

УДК 343.1:004.738.5:336.74

DOI [https://doi.org/10.36919/3041-1149\(Print\)14.2026.276-281](https://doi.org/10.36919/3041-1149(Print)14.2026.276-281)

І. О. Білинець,

аспірант кафедри кримінального права та процесу,

Державний податковий університет

email: bilinec90@gmail.com

ORCID 0009-0001-0822-7539

ПРОБЛЕМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ОБІГОМ КРИПТОВАЛЮТИ

PROBLEMS OF PRE-TRIAL INVESTIGATION OF CRIMINAL OFFENSES RELATED TO CRYPTOCURRENCY CIRCULATION

У статті досліджено проблемні аспекти досудового розслідування кримінальних правопорушень, пов'язаних з обігом криптовалюти, з урахуванням технологічних особливостей функціонування блокчейн-систем, цифрової природи віртуальних активів і транснаціонального характеру відповідних операцій. Встановлено, що основні труднощі правозастосовної практики зумовлені складністю ідентифікації фактичного власника криптовалютного гаманця, процесуального оформлення результатів блокчейн-аналітики, забезпечення належності, допустимості та достовірності цифрових доказів, а також вилучення, арешту й зберігання криптоактивів. Обґрунтовано доцільність застосування під час доказування «трикутника атрибуції», який охоплює блокчейн-рівень, сервісний рівень та персональний рівень і дає змогу комплексно встановлювати зв'язок між конкретною особою та криптовалютною адресою. Запропоновано запровадити уніфікований протокол блокчейн-аналітичного дослідження із фіксацією технічних параметрів, джерел даних, хешів транзакцій, аналітичних припущень і контрольних хеш-сум сформованих файлів. Доведено потребу в нормативному врегулюванні порядку роботи з приватними ключами, seed-фразами та іншими даними доступу до віртуальних активів, а також створення системи державних криптогаманців із використанням багатопідписного механізму. Запропоновано доповнити кримінальне процесуальне законодавство спеціальною нормою щодо особливостей тимчасового вилучення та зберігання віртуальних активів. Окрему увагу приділено розмежуванню відкритої блокчейн-аналітики й процесуального отримання ідентифікаційних даних від криптовалютних бірж і провайдерів відповідних послуг. Обґрунтовано двоетапний механізм міжнародного одержання даних, що передбачає їхнє невідкладне збереження та подальше процесуальне витребування. Зроблено висновок, що підвищення ефективності досудового розслідування цієї категорії правопорушень потребує стандартизації алгоритмів роботи з цифровими доказами, залучення спеціальних знань і належної міжвідомчої та міжнародної взаємодії.

Ключові слова: криптовалюта, віртуальні активи, досудове розслідування, цифрові докази, блокчейн-аналітика, кримінальне провадження, криптовалютний гаманець.

The article examines problematic aspects of pre-trial investigation of criminal offenses related to cryptocurrency circulation, taking into account the technological features of the functioning of blockchain systems, the digital nature of virtual assets and the transnational nature of the relevant operations. It is established that the main difficulties of law enforcement practice are due to the complexity of identifying the actual owner of a cryptocurrency wallet, the procedural registration of blockchain



analytics results, ensuring the appropriateness, admissibility and reliability of digital evidence, as well as the seizure, arrest and storage of cryptoassets. The feasibility of using the “attribution triangle” during proof is substantiated, which covers the blockchain level, service level and personal level and allows for a comprehensive connection between a specific person and a cryptocurrency address. It is proposed to introduce a unified protocol for blockchain analytical research with the fixation of technical parameters, data sources, transaction hashes, analytical assumptions and checksums of generated files. The need for regulatory regulation of the procedure for working with private keys, seed phrases and other access data to virtual assets, as well as the creation of a system of state crypto wallets using a multi-signature mechanism, is proven. It is proposed to supplement criminal procedural legislation with a special norm on the features of temporary seizure and storage of virtual assets. Special attention is paid to the distinction between open blockchain analytics and procedural receipt of identification data from cryptocurrency exchanges and providers of relevant services. A two-stage mechanism for international data receipt is substantiated, which provides for their immediate storage and subsequent procedural retrieval. It is concluded that increasing the efficiency of pre-trial investigation of this category of offenses requires standardization of algorithms for working with digital evidence, involvement of special knowledge and proper interagency and international cooperation.

Keywords: *cryptocurrency, virtual assets, pre-trial investigation, digital evidence, blockchain analytics, criminal proceedings, cryptocurrency wallet.*

Постановка проблеми та її актуальність. Стрімкий розвиток цифрових технологій, поширення віртуальних активів та активне використання криптовалют у фінансовому обороті істотно трансформують способи вчинення кримінальних правопорушень і водночас ускладнюють діяльність органів досудового розслідування. Криптовалюта дедалі частіше використовується не лише як засіб інвестування чи здійснення розрахунків, а й як інструмент приховування та переміщення активів, одержаних кримінально протиправним способом, фінансування незаконної діяльності, вчинення шахрайства, легалізації доходів, одержаних злочинним шляхом, вимагання, незаконного заволодіння майном, а також інших кримінальних правопорушень, що мають виражений цифровий і нерідко транснаціональний характер.

Суттєвою проблемою залишається специфіка доказування в кримінальних провадженнях, пов'язаних з обігом криптовалюти. Інформація про транзакції, адреси криптовалютних гаманців, приватні та публічні ключі, дані криптовалютних бірж, електронні пристрої, програмні застосунки, відомості блокчейн-мереж та інші цифрові дані потребують не лише своєчасного виявлення, а й належного процесуального оформлення, збереження їх цілісності та забезпечення можливості подальшого використання як доказів. Водночас технологічна складність відповідних об'єктів зумовлює потребу в широкому використанні спеціальних знань, залученні спеціалістів та експертів, застосуванні спеціалізованих програмно-аналітичних засобів і виробленні ефективних алгоритмів взаємодії слідчих, прокурорів, оперативних підрозділів та інших уповноважених суб'єктів. Тому підтримуємо позицію Л. В. Омельчук, В. О. Підгородецького, яка є актуальною і для досліджуваної категорії проваджень, що проблема допустимості цифрових доказів має не фрагментарний, а системний характер і не може бути вирішена виключно за рахунок удосконалення окремих процесуальних процедур, адже йдеться про потребу у формуванні цілісного стандарту поведінки із цифровою інформацією на всіх етапах кримінального провадження – від її виявлення до використання в судовому провадженні [5, с. 159].

Додаткові труднощі виникають у разі, коли криптовалютні операції здійснюються із залученням іноземних платформ, провайдерів або інших суб'єктів, діяльність яких перебуває поза межами юрисдикції України. У таких ситуаціях результативність розслідування значною мірою залежить від швидкості отримання інформації, ефективності міжнародного співробітництва та можливості забезпечити збереження цифрових даних до моменту їхнього процесуального витребування. Висока мобільність цифрових активів створює ризик їхнього оперативного переміщення між різними гаманцями, платформами та юрисдикціями, що може істотно ускладнювати забезпечення завдань кримінального провадження.

Викладене свідчить про наявність комплексної науково-прикладної проблеми, яка полягає в невідповідності між стрімким розвитком технологій використання криптовалют, постійним удосконаленням способів їхнього застосування в кримінально протиправній діяльності та наявними процесуальними й організаційно-тактичними можливостями органів досудового розслідування. Це зумовлює потребу в системному дослідженні проблем досудового розслідування кримінальних правопорушень, пов'язаних з обігом криптовалют, визначення найбільш проблемних аспектів збирання, перевірки й оцінювання цифрових доказів, простеження руху віртуальних активів і розроблення науково обґрунтованих рекомендацій, спрямованих на підвищення ефективності відповідної правозастосовної діяльності.

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання обігу криптовалют, використання віртуальних активів у кримінально протиправній діяльності та особливостей розслідування відповідної категорії кримінальних правопорушень упродовж останніх років привертає дедалі більшу увагу українських науковців. Безпосередньо проблемам розслідування кримінальних правопорушень, учинених із використанням криптовалют, присвячено дослідження Н. А. Лугіної та І. В. Кибиш. У праці «Проблеми розслідування кримінальних правопорушень, що вчиняються у процесі здійснення операцій з криптовалютою» авторами проаналізовано специфіку початку та здійснення кримінального провадження щодо правопорушень, пов'язаних із криптовалютними операціями, звернено увагу на труднощі проведення окремих слідчих (розшукових) дій, зокрема обшуку та допиту, а також на особливості роботи з комп'ютерною технікою та цифровою інформацією [3].

Важливий внесок у дослідження криміналістичних і кримінальних процесуальних аспектів цієї проблематики здійснили Т. П. Яцик та В. А. Шкелебей. Науковцями розглянуто особливості розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів, акцентовано на потребі у використанні спеціальних знань, розвитку технологічного забезпечення правоохоронної діяльності й належної взаємодії органів досудового розслідування з Державною службою фінансового моніторингу України, АРМА та іншими державними інституціями [8].

Окремі проблеми виявлення, вилучення та дослідження криптовалютних активів одержали розвиток у працях В. В. Козія, який дослідив порядок та особливості вилучення незаконно здобутої криптовалют в кримінальному провадженні [1], а також О. А. Самойленко та К. В. Тітуниної, які охарактеризували типові криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют [6].

Предметне значення мають також дослідження К. О. Юсупової, Р. П. Марчука та В. В. Юсупова, в яких розкрито особливості проведення огляду, обшуку, допиту та залучення експерта під час розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют [7]. Водночас О. В. Кузьменко та П. Ю. Кравчук дослідили віртуальні активи як предмет кримінального правопорушення крізь призму проблем їх визначення та доказування, наголосивши, зокрема, на складності встановлення власника криптовалютного гаманця, процесуального поведіння з вилученими криптоактивами й недостатній визначеності відповідних механізмів кримінального провадження [2].

К. В. Мартиненко, досліджуючи організацію розслідування кримінальних правопорушень, пов'язаних із використанням віртуальних активів, обґрунтовує потребу в комплексному криміналістичному підході, який має враховувати специфіку цифрових доказів і блокчейн-транзакцій, можливості спеціалізованих аналітичних інструментів, а також належну взаємодію слідчих, оперативних підрозділів, експертних установ та інших суб'єктів [4].

Метою статті є комплексне дослідження проблем досудового розслідування кримінальних правопорушень, пов'язаних з обігом криптовалют, з урахуванням особливостей функціонування віртуальних активів і цифрового середовища, визначення основних процесуальних, організаційних і тактичних труднощів, що виникають під час виявлення, фіксації, вилучення, дослідження та використання цифрових доказів, встановлення належності криптовалютних гаманців конкретним особам, відстеження руху криптовалютних активів і забезпечення їхнього збереження в кримінальному провадженні.

Виклад основного матеріалу дослідження. Особливість досудового розслідування кримінальних правопорушень, пов'язаних з обігом криптовалюти, полягає в тому, що традиційні процесуальні засоби застосовуються до об'єкта, який існує в розподіленому цифровому середовищі, не має єдиного місця зберігання та може бути переміщений між адресами фактично незалежно від фізичного місцезнаходження особи. Н. А. Лугіна та І. В. Кибиш слушно пов'язують результативність таких проваджень із невідкладністю первинних слідчих дій, належним технічним оснащенням і використанням спеціальних знань [3, с. 38–40].

Першою проблемою є правильне визначення предмета доказування в конкретному провадженні. Сам факт наявності транзакції в блокчейні не доводить ні особу її ініціатора, ні кримінально протиправне походження активу. Псевдонімність адрес дає змогу простежувати рух активів, але не встановлює автоматичного зв'язку між адресою та конкретною фізичною особою. О. В. Кузьменко та П. Ю. Кравчук звертають увагу на труднощі встановлення власника віртуального активу, верифікації цифрових слідів у блокчейні, фіксації та збереження доказів, а також допустимості інформації, одержаної з відкритих джерел чи іноземних платформ [3, с. 195]. Отже, доказування доцільно будувати за принципом «трикутника атрибуції»: 1) блокчейн-рівень – адреси, хеші транзакцій, блоки, час, сума та маршрут руху активу; 2) сервісний рівень – відомості біржі або іншого постачальника послуг про акаунт, KYC-дані, IP-адреси, історію входів, прив'язані банківські реквізити; 3) персональний рівень – дані пристроїв, листування, seed-фрази, паролі, показання, фінансові документи та інші відомості, що підтверджують фактичний контроль над гаманцем.

Другою проблемою є процесуальна форма використання результатів блокчейн-аналітики. Спеціалізоване програмне забезпечення здатне будувати графи транзакцій, кластеризувати адреси, встановлювати зв'язки з відомими сервісами та визначати ризикові маршрути. Однак аналітичний звіт програми не повинен сприйматись як самодостатній доказ лише тому, що його сформовано технічним засобом. О. А. Самойленко та К. В. Тітуніна вказують, що матеріали, одержані за допомогою спеціального програмного забезпечення, можуть використовуватись як матеріали, що доповнюють показання, або як документи чи довідки спеціалістів, долучені до протоколу процесуальної дії [6, с. 418].

У зв'язку з цим пропонуємо запровадити в практику досудового розслідування уніфікований протокол блокчейн-аналітичного дослідження як додаток до відповідної процесуальної дії. У ньому мають обов'язково зазначатися: назва та версія програмного продукту; дата й точний час формування даних; назва блокчейн-мережі; досліджувані адреси; хеші транзакцій; номери блоків; використані критерії пошуку й аналітичні припущення; джерела відомостей про належність адрес певному сервісу; повний експорт результатів; контрольна хеш-сума сформованого файлу. Принципово важливо відмежовувати безпосередньо відтворені дані блокчейну від аналітичних висновків програмного продукту. Перша група може бути повторно перевірена іншим суб'єктом, тоді як друга значною мірою залежить від алгоритмів кластеризації та баз даних конкретного сервісу. Це дає підстави запропонувати правило процесуальної верифікованості, відповідно до якого будь-який висновок блокчейн-аналітики, що істотно впливає на доведення причетності особи, повинен бути відтворюваним або підтвердженням незалежним джерелом.

Третій блок проблем пов'язаний з оглядом, обшуком і вилученням цифрової інформації. Н. А. Лугіна та І. В. Кибиш наголошували на потребі в дослідженні комп'ютерної техніки, засобів зв'язку та використанні спеціальних знань під час таких проваджень [3, с. 38–39]. Новітні дослідження конкретизують цю позицію: під час огляду потрібно фіксувати комп'ютерні дані, що відображають транзакції, а під час виявлення апаратного гаманця чи пристрою з криптододатком – забезпечувати належну участь спеціаліста [7, с. 324]. У протоколах доцільно відображати ідентифікаційні ознаки пристрою, програмне забезпечення, назву та кількість криптовалюти, публічні адреси, хеші транзакцій і час їх проведення, водночас не розголошуючи у відкритій частині протоколу приватні ключі, паролі та мнемонічні фрази [7, с. 325].

На цій основі пропонуємо нормативно закріпити спеціальний порядок роботи з даними доступу до криптоактивів. Його зміст має охоплювати розмежування загального протоколу слідчої (розшукової) дії та конфіденційного додатка, у якому фіксуються приватні ключі, seed-

фрази й інші автентифікаційні дані; обмеження кола осіб, які мають до них доступ; обов'язкове журналювання кожного використання таких даних; негайну зміну контрольованої адреси зберігання в разі ризику компрометації. Такий підхід одночасно забезпечує повноту процесуальної фіксації та мінімізує ризик повторного заволодіння активом унаслідок витоку інформації з матеріалів кримінального провадження.

Також проблемою є фактичне вилучення й подальше зберігання криптовалюти. В. В. Козій обґрунтовує покроковий алгоритм вилучення, що передбачає встановлення доступу до активу, фіксацію стану гаманця й транзакцій, переведення активу на контрольовану правоохоронним органом адресу та збереження приватних ключів [1, с. 481–483]. Водночас О. В. Кузьменко й П. Ю. Кравчук слушно зазначають, що відсутність чіткого правового механізму змушує слідчих і прокурорів ситуативно вирішувати питання вилучення та зберігання криптоактивів [2, с. 194–195].

Тому доцільно створити централізовану систему державних криптогаманців для потреб кримінального провадження, побудовану за принципом multi-signature, коли здійснення транзакції потребує підтвердження декількох уповноважених суб'єктів. Процесуально така модель повинна містити: рішення про переведення активу; фіксацію вихідної та контрольної адрес; хеш транзакції переміщення; курс і кількість активу на момент операції; відомості про осіб, які підтвердили транзакцію; журнал усіх подальших операцій. Вважаємо доцільним доповнити КПК України окремою нормою «Особливості тимчасового вилучення та зберігання віртуальних активів», яка передбачатиме не фізичне «вилучення» криптовалюти, а встановлення юридичного й технічного контролю над можливістю розпорядження нею. Така конструкція точніше відповідає технологічній природі криптовалюти та усуває штучне перенесення на неї правил, розроблених для матеріальних речей.

Наступна проблема стосується співвідношення огляду відкритого блокчейну й отримання даних від криптовалютних бірж. Відкритий характер блокчейну дає змогу слідчому встановлювати рух активів між публічними адресами. Проте дані, які ідентифікують користувача централізованої біржі, є іншою категорією інформації та мають отримуватися в належній процесуальній формі. Т. П. Яцик і В. А. Шкелебей обґрунтовано підкреслюють значення взаємодії правоохоронних органів із Держфінмоніторингом, АРМА та іншими установами, а також використання інформації про підозрілі операції та типології їх виявлення [8, с. 222]. Отже, у методиці розслідування доцільно чітко розмежувати «відкрити блокчейн-розвідку» й «процесуальне отримання ідентифікаційних даних».

Для транскордонних проваджень пропонуємо двоетапний механізм одержання інформації: спочатку – невідкладне забезпечення збереження даних у відповідного провайдера або криптобіржі, а після цього – їхнє одержання у формі, що відповідає вимогам кримінального процесу та міжнародного співробітництва. На організаційному рівні доцільно розробити для органів досудового розслідування типові форми термінових запитів про збереження КУС-даних, IP-логів, історії входів, адрес введення й виведення активів і внутрішніх ідентифікаторів транзакцій. Це дасть змогу відокремити невідкладне забезпечення збереження потенційного доказу від його подальшого процесуального одержання та використання.

Ще однією проблемою є фрагментарність використання спеціальних знань. За висновком К. О. Юсупової, В. В. Юсупова та Р. П. Марчука, успішне розслідування потребує залучення фахівців з інформаційних технологій, блокчейну, фінансового моніторингу та інших спеціалістів [7, с. 322–324]. К. В. Мартиненко також наголошує, що ефективна організація розслідування має поєднувати цифрові інструменти, аналітичні технології та взаємодію слідчих, оперативних підрозділів і експертних установ [4, с. 139–140]. На нашу думку, участь спеціаліста в провадженнях, де планується доступ до криптогаманця, копіювання даних блокчейн-застосунків або переміщення криптоактиву, повинна розглядатися не як факультативна можливість, а як відповідна процесуальна гарантія належності та достовірності одержаних результатів.

Потрібно також чітко розмежувати технічне відтворення загальнодоступних транзакцій; аналітичне встановлення зв'язків між адресами; дослідження пристрою або програмного середовища; вирішення питань, що потребують експертного висновку. Н. А. Лугіна та І. В. Кибиш ще 2022 року звертали увагу на недостатню визначеність кола питань, які мають ставитися перед

експертом у цій категорії проваджень [3, с. 39]. Практичним вирішенням проблеми може бути розроблення міжвідомчих методичних рекомендацій із типовими питаннями до спеціаліста й експерта та чіткими межами їхньої компетенції. Зокрема, встановлення факту існування транзакції, її часу, адрес відправника й отримувача не потребує вирішення правових питань експертом, тоді як дослідження програмного забезпечення, способу отримання доступу до гаманця, відновлення видалених даних або встановлення технічного механізму компрометації ключів може потребувати відповідного експертного дослідження.

Висновок. Основна проблема досудового розслідування кримінальних правопорушень, пов'язаних з обігом криптовалюти, полягає не в «невидимості» цифрових активів, а в недостатній процесуальній стандартизації способів перетворення технічної інформації на належні та перевірювані докази. Сучасний блокчейн, навпаки, формує значний масив стійких даних, придатних для ретроспективного аналізу; складність полягає в їх персоніфікації, процесуальній фіксації та зв'язуванні з іншими доказами [4, с. 144]. Тому перспективним є формування єдиного алгоритму досудового розслідування кримінальних правопорушень, пов'язаних з обігом криптовалюти, який охоплює раннє виявлення криптовалютної складової кримінального правопорушення; невідкладне збереження цифрових даних; блокчейн-аналітичне дослідження; встановлення сервісів та осіб, пов'язаних із відповідними адресами; процесуальне отримання КҮС-даних і логів; проведення огляду й обшуку із залученням спеціаліста; безпечне встановлення контролю над активом; накладення арешту; проведення експертного дослідження; міжнародне співробітництво та подальше вирішення процесуальної долі криптоактиву. Запровадження запропонованих стандартів здатне підвищити не лише оперативність розслідування, а насамперед належність, достовірність і перевірюваність сформованої доказової бази.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Козій В. В. Порядок та особливості вилучення у кримінальному провадженні незаконно здобутої криптовалюти. *Юридичний науковий електронний журнал*. 2023. № 2. С. 479–483.
2. Кузьменко О. В., Кравчук П. Ю. Віртуальні активи як предмет кримінального правопорушення: проблеми визначення та доказування. *Аналітично-порівняльне правознавство*. 2025. № 6, ч. 3. С. 194–198. DOI 10.24144/2788-6018.2025.06.3.29
3. Лугіна Н. А., Кибиш І. В. Проблеми розслідування кримінальних правопорушень, що вчиняються у процесі здійснення операцій з криптовалютою. *Українська поліцейстика: теорія, законодавство, практика*. 2022. № 2 (4). С. 37–41.
4. Мартиненко К. В. Організація розслідування кримінальних правопорушень, пов'язаних із використанням віртуальних активів: проблеми та стан наукових досліджень. *Аналітично-порівняльне правознавство*. 2026. № 2, ч. 3. С. 138–147.
5. Омельчук Л. В., Підгородецький В. О. До питання криміналістичного забезпечення дослідження цифрових (електронних) доказів у кримінальному провадженні. *Європейський правничий часопис*. 2026. № 13. С. 155–161. URL : https://cms.legal-journal.e-u.edu.ua/uploads/13_25_2c1aa5b5d0.pdf
6. Самойленко О. А., Тігуніна К. В. Типові криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют. *Актуальні питання у сучасній науці*. 2023. № 7 (13). С. 409–420.
7. Юсупова К. О., Марчук Р. П., Юсупов В. В. Особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень, пов'язаних з використанням криптовалют. *Аналітично-порівняльне правознавство*. 2025. № 5, ч. 3. С. 322–327. DOI 10.24144/2788-6018.2025.05.3.47
8. Яцик Т. П., Шкелебей В. А. Розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2023. Вип. 80, ч. 2. С. 219–223.

Дата надходження статті: 09.07.2026

Дата прийняття статті: 18.08.2026

Дата публікації статті: 14.09.2026