

Криптовалюта як об'єкт дослідження судової комп'ютерно-технічної експертизи

Андрій Дереча

судовий експерт, Науково-дослідний центр судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України, м. Київ, Україна,
e-mail: derechaandrej@gmail.com

Руслан Мірошник

судовий експерт, Науково-дослідний центр судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України, м. Київ, Україна,
e-mail: rus_miroshnik@ukr.net

Дмитро Хівренко

судовий експерт, Науково-дослідний центр судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України, м. Київ, Україна,
e-mail: dimankhivrenko@gmail.com

Розглянуто новий вид об'єктів судової експертизи — криптовалюту. Наведено визначення поняття терміна «криптовалюта», сучасний стан криптовалюту в різних аспектах. Розглянуто методичні питання дослідження криптовалюту.

Ключові слова: криптовалюта; судова комп'ютерно-технічна експертиза; Blockchain; майнінг; біткоїн.

Cryptocurrency as an Object of Forensic Computer Technical Examination

Andrii Derecha, Ruslan Miroshnyk, Dmytro Khivrenko

The article considers a new type of forensic examination object — cryptocurrency. The definition of the term “cryptocurrency” is given, the current state of cryptocurrency in various aspects is given. Methodological issues of forensic examination of cryptocurrency are considered.

Keywords: cryptocurrency; forensic computer-technical examination; blockchain; mining; bitcoin.

Сучасна світова спільнота характеризується всеохопним проникненням комп'ютерно-інформаційних технологій у різні галузі діяльності: соціальну, економічну, управлінську та ін. Комп'ютеризація в Україні зумовила розвиток ринку комп'ютерів і програмного забезпечення, збільшення потреб установ та організацій у застосуванні комп'ютерних технологій, підвищення професійної підготовки користувачів тощо. Водночас відбу-

вається застосування сучасних інформаційних технологій, програмних і програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання для скоєння високотехнічних злочинів щодо викрадення персональних даних, коштів із рахунків, конфіденційної та комерційної інформації.

Одним із ефективних засобів боротьби зі злочинністю у сфері сучасних інформаційних технологій

є залучення судових експертів із проведення судових комп'ютерно-технічних експертиз.

Методики проведення судових комп'ютерно-технічних експертиз сьогодні перебувають на стадії активного розвитку відповідно до потреб судово-правоохоронної діяльності у сфері злочинів, пов'язаних з комп'ютерами та програмними продуктами.

Так, одним із актуальних напрямів діяльності судових експертів є дослідження, пов'язані з таким об'єктом, як криптовалюта. Як відомо, у процесі стрімкого розвитку інформаційних технологій періодично з'являються нові інструменти управління економікою, поміж яких електронні гроші, що зумовлює появу на ринку аналогу традиційних валют — криптовалют, яка здобуває дедалі більшого поширення в Україні й інших економічно розвинених країнах. Фахівці Науково-дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності й Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» розробляють методичні рекомендації з дослідження транзакцій у криптовалютних системах під час проведення комп'ютерно-технічної експертизи.

Дослідження транзакцій у криптовалютних системах у межах комп'ютерно-технічної експертизи набуває особливої актуальності в сучасних умовах, коли обсяги застосування цифрових активів і *Blockchain*-технологій день у день збільшуються. Із поширенням криптовалют (таких, як

Bitcoin, *Ethereum* та ін.) виникають нові можливості для фінансових операцій, які водночас створюють нові виклики для правоохоронних органів і експертів. У зв'язку з анонімністю та децентралізованим характером криптовалют, їх дедалі частіше застосовують для відмивання грошей, фінансування тероризму, кіберзлочинів та інших незаконних дій. Це потребує від спеціалістів з комп'ютерно-технічної експертизи розробляти нові методи й підходи до аналізу та відстеження криптовалютних транзакцій. Розвиток нових технологічних рішень і алгоритмів аналізу даних дає змогу фахівцям ефективніше виявляти підозрілі активності, аналізувати зв'язки між транзакціями й визначати реальних бенефіціарів, які ховаються за цифровими адресами. Ця робота є критично важливою не тільки для розслідування конкретних злочинів, а й для стримування поширення незаконної діяльності загалом. Урахування новітніх технологічних рішень та алгоритмів машинного навчання підвищують точність і швидкість аналізу, що загалом сприяє розвитку інструментарію комп'ютерно-технічної експертизи у сфері цифрової економіки [1].

Дослідженню криптовалюти приділяли увагу такі вчені України та закордоння, як О. А. Самойленко та К. В. Тітуніна [2], А. W. Wang [3], P. Franco [4] та ін.

Під час дослідження криптовалюти експерт має визначити: конкретний вид, основні характеристики криптовалюти, її кількість; наявність цього типу криптовалюти свого *Blockchain*,

оскільки криптовалюта завжди ґрунтується на технології *Blockchain*; тип застосованого електронного гаманця; чи брала участь ця криптовалюта в раніше скоєних злочинах (для сплати за незаконні товари та послуги); чи застосовано тіньовий сегмент мережі «Інтернет» під час проведення операцій із криптовалютою; історію операцій із рахунку цього криптовалютного гаманця; приблизну вартість криптовалют у фіатних грошових одиницях на момент дослідження; тип і номер криптогаманця, етап-адреса, до якої прив'язаний криптовалютний гаманець; криптовалютні адреси, які взаємодіють з криптогаманцем власника; реальні дані про власника криптовалютного гаманця тощо.

У деяких випадках криміналістично значущі обставини можна визначити лише шляхом призначення та проведення комплексної судової комп'ютерно-технічної та економічної експертизи.

Криптовалюта — цифрова або віртуальна валюта, забезпечена криптографією (наприклад, *Bitcoin*, *Ethereum*, *Litecoin*). *Blockchain* — це децентралізована публічна книга, яка записує транзакції через мережу комп'ютерів, до того ж кожна транзакція криптографічно пов'язана з попередньою, утворюючи безпечний і захищений ланцюг. Псевдонімний характер транзакцій *Blockchain* означає, що хоча всі транзакції публічно видно, реальна ідентичність учасників стає невидимою за допомогою криптографічних адрес. На відміну від традиційних банківських рахунків, транзакції криптовалют без-

посередньо не пов'язані з ідентичністю в реальному світі. Відсутність центрального органу ускладнює зусилля для відстеження та заморожування незаконних коштів. Аналізуючи потік транзакцій на *Blockchain*, можна відстежувати рух коштів: простежувати серію транзакцій *Bitcoin* від оплати викупів на кілька адрес. Застосовуючи кластеризацію адрес, можна ідентифікувати кластер, пов'язаний із відомим обміном, що сприяє ідентифікації злочинця.

Групування адрес, які контролює та сама особа, допомагає зв'язати псевдонімичні транзакції. Методи (такі, як *Co-Sendings*), застосовуючи декілька адрес в одній транзакції, допомагають кластеризації. Цифрові гаманці зберігають приватні ключі, необхідні для транзакцій криптовалюти. Витягання даних гаманця з пристроїв передбачає розміщення файлів гаманця або застосування пам'яті для відновлення приватних ключів. Наприклад, на дослідження надано ноутбук підозрюваного; експерт проводить аналіз і виявляє файл гаманця *Bitcoin*. Вилучені приватні ключі дають змогу отримати доступ та відстежувати незаконні кошти. Створення зображень підозрюваних пристроїв забезпечує цілісність даних і дає змогу проводити детальний аналіз. Такі інструменти, як *FTK Imager* та *Encase*, застосовують для візуалізації й аналізу цифрових доказів.

Знаючи правила свого клієнта (англ. KYC), проводять збирання ідентифікаційної інформації користувача, що може пов'язати адреси *Blockchain* з особами в реальності. Наприклад,

у разі виявлення адреси *Bitcoin*, пов'язаної з ринком *Darknet* (із застосуванням для цього *OSINT*), знаходять публікації на форумі, де підозрюваний поділився своєю адресою. Повна інформація запису ринку підтверджує особу підозрюваного.

Такі методи, як пошук форумів, соціальні медіа й ринки *Darknet*, здатні розкрити інформацію про адреси та транзакції криптовалют. Нові методи теги транзакцій *Blockchain*: призначення мітків (наприклад, «викуп», «ринок *Darknet*») до транзакцій на основі походження або призначення може прискорити ідентифікацію підозрілої активності.

Інструменти, які автоматично ідентифікують суб'єкти реального світу, що беруть участь у транзакціях криптовалют на основі адрес і моделей транзакцій, здатні сприяти зв'язку ідентичностей. Операції, які обмінюються однією криптовалютою на інші без посередників, потребують одночасного моніторингу декількох *Blockchains*.

Аналіз коду й журнали транзакцій розумних контрактів (програми самостійного виконання на *Blockchain*) може виявити незаконну діяльність. Наприклад, злочинець розгортає схему Понзі на *Ethereum*. Експерти аналізують код та історію транзакцій контракту, визначивши жертв і кінцеве призначення викрадених фондів. Відстеження руху жетонів, що представляють активи на *Blockchain*, передбачає аналіз відповідної історії транзакцій *Blockchain*.

Платформи аналізу *Blockchain* (Лейналіз, еліптичний, шифротрас)

забезпечують експертам змогу простежити транзакції криптовалют, ідентифікувати підозрілі мережі й адреси кластерів, пов'язані з незаконною активністю.

Цифрові технології в добу криптовалют потребують усебічного розуміння технології *Blockchain* і спеціалізованих методів розслідування. Застосовуючи комбінацію інструментів та методів для аналізу *Blockchain*, вилучення гаманця, адреси атрибуції тощо, експерти можуть розв'язати проблеми, що виникають під час розслідування злочинів, пов'язаних з криптовалютами.

У міру розвитку ринку криптовалют має постійно тривати прогрес у розвитку судової експертизи, що є вирішальним для підтримання безпечної та прозорої фінансової системи. Експерти мають бути адаптивними в умовах постійних змін, застосовуючи новітні технології та методологію для боротьби з мінливою тактикою кіберзлочинців. Завдяки всебічній підготовці, надійним інструментам і глибокому розумінню системи цифрової валюти, судові експерти спроможні ефективно розв'язувати проблеми, спричинені криптовалютними злочинами й допомогати підтримувати цілісність фінансових систем у сучасних умовах цифрових технологій в Україні.

Отже, від результативності проведення судово-експертних досліджень і засобів новітніх комп'ютерних технологій багато в чому залежать ефективність та оперативність розслідування злочинів у сфері комп'ютерних технологій.

З урахуванням важливості та значущості розвитку й удосконалення судової комп'ютерно-технічної експертизи, зокрема, з дослідження криптовалют, пропонуємо вжити таких заходів:

- створювати новітні методики й методичні рекомендації з проведення судових комп'ютерно-технічних експертиз;
- організовувати та проводити науково-практичні конференції, семінари, круглі столи із розгляду процесуальних, організаційних і методичних аспектів судової комп'ютерно-технічної експертизи, особливостей організації та провадження окремих напрямів експертних досліджень, їхніх можливостей і перспектив розвитку;
- започаткувати стажування експертів, які спеціалізуються в галузі судово-комп'ютерної експертизи, із метою підвищення їхньої кваліфікації;
- проводити спільні засідання з експертами-економістами із дослідження криптовалют;
- провадити міжнародну співпрацю щодо транскордонних розслідувань, пов'язаних із криптовалютою;
- посилити матеріально-технічне оснащення судових експертів сучасними комп'ютерними засобами та програмним забезпеченням.

Реалізація зазначених рекомендацій, безумовно, сприятиме подальшому розвитку судової комп'ютерно-технічної експертизи, ефективному й оперативному розкриттю злочинів, отже — захисту прав, свобод і законних інтересів громадян України.

Перелік джерел посилання

1. Derecha L., Bykova T. Formation of new types of forensic expertise. *The place of judicial expertise in criminalistics and judicial process* : International Conference (Chisinau, Oct 04, 2024). 2024. Pp. 43—46.
2. Самойленко О. А., Тітуніна К. В. Типові криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют. *Актуальні питання у сучасній науці*. 2023. № 7 (13). С. 409—420. DOI: 10.52058/2786-6300-2023-7(13)-409-420 (дата звернення: 07.04.2025).
3. Wang A. W. *Crypto Economy: How Blockchain, Cryptocurrency, and Token-Economy Are Disrupting the Financial World*. New York, 2018. 148 p.
4. Franco P. *Understanding Bitcoin: Cryptography, Engineering, and Economics*. Chichester, 2015. 268 p. DOI: 10.1002/9781119019138 (дата звернення: 07.04.2025).