.qref.2021.01.00.
5. Lin D., Wu J., Xuan Q., Tse C. K. Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction. *Physica A: Statistical Mechanics and its Applications*. 2022. Vol. 600. DOI: https://doi.org/10.1016/j.physa.2022.127504.
6. Marchant G. E. Emerging Technologies and the Courts. *Court Review*. 2019. Vol. 55, Iss. 4. Pp. 146–153.
7. Paquet-Clouston M., Haslhofer B., Dupont B. Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*. 2019. Vol. 5, Iss. 1. DOI: https://doi.org/10.1093/cybsec/tyz003.
8. Paschal Mgembe I., Ladislaus Msongaleli D., Chaundhary N. K. Progressive Standard Operating Procedures for Darkweb Forensics Investigation // 10th International Symposium on Digital Forensics and Security (Istanbul, Turkey, 22 June 2022). Istanbul, 2022. DOI: https://doi.org/10.1109/ISDFS55398.2022.9800830.
9. Taylor S. K., Ariffin A., Zainol Ariffin K. A., Sheikh Abdullah S. N. H. Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets // 3rd International Cyber Resilience Conference (Langkawi Island, Malaysia, 29–31 January 2021). Langkawi Island, 2021. DOI: https://doi.org/10.1109/CRC50527.2021.9392446.
10. Taylor S., Kim S. H.-Y., Zainol Ariffin K. A., Sheikh Abdullah S. N. H. A comprehensive forensic preservation methodology for crypto wallets. *Forensic Science International: Digital Investigation*. 2022. Vol. 42–43. DOI: https://doi.org/10.1016/j.fsidi.2022.301477.
11. Tironsakkul T., Maarek M., Eross A., Just M. Context matters: Methods for Bitcoin tracking. *Forensic Science International: Digital Investigation*. 2022a. Vol. 42–43. DOI: https://doi.org/10.1016/j.fsidi.2022.301475.
12. Tironsakkul T., Maarek M., Eross A., Just M. The Unique Dressing of Transactions: Wasabi CoinJoin Transaction Detection // EICC '22: Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference. 2022b. Pp. 21–28. DOI: https://doi.org/10.1145/3528580.3528585
13. Trozze A., Davies T., Kleinberg B. Explaining prosecution outcomes for cryptocurrency-based financial crimes. *Journal of Money Laundering Control*. 2022. Vol. 26. No. 1. DOI: https://doi.org/10.1108/JMLC-10-2021-0119.
14. Wu H., Zheng G. Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Security Review*. 2020. Vol. 36. DOI: https://doi.org/10.1016/j.clsr.2020.105401.
15. Yadav S. K., Sharma K., Kumar C., Arora A. Blockchain-based synergistic solution to current cybersecurity frameworks. *Multimedia Tools and Applications*. 2022. Vol. 81, Iss. 25. DOI: https://doi.org/10.1007/s11042-021-11465-z.

16. Zhong Z., Zhu C., Yang Y., Liao X., Wang R., Zhao Y., Zhou F., Shi R., Qin Z. Money Laundering Detection for Cryptocurrency Transactions. *Journal of Hunan University Natural Sciences*. 2022. Vol. 49, Iss. 10. Pp. 119–129. DOI: https://doi.org/10.16339/j.cnki.hdxbzkb.2022288.

17. Zhou J., Yan S., Zhang J. Prediction and analysis of illegal accounts on Ethereum based on Catboost algorithm // International Conference on Big Data, Information and Computer Network (Sanya, China, 20–22 January 2022). Sanya, 2022. Pp. 63–67. DOI: https://doi.org/10.1109/BDICN55575.2022.00020.

Надійшла до редакції: 16.11.2022

Прийнята до опублікування: 18.12.2022

REFERENCES

1. Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H., & Baz, A. (2022). Money Laundering Detection using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*, *13*(10), 732-738. https://doi.org/10.14569/IJACSA.2022.0131087.

2. Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal, 89*(1), 441-472.

3. Hendrickson, J. R., & Luther, W. J. (2022). Cash, crime, and cryptocurrencies. *The Quarterly Review of Economics and Finance, 85*, 200-207. https://doi.org/10.1016/j.qref.2021.01.004.

4. Lin, D., Wu, J., Xuan, Q., & Tse, C. K. (2022). Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction. *Physica A: Statistical Mechanics and its Applications, 600*. https://doi.org/10.1016/j.physa.2022.127504.

5. Marchant, G. E. (2019). Emerging Technologies and the Courts. *Court Review, 55*(4), 146-153.

6. 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.

7. Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz003.

8. Paschal Mgembe, I., Ladislaus Msongaleli, D., & Chaundhary, N. K. (2022, June 22). *Progressive Standard Operating Procedures for Darkweb Forensics Investigation* [Conference presentation abstract]. 10th International Symposium on Digital Forensics and Security, Istanbul, Turkey. https://doi.org/10.1109/ISDFS55398.2022.9800830.

9. Taylor, S. K., Ariffin, A., Zainol Ariffin, K. A., & Sheikh Abdullah, S. N. H. (2021, January 29-31). *Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets* [Conference presentation abstract]. 3rd International Cyber Resilience Conference, Langkawi Island, Malaysia. https://doi.org/10.1109/CRC50527.2021.9392446.

10. Taylor, S., Kim, S. H.-Y., Zainol Ariffin, K. A., & Sheikh Abdullah, S. N. H. (2022). A comprehensive forensic preservation methodology for crypto wallets. *Forensic Science International: Digital Investigation, 42-43*. https://doi.org/10.1016/j.fsidi.2022.301477.

11. Tironsakkul, T., Maarek, M., Eross, A., & Just, M. (2022a). Context matters: Methods for Bitcoin tracking. *Forensic Science International: Digital Investigation*, *42-43*. https://doi.org/10.1016/j.fsidi.2022.301475.

12. Tironsakkul, T., Maarek, M., Eross, A., & Just, M. (2022b). *The Unique Dressing of Transactions: Wasabi CoinJoin Transaction Detection* [Conference presentation abstract]. EICC '22: Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference. https://doi.org/10.1145/3528580.3528585.

13. Trozze, A., Davies, T., & Kleinberg, B. (2022). Explaining prosecution outcomes for cryptocurrency-based financial crimes. *Journal of Money Laundering Control, 26*(1). https://doi.org/10.1108/JMLC-10-2021-0119.

14. Wu, H., & Zheng, G. (2020). Electronic evidence in the blockchain era: New rules on authenticity and integrity. *Computer Law & Security Review, 36*. https://doi.org/10.1016/j.clsr.2020.105401.

15. Yadav, S. K., Sharma, K., Kumar, C., & Arora, A. (2022). Blockchain-based synergistic solution to current cybersecurity frameworks. *Multimedia Tools and Applications, 81*(25). https://doi.org/10.1007/s11042-021-11465-z.

16. Zhong, Z., Zhu, C., Yang, Y., Liao, X., Wang, R., Zhao, Y., Zhou, F., Shi, R., & Qin, Z. (2022). Money Laundering Detection for Cryptocurrency Transactions. *Journal of Hunan University Natural Sciences*, *49*(10), 119-129. https://doi.org/10.16339/j.cnki.hdxbzkb.2022288.

17. Zhou, J., Yan, S., & Zhang, J. (2022, January 20-22). *Prediction and analysis of illegal accounts on Ethereum based on Catboost algorithm* [Conference presentation abstract]. International Conference on Big Data, Information and Computer Network, Sanya, China. https://doi.org/10.1109/BDICN55575.2022.00020.

Received the editorial office: 16 November 2022

Accepted for publication: 24 December 2022

ВИТАЛИЙ ВИКТОРОВИЧ НОСОВ,
кандидат технических наук, доцент,
Харьковский национальный университет внутренних дел,
кафедра противодействия киберпреступности;
ORCID: https://orcid.org/0000-0002-7848-6448,
e-mail: vitnos.g@gmail.com;

АЛЕКСАНДР ВЛАДИМИРОВИЧ МАНЖАЙ,
кандидат юридических наук, доцент,
Харьковский национальный университет внутренних дел,
кафедра противодействия киберпреступности;
ORCID: https://orcid.org/0000-0001-5435-5921,
e-mail: sofist@ukr.net;

ЕВГЕНИЙ ВИКТОРОВИЧ ПАНЧЕНКО,
Национальная полиция Украины,
Департамент кибеполиции,
4-е управление (опертивно-аналитического обеспечения
и анализа открытых источникв);
ORCID: https://orcid.org/0000-0001-5755-7457,
e-mail: panch.evg@gmail.com

АНАЛИЗ ЭТЕРИУМ-ТРАНСАКЦИЙ ВО ВРЕМЯ ПРЕДУПРЕЖДЕНИЯ И РАССЛЕДОВАНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ

Предложен механизм анализа этериум-трансакций при предупреждении и расследовании уголовных правонарушений на основе изучения современного опыта в этой сфере. Изучено состояние нормативно правового урегулирования криптовалют в Украине. Затронут вопрос невозможности наложения ареста на криптовалютные активы в ходе уголовного расследования. Намечены проблемные моменты, с которыми сталкиваются правоохранительные органы в других странах при наложении ареста на криптовалюты. Раскрыты структура и особенности обращения криптовалюты этер. Путем эксперимента произведена оценка некоторых программных инструментов, используемых для анализа этериум-трансакций. Продемонстрированы автоматизация поиска и построение схемы отношений различных идентификаторов эфиров на примере Maltego Community Edition и Crystal Expert. Описано значение проведения эффективного анализа криптовалют для проведения расследования. Раскрыта техническая сторона обучения правоохранителей по изъятию криптовалютных активов. Предложен механизм контролируемого перевода криптовалютных активов для кастодиальных и некастодиальных кошельков.

Ключевые слова: *криптовалюта, эфир, ethereum, криптовалютные трансакции, блокчейн, правоохранительные органы, противодействие преступности.*

VITALII VICTOROVICH 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, Associate Professor,
Kharkiv National University of Internal Affairs,
Department of Cybercrime Combating;
ORCID: https://orcid.org/0000-0001-5435-5921,
e-mail: sofist@ukr.net;

YEVHENII VICTOROVYCH PANCHENKO,
National Police of Ukraine,
Cyberpolice Department,
4th Department (operational and analytical
support and analysis of open sources);
ORCID: https://orcid.org/0000-0001-5755-7457,
e-mail: panch.evg@gmail.com

ANALYSIS OF ETHEREUM TRANSACTIONS DURING THE PREVENTION AND INVESTIGATION OF CRIMINAL OFFENSES

The mechanism of Ethereum transactions analysis during the prevention and investigation of criminal offenses based on the study of modern experience in this area has been proposed. The directions of cryptocurrency use by offenders have been revealed. The relationship between the decrease of the cash market and the increase in the use of cryptocurrencies has been described. The state of legal regulation of cryptocurrencies in Ukraine has been studied. The insufficient regulation of the issue of handling cryptocurrencies in criminal proceedings has been emphasized. The issue of impossibility to seize cryptocurrency assets during criminal investigation has been raised. The problematic issues faced by law enforcement agencies in other countries when seizing cryptocurrencies have been outlined.

The structure and peculiarities of the cryptocurrency Ethereum circulation have been revealed. The features of the Ethereum platform and its distinctive features have been studied. The key standards that characterize the work of the Ethereum platform have been analyzed, explanations of key terms have been provided. The essential data in the blockchain for analysis have been highlighted, the procedure for accessing the Ethereum blockchain transactions has been described. Various web resources which one can access the Ethereum transaction blockchain through have been provided.

The purpose of email mixing, the conditions under which the anonymity of the email address is lost have been revealed. Some software tools used to analyze ethereum transactions have been evaluated by experiment. Automation of searching and building a schema of relations of different identifiers of e-transactions on the example of Maltego Community Edition and Crystal Expert have been demonstrated. Additional modules that need to be installed in Maltego Community Edition to analyze the relevant transactions effectively have been described.

It has been emphasized that when analyzing ethereum transactions, it is necessary to use not only ready-made tools, but also various scientific methods, such as identifying key criminal groups and wallets, identifying cases of money laundering using cryptocurrencies, additional address profiling, prevention of illegal behavior on the trading ethereum platform. The importance of effective analysis of cryptocurrencies for investigation has been described. The effectiveness of the Crystal Blockchain platform as a tool for analyzing Ethereum transactions in criminal investigations has been evaluated. The technical side of law enforcement training on the seizure of cryptocurrency assets has been revealed. For this purpose, it is recommended to use the so-called test networks. The mechanism of controlled transfer of cryptocurrency assets for custodial and non-custodial wallets has been proposed.

Key words: *cryptocurrency, Ethereum, cryptocurrency transactions, blockchain, law enforcement agencies, combating crime.*

Цитування (ДСТУ 8302:2015): 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.

Citation (APA): 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.