

**ФІКСАЦІЯ ЦИФРОВИХ СЛІДІВ У БЛОКЧЕЙН-МЕРЕЖАХ:
КРИМІНАЛІСТИЧНІ ТА ПРОЦЕСУАЛЬНІ АСПЕКТИ****CAPTURING DIGITAL TRACES IN BLOCKCHAIN NETWORKS:
FORENSIC AND PROCEDURAL ASPECTS**

**Цимбал П.В., д.ю.н., професор,
завідувач кафедри права,
ПВНЗ «Європейський університет»
orcid.org/0000-0002-7244-4669**

**Кравчук П.Ю., к.ю.н., доцент,
доцент кафедри права,
ПВНЗ «Європейський університет»
orcid.org/0000-0003-4246-974X**

**Малярчук Н.В., к.ю.н.,
доцент кафедри права,
ПВНЗ «Європейський університет»
orcid.org/0009-0000-3397-9807**

Стаття присвячена комплексному дослідженню криміналістичних і процесуальних аспектів фіксації цифрових слідів у блокчейн-мережах у контексті досудового розслідування та судового розгляду кримінальних правопорушень, пов'язаних із використанням криптовалют та технологій розподіленого реєстру. Актуальність теми зумовлена стрімким поширенням блокчейн-технологій у фінансовій та господарській діяльності, що супроводжується зростанням кількості кримінальних правопорушень, у яких цифрові сліди мають нетрадиційну природу, високий рівень технічної складності та транскордонний характер.

Проаналізовано особливості виявлення, фіксації, вилучення, збереження та подальшого аналізу інформації, що міститься у блокчейн-транзакціях, смартконтрактах і пов'язаних метаданих, з урахуванням вимог криміналістичної тактики та процесуальної форми. Особливу увагу приділено використанню спеціальних знань і програмно-аналітичних інструментів для ідентифікації адрес, відстеження руху віртуальних активів і встановлення причинно-наслідкових зв'язків між подіями.

Досліджено доказовий потенціал блокчейн-даних як різновиду електронних доказів, окреслено проблеми їх процесуального оформлення, допустимості та оцінки в умовах чинного кримінального процесуального законодавства України. Виявлено прогалини та колізії у правовому регулюванні, пов'язані з фіксацією цифрових слідів у розподілених мережах, а також складнощі забезпечення автентичності, цілісності та відтворюваності таких даних у судовому провадженні.

Проаналізовано міжнародний досвід і практику правоохоронних органів та судів щодо використання блокчейн-інформації як доказу, а також стандарти та рекомендації, що можуть бути імplementовані в національну правозастосовну діяльність. За результатами дослідження сформульовано науково обґрунтовані пропозиції щодо вдосконалення криміналістичних методик фіксації цифрових слідів у блокчейн-мережах, оптимізації процесуальних механізмів роботи з електронними доказами та підвищення ефективності їх використання під час судового розгляду кримінальних проваджень.

Ключові слова: блокчейн, цифрові сліди, електронні докази, криптовалюта, криміналістика, кримінальне провадження.

The article is devoted to a comprehensive study of the forensic and procedural aspects of recording digital traces in blockchain networks in the context of pre-trial investigation and trial of criminal offenses related to the use of cryptocurrencies and distributed ledger technologies. The relevance of the topic is due to the rapid spread of blockchain technologies in financial and economic activities, which is accompanied by an increase in the number of criminal offenses in which digital traces have an unconventional nature, a high level of technical complexity and a cross-border nature.

The features of detection, recording, extraction, storage and further analysis of information contained in blockchain transactions, smart contracts and related metadata are analyzed, taking into account the requirements of forensic tactics and procedural form. Special attention is paid to the use of special knowledge and software-analytical tools for identifying addresses, tracking the movement of virtual assets and establishing cause-and-effect relationships between events.

The evidentiary potential of blockchain data as a type of electronic evidence has been studied, the problems of their procedural registration, admissibility and assessment in the current criminal procedural legislation of Ukraine have been outlined. Gaps and conflicts in legal regulation related to the recording of digital traces in distributed networks have been identified, as well as the difficulties of ensuring the authenticity, integrity and reproducibility of such data in judicial proceedings. The international experience and practice of law enforcement agencies and courts regarding the use of blockchain information as evidence have been analyzed, as well as standards and recommendations that can be implemented in national law enforcement activities. Based on the results of the study, scientifically substantiated proposals have been formulated to improve forensic methods for recording digital traces in blockchain networks, optimize procedural mechanisms for working with electronic evidence and increase the efficiency of their use during the trial of criminal proceedings.

Key words: blockchain, digital traces, electronic evidence, cryptocurrency, forensics, criminal proceedings.

Постановка проблеми. Стрімкий розвиток цифрових технологій, зокрема блокчейн-мереж, суттєво трансформуює характер сучасної злочинності, надаючи правопорушникам нові можливості для приховування слідів протиправної діяльності та ускладнюючи роботу правоохоронних органів. Криптовалюти, децентралізовані плат-

форми та інші елементи блокчейн-інфраструктури дедалі частіше використовуються для здійснення шахрайств, легалізації доходів, фінансування тероризму, фішингових схем і кіберзлочинів. Особливість таких правопорушень полягає в їхній транснаціональності, високому рівні анонімності та специфіці цифрових слідів, що потребують

якісно інших, ніж традиційні, підходів до їх фіксації, збереження та подальшої оцінки.

Національна правозастосовна практика демонструє, що існуючі криміналістичні методики та процесуальні алгоритми не повною мірою пристосовані до роботи з даними блокчейн-мереж. Зокрема, проблемними залишаються питання встановлення джерела походження транзакцій, визначення фактичного власника криптоактивів, забезпечення цілісності цифрової інформації, її вилучення, збереження та верифікації. У кримінальному провадженні особливої ваги набуває питання допустимості таких електронних доказів, адже їх технічна природа не завжди узгоджується з існуючими процесуальними стандартами.

Актуальність теми зумовлюється також необхідністю гармонізації українського законодавства з міжнародними підходами до фіксації та оцінки електронних доказів, зокрема у контексті виконання вимог Будапештської конвенції про кіберзлочинність, практики Європейського суду з прав людини та рекомендацій Європолу, Інтерполу, ФАТФ. Успішна імплементація таких стандартів неможлива без опрацювання теоретичних і практичних засад роботи з цифровими слідами у блокчейн-середовищі.

Таким чином, формування ефективної системи криміналістичних та процесуальних механізмів фіксації цифрових слідів у блокчейн-мережах є нагальною потребою сучасного кримінального провадження. Це дозволить забезпечити належний рівень доказування, підвищити ефективність розслідування кримінальних правопорушень, пов'язаних із криптовалютами, та зміцнити спроможність держави протидіяти кіберзагрозам у цифрову епоху.

Аналіз останніх досліджень і публікацій. У науковій літературі останніх років проблема фіксації цифрових слідів у блокчейн-мережах розглядається у контексті розвитку електронних доказів, кіберкриміналістики та сучасних методів цифрової експертизи. Міжнародні дослідники та експертні організації акцентують увагу на важливості стандартизації процедур збору та збереження блокчейн-даних, необхідності застосування спеціалізованих інструментів для аналізу транзакцій криптоактивів, а також дотримання вимог автентичності та відтворюваності цифрових доказів. У низці публікацій наголошується, що блокчейн-інформація має високий доказовий потенціал за умови її належної технічної фіксації та процесуальної верифікації.

Українські науковці також приділяють значну увагу питанням використання цифрових слідів у кримінальних провадженнях, пропонуючи напрями модернізації криміналістичних методик і процесуальних підходів. У дослідженнях підкреслюється потреба адаптації національного законодавства до сучасних технічних можливостей роботи з децентралізованими реєстрами, а також формування уніфікованих правил документування дій слідчого при вилученні та аналізі блокчейн-даних. Особливо акцентується на важливості забезпечення безперервності ланцюга зберігання цифрових слідів, оскільки це безпосередньо впливає на їх допустимість у суді.

Серед українських досліджень варто відзначити праці Лугіної, яка розглядає правові та криміналістичні підходи до фіксації електронних доказів у криптовалютних провадженнях, а також увагу інших учених, що аналізують технічні особливості блокчейн-інфраструктури, проблеми ідентифікації учасників транзакцій та питання міжнародної взаємодії у сфері цифрових доказів. Сукупність цих напрацювань формує цілісне уявлення про ключові виклики та перспективи удосконалення практики роботи зі слідами, що виникають у блокчейн-мережах.

Таким чином, огляд досліджень свідчить про наявність значного наукового інтересу до теми, однак водночас підкреслює необхідність подальшого розвитку методичних,

технічних і процесуальних рішень, які б забезпечили ефективне використання блокчейн-даних як електронних доказів у кримінальному провадженні.

Метою статті є комплексне дослідження криміналістичних та процесуальних аспектів фіксації цифрових слідів у блокчейн-мережах, визначення їхнього доказового потенціалу та окреслення підходів до удосконалення методик вилучення, збереження й оцінки таких даних у кримінальному провадженні. Особлива увага приділяється узагальненню міжнародних стандартів роботи з блокчейн-інформацією, аналізу сучасних викликів, пов'язаних із децентралізованою природою криптоактивів, а також формуванню пропозицій щодо адаптації національних процедур до вимог цифрового середовища.

Виклад основного матеріалу. Однією з ключових складових ефективного кримінального провадження щодо кримінальних правопорушень із використанням криптовалют є належна фіксація цифрових слідів у блокчейн-мережах, яка передбачає не лише технічне виявлення інформації, а й її правильне правове оформлення як доказу. У сучасних умовах цифрові сліди становлять собою інший, якісно новий вид слідової інформації, що виникає внаслідок взаємодії суб'єкта з цифровою інфраструктурою та мережевими сервісами. Така інформація має особливу природу: вона подкує нестабільна, легко змінюється або видаляється, що обумовлює необхідність застосування спеціальних підходів криміналістичної фіксації й аналізу.

Цифрові сліди характеризуються певною множинністю носіїв і джерел: вони містяться не лише на фізичних пристроях, а й у цифрових сервісах, операційних системах, мережних логах та децентралізованих реєстрах. Зокрема, у разі транзакцій у блокчейн-мережах такими слідами є записи про переміщення криптоактивів, метадані транзакцій, адреси гаманців та інша інформація, що фіксується в розподіленому реєстрі. Підхід до виявлення і документування таких слідів значно відрізняється від традиційного огляду місця події або вилучення цифрового пристрою, адже він потребує не тільки фіксації даних як таких, але й належної фіксації умов їхнього отримання, забезпечення цілісності й можливості відтворення.

Українські дослідники вказують на відсутність єдиного підходу до дефініції цифрових слідів у межах криміналістичної науки. Національна юридична практика досі не виробила однозначної термінології: у вітчизняній літературі трапляються такі поняття, як «електронні сліди», «цифрові сліди» або «цифрові докази», які часто використовуються як синоніми, але мають різні значення залежно від контексту дослідження. Це ускладнює формування чіткої методологічної бази для роботи з доказами, отриманими з децентралізованих мереж, зокрема блокчейн-мереж [3, с. 29].

Загалом у криміналістиці цифрові сліди розглядаються як важливі елементи доказової картини, що дозволяють відтворити як механізм вчинення кримінального правопорушення, так і поведінку його суб'єкта. Вони здатні містити не лише інформацію про джерело даних і маршрути їхнього пересування цифровою інфраструктурою, а й метадані, що відображають часові позначки операцій, послідовність дій користувачів, зміни у структурі файлів та взаємодію з іншими цифровими об'єктами. Крім того, цифрові сліди можуть фіксувати обставини, які безпосередньо пов'язані з правопорушенням, наприклад, використання спеціальних програмних засобів, доступ до захищених ресурсів або спроби приховати сліди своєї діяльності.

Таке бачення підкреслює, що цифрові сліди становлять окрему категорію об'єктів криміналістичного вивчення, яка суттєво відрізняється від класичних фізичних слідів, як-от відбитки пальців, сліди крові чи сліди знарядь кримінального правопорушення. На відміну від традицій-

них слідів, цифрові об'єкти є динамічними, здатними до швидких змін і видалення, що вимагає спеціальних методик їх фіксації, збереження та дослідження. Цифрові сліди дозволяють відтворювати дії та наміри злочинця у цифровому середовищі, а також встановлювати взаємозв'язки між учасниками злочинної діяльності. У цьому контексті вони набувають не лише технічного, а й процесуального значення, оскільки належне документування цифрових слідів забезпечує їх допустимість як доказів у судовому процесі [4, с. 15].

Аналіз сучасних наукових розробок в Україні демонструє, що багато авторів акцентують увагу на проблемах класифікації та методик виявлення цифрових слідів. Зокрема, А. В. Коваленко у своїй праці пропонує виділяти електронні (цифрові) сліди правопорушення як особливу категорію слідової інформації, що виникає під час використання комп'ютерних пристроїв та мережевих сервісів у контексті злочинної діяльності. Він підкреслює важливість розробки класифікації таких слідів із урахуванням їх форми, джерела походження й ознак, які можуть бути використані в процесуальному доказуванні [1, с. 307].

Тенденції розвитку цифрової криміналістики в Україні також відображено у роботі Є. Демидової, де наголошується на ключових викликах, що постають перед правоохоронними органами: швидкі зміни цифрового середовища, збільшення обсягів даних, що створюються щоденно, а також необхідність постійної адаптації криміналістичних методик до нових технологій. Демидова визначає основні етапи роботи з цифровими доказами - виявлення, фіксація, вилучення та дослідження, підкреслюючи, що ці стадії мають бути взаємопов'язані й системно організовані для забезпечення збереження цілісності інформації та належної доказової сили [3, с. 27].

Окрему увагу в наукових колах приділяють процесуальній стороні фіксації електронних доказів у кримінальному провадженні. Незалежно від того, чи йдеться про традиційні цифрові сліди, чи про спеціальні дані з блокчейн-мереж, процесуальне закріплення таких доказів має відповідати вимогам допустимості та належності. Так, Я. В. Неділько підкреслює, що існуюче кримінальне процесуальне законодавство України не містить чітких визначень для цифрових доказів, що створює прогалини у регулюванні їх виявлення, дослідження, вилучення, зберігання та оцінки. Це ускладнює роботу слідчих і суддів, оскільки відсутність норм про цифрові докази призводить до розбіжностей у практиці їх використання в кримінальному процесі [4, с. 18].

В контексті фіксації цифрових слідів у блокчейн-мережах ці процесуальні питання набувають ще більшої ваги. Блокчейн як технологія забезпечує розподілене і незмінне зберігання даних транзакцій, однак це не означає автоматичної допустимості таких даних як доказів у суді. Правильне документування походження і умов отримання даних із блокчейн-мережі стає ключовим елементом для їхньої подальшої оцінки, оскільки суд має бути впевнений у тому, що інформація отримана належним чином і не була змінена під час процедури фіксації.

Важливим аспектом є також забезпечення ланцюга зберігання («chain of custody») для цифрових доказів, включно з тими, що отримані з блокчейн-мереж. Це вимога, яка має не лише технічне, а й процесуальне значення: документування кожного кроку фіксації, передачі та зберігання даних дозволяє забезпечити їхню незаперечність перед судом, а також зменшити ризики оскарження доказів через порушення процедурних норм [1, с. 2].

У науковій думці відзначають, що з огляду на міжнародний досвід, робота з цифровими доказами, включно

з даними з розподілених реєстрів, передбачає використання спеціалізованих інструментів та технологій, які дозволяють не тільки виявляти й вилучати інформацію, а й забезпечувати її збереження у формі, що є прийнятною для суду [5]. Це включає використання апаратних і програмних засобів, що підтримують зчитування, збереження метаданих, а також створення електронних копій із збереженням їх форензичного статусу.

Таким чином, огляд наукових підходів свідчить про те, що фіксація цифрових слідів у блокчейн-мережах є складним багатовимірним процесом, який поєднує у собі криміналістичні, технічні та процесуальні аспекти. Наукова література підкреслює необхідність уніфікації термінів і підходів, удосконалення законодавчого регулювання, розробки спеціалізованих методик та забезпечення їх практичної застосовності для ефективного використання блокчейн-даних як доказів у кримінальному правосудді.

Висновки. Фіксація цифрових слідів у блокчейн-мережах постає одним із найбільш складних і водночас перспективних напрямів сучасної криміналістики та кримінального процесу. Децентралізована архітектура, високий рівень анонімності користувачів, транскордонний характер передавання даних і відсутність єдиного центру контролю зумовлюють необхідність формування нових підходів до роботи з електронними доказами, що виникають під час використання криптовалют та інших технологій розподіленого реєстру.

Проведене дослідження засвідчило, що цифрові сліди блокчейну мають високий доказовий потенціал, оскільки вони є стійкими, незворотними та верифікованими незалежними учасниками мережі. Проте практичне використання таких даних у кримінальному провадженні потребує технологічної підготовки фахівців та належного правового забезпечення процедур їх виявлення, вилучення, збереження й оцінки. Особливе значення мають методики аналізу блокчейн-транзакцій, можливості відстеження криптоактивів, застосування спеціалізованого програмного забезпечення для реконструкції ланцюгів операцій та встановлення зв'язків між суб'єктами.

Водночас національна правозастосовна практика стикається з низкою викликів, серед яких недостатня регламентація порядку роботи з децентралізованими цифровими активами, нестача усталених стандартів фіксації електронної інформації, відсутність чіткого механізму міжнародної взаємодії під час отримання даних, що фізично зберігаються за межами юрисдикції України. З огляду на це необхідним є подальше вдосконалення процесуальних норм щодо електронних доказів, інтеграція міжнародних рекомендацій та кращих практик, а також розроблення спеціалізованих криміналістичних методик.

Перспективним напрямом розвитку є створення у правоохоронних органах спеціалізованих підрозділів з аналізу блокчейнів, впровадження практики комплексної цифрової forensics, а також підвищення кваліфікації слідчих, прокурорів та експертів у сфері обігу криптоактивів. Розвиток цих компетенцій дозволить забезпечити ефективну протидію кримінальним правопорушенням, що вчиняються з використанням новітніх цифрових технологій, та підвищить рівень довіри до електронних доказів у судовому процесі.

Таким чином, фіксація цифрових слідів у блокчейн-мережах потребує комплексного поєднання технічних, організаційних і правових заходів, що дасть змогу адаптувати криміналістичну та процесуальну практику до вимог сучасного цифрового середовища та міжнародних стандартів доказування.

ЛІТЕРАТУРА

1. Коваленко А. В. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. Вип. 161. С. 304-310.
2. Karaman K. V. Modern paradigm of the forensic significance of digital traces in criminal proceedings. *Bulletin of criminological association of Ukraine*. 2025. №2. С. 1-10.
3. Demydova Y. Trends in the Development of Digital Forensics: Challenges and Prospects for Criminal Justice Agencies. *Проблеми законності*. 2025. Вип. 168. С. 25-32.
4. Неділько Я. В. Доктрина електронних доказів у кримінальному процесі: національні особливості та світові тенденції. *Правова держава*. 2025. №57. С. 12-20.
5. Лугіна, Н. А., Вартовнік, А. М. Блокчейн в Україні: проблеми правового регулювання. *Міжнародний науковий журнал Інтернаука*, 2020. №8 (2), С. 74-79.

Дата першого надходження рукопису до видання: 23.10.2025
Дата прийнятого до друку рукопису після рецензування: 19.11.2025
Дата публікації: 28.11.2025