УДК 343.13:343.14:343.3/.7:004.056.5:341.645
DOI https://doi.org/10.32782/1813-338X-2025.3.10

М. А. Погорецький
доктор юридичних наук, професор, член-кореспондент
Національної академії правових наук України,
заслужений діяч науки і техніки України,
проректор з науково-педагогічної роботи
Київського національного університету імені Тараса Шевченка
https://orcid.org/0000-0002-9012-7686

КРИПТОВАЛЮТА ЯК ОБ'ЄКТ, ПРЕДМЕТ ТА ЗАСІБ ВЧИНЕННЯ ЗЛОЧИНУ: ПРОБЛЕМИ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ І ДОКАЗУВАННЯ В ДОСУДОВОМУ ТА СУДОВОМУ ПРОВАДЖЕННЯХ

Стаття присвячена формуванню системного процесуального підходу до роботи з криптоактивами у кримінальному провадженні – від моменту виявлення до судового розгляду. Запропоновано модель інтеграції цифрових доказів, що враховує функціональну участь оперативних і контррозвідувальних підрозділів, слідчих, прокурорів та суду.

Метою дослідження є визначення правової класифікації ролей криптовалюти (об'єкт, предмет, засіб) і розроблення процесуально-криміналістичної рамки, яка забезпечує належність, допустимість і відтворюваність цифрових доказів на всіх стадіях провадження. Особлива увага приділяється узгодженню результатів оперативно-розшукової та контррозвідувальної діяльності з матеріалами досудового розслідування, перевірці їх автентичності та дотриманню ланцюга збереження доказів (chain of custody).

Методологічну основу статті становлять формально-юридичний і порівняльно-правовий методи із залученням положень Регламентів ЄС MiCA і TFR, механізмів Європейського ордера на розслідування та міжнародних договорів про взаємну правову допомогу. Дослідження спирається на стандарти фіксації та збереження цифрових слідів, розроблені у Berkeley Protocol, ENFSI та NIST, адаптовані до триангуляційної моделі перевірки даних із блокчейнових, позаблокчейнових та відкритих джерел.

Наукова новизна полягає в поєднанні класифікації «об'єкт – предмет – засіб» із поетапним процесуальним алгоритмом інтеграції цифрових доказів («виявлення → фіксація → перевірка → документування → судова оцінка») та у формуванні правової схеми співвіднесення «роль криптовалюти – юридичні наслідки – доказова стратегія».

Практичне значення дослідження полягає у створенні уніфікованих контрольних переліків і шаблонів документування (протоколи огляду вебресурсів/API, хеш-таблиці, описи інструментів, акти ОРД/КРД), мінімального пакета розкриття для судової перевірки та сторони захисту, а також орієнтирів для суддів щодо оцінки прозорості методики, відтворюваності та кореляції між блокчейновими та позаблокчейновими даними (on-chain ↔ off-chain).

Запропонована процесуально-криміналістична модель забезпечує трансформацію технічних і відомчих інформаційних масивів – зокрема даних блокчейна, комплаєнс-інформації провайдерів та результатів оперативно-розшукових і контррозвідувальних заходів – у процесуальну форму доказів, що відповідає критеріям належності, допустимості й достовірності, узгодженим зі стандартами справедливого судового розгляду.

Ключові слова: *криптовалюта, блокчейн, об'єкт злочину, предмет злочину, засіб вчинення злочину, Європейський ордер на розслідування (EIO), оперативно-розшукова діяльність, досудове розслідування, судове провадження, цифрові докази, цифрова криміналістика.*

Вступ. Криптовалюта дедалі частіше охоплюється сферою кримінально-правових і процесуальних відносин, у межах яких вона може виконувати функцію об'єкта посягання, предмета злочину або засобу його вчинення, що зумовлює потребу у її належній правовій кваліфікації та доказовій ідентифікації ролі в механізмі злочинної діяльності. Такий підхід

безпосередньо впливає на кваліфікацію кримінального правопорушення, структуру предмета доказування та вибір оперативно-розшукових та процесуальних засобів виявлення й документування та відповідної криміналістичної тактики – від виявлення, первинної фіксації цифрових слідів до стандартизованої судової перевірки цифрових доказів, поданих сторонами у судовому розгляді.

У практиці найпоширенішими залишаються злочини, пов'язані з шахрайством у сфері криптоактивів (інвестиційні піраміди, фішингові схеми, викрадення сид-фраз *(seed phrase)*, застосування методів соціальної інженерії), у яких криптовалюта може одночасно виступати предметом заволодіння і каналом швидкого виведення активів. Водночас значне поширення мають схеми легалізації (відмивання) доходів, де використовуються мікшери, ланцюгові перестрибування *(chain-hopping)*, смартконтрактні сценарії, а також механізми фінансування забороненої діяльності – тероризму, торгівлі людьми, зброєю, наркотичними засобами, екстремізму чи сепаратизму. У таких випадках вирішальне значення має інтеграційне співвіднесення внутрішньоланцюгових *(on-chain)* транзакцій із позаланцюговими ідентифікаційними атрибутами бенефіціарів, що дозволяє встановити їх фактичний контроль над активами та правовий зв'язок із предметом злочину.

Окрему групу становлять порушення режимів фінансового моніторингу, зокрема обхід процедур KYC / AML, провадження діяльності без належної реєстрації чи ліцензії, недотримання санкційних обмежень, а також злочини у сфері службової діяльності – незаконне збагачення та одержання неправомірної вигоди, коли криптовалюта виконує роль «безготівкового» носія корупційного прибутку з підвищеним ризиком маскування його походження. У кожній із зазначених категорій правопорушень роль криптовалюти детермінує структуру доказового аналізу: ідентифікацію суб'єкта або бенефіціара, простежуваність руху активів, встановлення джерела їх походження, перевірку законності способу одержання даних та забезпечення можливості незалежного відтворення висновків стороною захисту.

Транскордонний характер блокчейн-операцій, псевдонімність ідентифікаторів та залежність результатів графового аналізу від позаланцюгових даних (KYC-пакетів, журналів доступу провайдерів, записів бірж, платіжних шлюзів) обумовлюють підвищені вимоги до виявлення, консервації та перевірки достовірності цифрових слідів. Мінімізація ризиків хибної атрибуції потребує поєднання внутрішньоланцюгової аналітики з процесуально коректним отриманням позаланцюгових відомостей, забезпечення ланцюга збереження доказів (chain of custody), прозорого опису застосованих інструментів, версій і конфігурацій, а також відтворюваності методики як передумови незалежної перевірки доказів у суді [2].

Міжнародна практика розслідування кримінальних правопорушень у сфері функціонування криптосервісів демонструє зростаюче значення ідентифікації клієнтів, дотримання реєстраційних і санкційних режимів, а також якості лог-даних, що у сукупності формують дорожню карту слідчих (розшукових) дій та міжнародної взаємодії у справах про шахрайство, легалізацію доходів і фінансування забороненої діяльності [1].

В українському правопорядку визначення правового статусу криптоактивів є ключовою передумовою для окреслення меж допустимого втручання, коректної правової кваліфікації (зокрема, у провадженнях щодо хабарництва та незаконного збагачення, де криптовалюта може виконувати функцію неправомірної вигоди), а також стандартизованої судової оцінки цифрових доказів [24; 25].

Отже, актуальність теми зумовлюється необхідністю формування цілісної оперативно-розшукової та процесуально-криміналістичної моделі виявлення, документування та доказування злочинів, у яких криптовалюта є об'єктом, предметом чи засобом вчинення, що забезпечить її правову визначеність, простежуваність і належне використання у кримінальному процесуальному доказуванні.

Аналіз останніх досліджень і публікацій. У сучасному науковому дискурсі сформувалися три взаємодоповнювальні підходи до визначення правового статусу криптоактивів, від якого безпосередньо залежить їх кримінально-правова кваліфікація, що, у свою чергу, зумовлює структуру предмета доказування у відповідних кримінальних провадженнях. *Перший – майно / нематеріальний актив:* акцент на походженні активу, моменті набуття, контролі над ключами/адресами та можливості конфіскації чи спеціальної конфіскації, що розвинено в українській доктрині та прикладних працях [24; 37; 42; 43; 48] і корелює з практикою національних судів щодо оцінки цифрових активів як об'єкта посягання чи неправомірної

вигоди [38; 39; 40; 41]. *Другий – фінансовий інструмент:* регуляторні наслідки (реєстрація, ліцензування, публічні обов'язки провайдерів), що впливають на кваліфікацію порушень правил обігу, розкриття інформації, фінмоніторинг і ринковий нагляд; тут релевантні MiCA/TFR і суміжні джерела [6; 12; 13; 22; 23; 52; 53], а також судові рішення у спорах зі «світчем» ціннопаперової кваліфікації (Coinbase, Kraken, Ripple) [34; 35; 36]. *Третій – цифровий товар / послуга:* приватноправова природа зобов'язань та значення договірних умов для визначення добросовісності, волевиявлення і розподілу ризиків; підхід підтримано економіко-правовими оглядами та українськими працями про цивілістичні аспекти криптообігу [20; 42; 46; 48].

Процесуально-методичний пласт зосереджується на стандартах роботи з відкритими цифровими джерелами та мережевими слідами. Базові вимоги автентичності, цілісності, відтворюваності та атрибуції закріплені міжнародними протоколами / настановами (фіксація джерела, збереження метаданих, хешування, опис інструментів / версій / конфігурацій, реплікованість методики) [2; 9; 10; 12; 16; 21]. Для аналізу даних, що зберігаються безпосередньо в ланцюгу блокчейна (on-chain), це передбачає прозоре відображення застосованих евристичних методів та визначення допустимих меж похибки; для даних, що знаходяться поза блокчейном (off-chain), – належне оформлення запитів до постачальників послуг, криптовалютних бірж і платіжних провайдерів, з обов'язковим збереженням журналів доступу, досьє ідентифікації клієнтів (KYC), копій договорів та службового листування як повноцінних джерел доказової інформації [8; 9; 12; 21]. Європейські процесуальні інструменти забезпечують отримання транскордонних даних (EIO), тоді як стандарти захисту прав людини визначають критерії законності, пропорційності та якості закону, що встановлюють допустимі межі втручання у приватне життя [7; 55; 56]. Додаткові орієнтири щодо цифровізації провадження й допустимості цифрових доказів напрацьовано в українській науковій доктрині [54; 48; 49; 50].

Правозастосовна та аналітична практика останніх років систематизує ризики й тенденції кримінального використання криптоактивів (шахрайство, відмивання коштів, фінансування забороненої діяльності, обхід санкцій тощо), що підкреслює необхідність інтегрованого опрацювання внутрішньоланцюгових і позаланцюгових даних (on-chain ↔ off-chain транзакцій і процесів) [3; 4; 11; 25; 26; 27; 30]. Практика переслідування криптосервісів і формування доказової бази виразно демонструє центр ваги на KYC/AML, санкційних і реєстраційних режимах та якості журналів доступів/платіжних слідів [1; 14; 21; 28; 29]. У США суди окреслили стандарти доступу до даних бірж і допустимості блокчейн-трасування, а також конфіскаційні підходи, що має важливе значення для подальшої гармонізації стандартів доказування [28; 29; 31; 32; 33]. Узагальнення кейсів та аналітичних оглядів, підготовлених приватними й міжурядовими інституціями, поглиблює розуміння тактики виявлення та розслідування злочинів, пов'язаних із використанням криптоактивів, а також конкретизує правові вимоги до діяльності провайдерів [6; 13; 15; 17; 21]. В українському контексті поступово формуються підходи до оподаткування та декларування криптоактивів, а також до їх відображення у практиці публічних органів, що безпосередньо впливає на визначення предмета доказування у справах про незаконне збагачення та хабарництво [18; 19; 20; 45; 51].

Узагальнюючи, українська наукова доктрина, спираючись на порівняльно-правові моделі, наголошує: коректне визначення правового статусу криптовалюти є необхідною передумовою належної кримінально-правової кваліфікації шахрайства, легалізації (відмивання) доходів, фінансування забороненої діяльності (тероризму, торгівлі людьми, зброєю, наркотичними засобами, екстремізму, сепаратизму тощо), а також порушення вимог фінансового моніторингу, незаконного збагачення та хабарництва, коли криптовалюта виступає предметом неправомірної вигоди [24; 41; 42; 43; 48]. Водночас, попри наявні наукові та практичні напрацювання щодо окремих аспектів виявлення, документування й доказування у досудовому та судовому провадженні, залишається не розробленим системно: (1) уніфікований критерій розмежування ролі криптовалюти у фабулі кримінального правопорушення (об'єкт, предмет чи засіб вчинення) з прямими наслідками для її кримінально-правової кваліфікації за групами злочинів; (2) процесуальний механізм верифікації та співвіднесення внутрішньоланцюгових ↔ позаланцюгових даних (on-chain ↔ off-chain) – графових евристик ↔ досьє з перевірки клієнта (KYC/AML), журналів доступу, записів бірж – із визначенням меж похибки та застосуванням тесту відтворюваності; (3) експертно-криміналістичні протоколи збереження вебджерел

і відповідей прикладних програмних інтерфейсів (API) – скрінкасти, цифрові зліпки, хеш-таблиці «сирі ↔ робочі копії», фіксація використаних інструментів, версій і конфігурацій – із встановленням вимог до ланцюга збереження доказів *(chain of custody)*; (4) алгоритми міжнародної взаємодії з постачальниками цифрових послуг – запити про заморожування даних *(freeze-запити)*, строки їх зберігання, санкційні та реєстраційні режими – для оперативного отримання позаланцюгових доказів *(off-chain evidence)*; (5) модель судового контролю та стандарти мотивування допустимості й належності цифрових доказів, а також правила оцінки вартості, спеціальної конфіскації та фіксації неправомірної вигоди у криптовалютній формі [2; 7; 9; 10; 20; 21; 28; 29; 51; 55; 56].

Отже, виявлені прогалини та узагальнені результати проведеного огляду – від визначення ролі криптовалюти у фабулі кримінального правопорушення до встановлення стандартів документування та інтеграції внутрішньоланцюгових *(on-chain)* і позаланцюгових *(off-chain)* даних із подальшою судовою перевірюваністю – обумовлюють необхідність чіткого формулювання мети й завдань цієї статті.

Метою статті є розроблення цілісної моделі ідентифікації ролі криптовалюти у структурах кримінальних правопорушень відповідних категорій та формування узгоджених процесуально-криміналістичних підходів до їх виявлення, документування і доказування, що забезпечують належність, допустимість і перевірюваність цифрових доказів при збереженні засад змагальності та балансу процесуальних можливостей сторін.

Матеріали і методи. Джерельну базу дослідження становлять чотири взаємопов'язані блоки. *Перший* – міжнародні та галузеві стандарти цифрової криміналістики та розвідки з відкритих джерел (OSINT), які встановлюють вимоги до автентичності, цілісності, атрибуції та відтворюваності цифрових доказів. Зокрема, йдеться про фіксацію джерела, збереження метаданих, хешування, опис інструментів, версій і конфігурацій. До цього блоку належать *Berkeley Protocol*, настанови Європейської мережі судово-експертних установ (ENFSI), пов'язані керівництва з найкращих практик, а також орієнтири Європейського парламенту й Організації з безпеки і співробітництва в Європі (ОБСЄ) для правоохоронних органів [2; 9; 10; 12; 21; 16]. *Другий* блок охоплює нормативно-правову та політико-регуляторну модель транскордонного доступу до даних і регулювання ринку криптоактивів: Європейський ордер на розслідування (EIO), Регламенти ЄС щодо ринків криптоактивів (MiCA) та супровідної інформації про перекази (TFR), національні акти з протидії відмиванню доходів, а також положення Кримінального процесуального кодексу України [7; 22; 23; 51; 44]. *Третій* блок складається із судової та правозастосовної практики, яка ілюструє стандарти допустимості й належності цифрових доказів, підходи до конфіскації криптоактивів та особливості проваджень щодо криптосервісів і користувачів *(OKX/OKEx, Sterlingov/ Bitcoin Fog, Gratkowski, Ulbricht)*, а також справи з ринкового нагляду *(SEC v. Coinbase, Kraken, Ripple)* і відомчі настанови Міністерства юстиції США щодо конфіскації цифрових активів [1; 28; 29; 31–36]. Четвертий блок охоплює аналітичні звіти та огляди тенденцій криптозлочинності, підготовлені *Chainalysis, TRM Labs, COPOLAD, Євроюстом, Європолом*, Міністерством фінансів США, юридичними фірмами (зокрема *DLA Piper*), а також матеріали українських органів щодо декларування, оподаткування й судового розгляду справ, пов'язаних із криптоактивами [3; 4; 6; 11; 13; 15; 17; 18; 20; 25; 26; 30; 45].

Методологія дослідження поєднує чотири взаємодоповнювальні компоненти. *По-перше*, формально-юридичний аналіз застосовується для розмежування ролі криптовалюти (як об'єкта, предмета або засобу злочину) та деталізації елементів предмета доказування у справах про шахрайство, легалізацію (відмивання) доходів, фінансування забороненої діяльності, порушення фінансового моніторингу, хабарництво та незаконне збагачення. Метод опирається на положення української юридичної доктрини й порівняльно-правові дослідження [24; 37; 42; 43; 48]. *По-друге*, порівняльно-правовий підхід дозволяє зіставити регуляторні режими та процедурні моделі провайдерів (VASP), визначити оптимальні канали для отримання позаблокчейнових доказів (off-chain) – через MiCA, TFR, EIO та інші механізми [7; 21–23]. *По-третє*, процесуально-криміналістичний аналіз застосовано для розроблення протоколів фіксації та збереження (консервації) цифрових доказів і електронних слідів: вебресурсів, API-відповідей, лог-файлів, із використанням техніки скрінкастів, форензійних зліпків, хеш-таблиць для «сирих» і робочих копій, документування застосованих інструментів, версій, конфігурацій

і оформлення безперервного ланцюга збереження (chain of custody). В основу покладено стандарти ENFSI, NIST і відповідні орієнтири Європейського парламенту [2; 9; 12; 16].

По-четверте, емпіричний компонент реалізовано у вигляді case-oriented синтезу, що передбачає картографування зв'язків між on-chain і off-chain джерелами (кластеризація адрес, KYC/AML-досьє, біржові журнали доступу, платіжні шлюзи), на підставі судових матеріалів, відкритих джерел і профільних звітів [1; 3; 11; 21; 25; 31; 32].

З метою перевірки належності, допустимості та достатності доказової інформації здійснено криміналістичне зіставлення джерел, спрямоване на забезпечення перехресної перевірки даних, виявлення можливих розбіжностей і мінімізацію похибок. Такий підхід дозволяє зіставити відомості, отримані з різних інформаційних масивів – цифрових, документальних та свідчень осіб, – з метою формування узгодженої та внутрішньо несуперечливої системи доказів, що відповідає критеріям об'єктивності й процесуальної надійності – зіставлення висновків блокчейн-трасування з незалежними off-chain даними, повторна перевірка відтворюваності аналітичної методики, підтверджена можливістю незалежної реплікації з боку захисту на основі наданих хеш-таблиць, експортів даних і описів інструментів [2; 9; 10]. Дотримання стандартів прав людини гарантується через застосування тестів законності, необхідності та пропорційності втручання у приватне життя при отриманні цифрових доказів (у тому числі – через EIO/MLAT), відповідно до практики Європейського суду з прав людини [55; 56], а також із урахуванням національних процесуальних приписів і рекомендацій щодо цифровізації кримінального процесу [44; 54].

Нарешті, український контекст досліджено шляхом верифікації на локальній судовій практиці – через аналіз вироків та ухвал антикорупційної і загальної юрисдикції, в яких криптоактиви виступають як форма неправомірної вигоди або доходу, а також як доказовий інструмент, що вимагає належної фіксації цифрових слідів як майбутніх доказів у матеріалах кримінального провадження [38–41; 49; 50].

Виклад основного матеріалу. Роль криптовалюти у відповідному кримінальному правопорушенні (як об'єкта, предмета чи засобу вчинення) має бути визначена по можливості ще до планування оперативно-розшукових заходів під час ОРД або процесуальних дій в ході досудового розслідування, залежно від способу виявлення та документування ознак правопорушень, пов'язаних із криптовалютою, оскільки від цього залежать кримінально-правова кваліфікація, елементи предмета документування й доказування, допустимі процесуальні інструменти доступу до даних і перелік позаблокчейнових ("off-chain") джерел (KYC/AML-досьє, журнали доступу, записи біржових рахунків) [22; 23; 42; 43; 48; 51].

Уніфікований підхід спирається на доктрину доказування й судового контролю з вимогами прозорої методики, відтворюваності та ланцюга збереження цифрових слідів *(chain of custody)* [2; 9; 10; 12; 16; 48; 49] і узгоджується зі стандартами пропорційності втручання у приватність під час отримання транскордонних даних (EIO/MLAT) [7; 55; 56].

З урахуванням актуальної кримінологічної аналітики щодо шахрайств, схем легалізації, обходу санкцій і фінансування забороненої діяльності пропонується класифікація ролей «об'єкт – предмет – засіб» та пов'язані з нею доказові наслідки [3; 4; 11; 13; 14; 21; 25; 26; 30].

Об'єктом є охоронювані кримінальним законом суспільні відносини (власність, фінансова безпека, публічний порядок і порядок управління, довіра до фінансової системи та протидія відмиванню), у тому числі в площині запобігання легалізації доходів і фінансуванню тероризму; доступ до релевантних цифрових даних здійснюється з використанням інструментів, сумісних з європейськими стандартами прав людини й транскордонної співпраці (Європейський ордер на розслідування, тести «якість закону», «необхідність і пропорційність») [7; 13; 22; 23; 30; 51; 55; 56], що в національному процесі поєднується з вимогами допустимості та належної процесуальної форми фіксації електронних слідів і узагальненнями щодо цифровізації провадження [48; 49; 50; 54]. У цьому контексті кіберпростір розглядається як інфраструктурне середовище вчинення посягань із власними моделями слідоутворення, що обумовлює іншу логіку пошуку й фіксації цифрових слідів [54].

Предметом є те, з приводу чого здійснюється посягання або що становить майнову вигоду – криптоактив як майно/нематеріальний актив у складі злочину (токени, баланси гаманців, приватні ключі, seed-фрази, облікові записи бірж, «квазі-грошові» похідні), для чого враховуються податково-облікові підходи та режим декларування, що впливає на доказування

походження і розміру неправомірної вигоди, зокрема у справах про хабарництво чи незаконне збагачення [18; 20; 24; 37; 42; 43; 48; 51]; у компаративному аспекті використовується позиція CJEU щодо природи операцій з віртуальною валютою (Hedqvist) [5], а американська практика окреслює стандарти використання блокчейн-трасування та даних бірж для ідентифікації володіння активом і доведення зв'язку адреси з особою, а також підходи до конфіскації / спецконфіскації цифрових активів [28; 29; 31; 32; 33]. Аналогічно до моделей рейдерських посягань, вирішальним для предмета є фактичний контроль і економічний еквівалент вартості, що підлягає обчисленню для кваліфікації й спеціальної конфіскації [44].

Засобом є інструмент виконання злочину: використання мікшерів / «тумблерів», протоколів підвищеної приватності (privacy-coins), "chain-hopping", крос-чейн-мостів, смартконтрактних сценаріїв (у т. ч. DeFi), сервісів-обфускаторів, а також порушення правил «подорожуючої інформації» при переказах; у такому разі криптовалюта є «каналом» перетворення / маскування / переспрямування вартості, що впливає на кваліфікацію (легалізація доходів, фінансування забороненої діяльності, порушення фінмоніторингу) і на набір доказових питань: ідентифікація протоколу / маршруту, кореляція on-chain висновків із "off-chain" слідами (KYC-досьє, журнали доступу, платіжні зв'язки, договори) [3; 4; 11; 14; 21; 22; 25; 26; 30; 51]. Додатковий доказовий вимір формують провадження у сфері ринкового та регуляторного нагляду за обігом криптоактивів (кваліфікація окремих токенів як фінансових інструментів / цінних паперів; віднесення відповідних сервісів до регульованої біржової / професійної діяльності), результати яких зумовлюють наявність спеціальних (регуляторних) ознак складу кримінального правопорушення та породжують документальні джерела доказів – комплаєнс-документи, матеріали розкриття інформації, ліцензійні (реєстраційні) досьє й наглядові акти – що використовуються як документи у розумінні КПК України [23; 34; 35; 36; 52].

У підсумку чітке розмежування *«об'єкт – предмет – засіб»* визначає предмет доказування для типових категорій справ: у шахрайствах – факт заволодіння та простежуваність вартості; у легалізації – доведення злочинного походження й трансформаційного ланцюга; у фінансуванні забороненої діяльності – атрибуція адрес / вузлів до бенефіціарів і зв'язок платежів із забороненими цілями; у порушеннях фінмоніторингу – невиконання обов'язків провайдерів / KYC і порушення TFR; у хабарництві / незаконному збагаченні – ототожнення криптовалюти з неправомірною вигодою й визначення її вартості; у кожному випадку потрібні стандартизовані методики фіксації та перевірюваності (опис інструментів і версій, збереження метаданих і хешів «сирих» та робочих копій, належні канали отримання "off-chain" даних через EIO / MLAT, документи комплаєнсу провайдерів, а також перевірка пропорційності втручання за практикою ЄСПЛ) [2; 3; 7; 9; 10; 12; 16; 18; 20–23; 25; 42; 43; 48; 51; 59; 60].

Роль криптовалюти *(«об'єкт – предмет – засіб»)* безпосередньо визначає предмет доказування, формулювання диспозиції та коло ознак складу злочину: коли криптовалюта є предметом шахрайства, ключовими стають доведення факту заволодіння (механізм обману чи зловживання довірою), вартості активу та зв'язку між адресою / гаманцем і конкретною особою, що спирається на трасування транзакцій і їх кореляцію з *"off-chain"* даними провайдерів (KYC-досьє, журнали доступу, записи бірж) [1; 3; 25; 31–33]; коли вона виконує роль засобу легалізації, фокус зміщується на встановлення злочинного походження вартості, опис трансформаційного ланцюга (мікшери, *"chain-hopping"*, крос-чейн-мости, DeFi-сценарії), визначення ролі посередників (VASPs) і перевірку дотримання ними належної обачності та правил «подорожуючої інформації» [4; 11; 14; 21; 22; 30]; у фінансуванні забороненої діяльності вирішальними є атрибуція вузлів/гаманців до бенефіціарів і зв'язок платежів із забороненими цілями, що потребує поєднання on-chain аналізу з KYC/санкційними переліками та транскордонного доступу до доказів через EIO/MLAT [3; 7; 13; 14; 21; 25]; у справах про порушення фінмоніторингу предметом є невиконання провайдерами обов'язків і процедур (ідентифікація, зберігання та передача даних, дотримання TFR), що підтверджується політиками комплаєнсу, журналами доступів, кореспонденцією з регуляторами та матеріалами наглядових перевірок [6; 12; 22; 23; 51]. Відповідно до вітчизняних реалій додатково підлягають обов'язковому врахуванню деклараційно-податкові режими та механізми фінансового моніторингу, які мають істотне значення для встановлення законності походження активів і визначення (ідентифікації та розміру) неправомірної вигоди; відповідні відомості формують

складову предмета доказування у провадженнях щодо незаконного збагачення та одержання неправомірної вигоди [18; 20; 41; 51], а стандарти допустимості та належності цифрових доказів вимагають прозорості методики, відтворюваності та пропорційності втручання у приватність відповідно до практики ЄСПЛ і національних процесуальних вимог [59; 60; 44; 54]; у регуляторно-ринкових конфліктах (ціннопаперова природа окремих токенів/послуг) кваліфікаційні наслідки конкретизуються у справах *SEC v. Coinbase / Kraken / Ripple* [34–36], тоді як американські кримінальні кейси *(Gratkowski, Ulbricht, Sterlingov)* формують стандарти допустимості та процесуальні межі використання відомостей криптовалютних бірж у доказуванні, окреслюють правові умови, порядок одержання та перевірки автентичності відомостей криптовалютних бірж у кримінальному провадженні, графового аналізу та конфіскаційних підходів [28; 29; 31–33].

Узагальнюючи ці підходи, у додатку наведено таблицю відповідності «роль криптовалюти → юридичні наслідки → доказова стратегія», що регламентує порядок та критерії вибору між «предметом», «засобом» і «об'єктом»: для ролі «предмет» фіксуються юридичні наслідки у вигляді встановлення права / факту володіння, вартості, шкоди та спеціальної конфіскації, типові джерела (експорти з блокчейна, дані бірж, KYC-пакети, журнали входів / IP, платіжні зв'язки, дані декларування / оподаткування) і процесуальні інструменти (огляди / вилучення, запити до VASPs, EIO/MLAT), із приписами до консервації й відтворюваності за Berkeley Protocol / ENFSI / NIST [2; 7; 9; 16; 18; 20–23]; для ролі «засіб» систематизуються наслідки у вигляді доведення трансформаційного ланцюга та порушень «подорожуючої інформації», джерела (кластери / евристики, журнали API, комплаєнс-політики, санкційні / реєстраційні пакети) та інструменти міжнародної взаємодії й тимчасового замороження, зі стандартами FATF R.15/INR.15, TFR і методичними орієнтирами OSCE / Європарламенту [14; 22; 21; 4; 12]; для ролі «об'єкт» окреслюються посягання на власність / фінансову безпеку/публічні інтереси, джерела (нормативні акти, судова практика щодо меж втручання та допустимості електронних доказів), інструменти (процесуальні дії за КПК, EIO, судовий контроль) і стандарти пропорційності та «якості закону» за ЄСПЛ [7; 44; 55; 56].

Структурно-логічна модель також встановлює контрольні точки відтворюваності (опис інструментів / версій / конфігурацій, хеш-таблиці «сирі ↔ робочі копії», протоколи збереження метаданих, вимоги до незалежної реплікації), перелік типових помилок недопустимості (скріншоти без форензійного еквівалента, відсутність хешів / метаданих, нечіткий метод) [2; 9; 10; 12] і вшиває порівняльно-регуляторний вимір (MiCA/TFR; позиції SEC-кейсів) для виявлення похідних доказів комплаєнсу та ринкового нагляду, релевантних кваліфікації й доказуванню, з урахуванням української судової практики та специфіки декларування / оподаткування [18; 20; 22; 23; 34–36; 38–41].

Залежно від складу злочину, його підвідомчості та підслідності первинні дії з виявлення, фіксації та збереження цифрових (електронних) слідів можуть виконувати працівники оперативних та контррозвідувальних підрозділів органів правопорядку, а також слідчі / детективи; у всіх випадках вони мають діяти в межах процесуальної форми та з урахуванням транскордонного характеру криптоактивів і стандартів прав людини [7; 44; 55; 56]. *On-chain* джерела охоплюють дані публічних блокчейн-реєстрів, що отримуються через блокчейн-експлорери та інструменти графового аналізу транзакцій, з подальшим формуванням адресних кластерів і застосуванням евристик (наприклад, «спільне витрачання», «зміна» тощо); при цьому обов'язковими є опис використаних інструментів / версій / конфігурацій, збереження метаданих і хешування експорту як передумова відтворюваності, а також чітке фіксування меж інференцій і ризиків хибнопозитивних зв'язків (особливо в контексті мікшерів, DeFi та «chain-hopping») [2; 3; 8–10; 25; 26]. *Off-chain джерела* формуються з матеріалів провайдерів і посередників (VASPs): журнали доступу й сесій, KYC/AML-досьє, записи біржових рахунків, договори, платіжні зв'язки, листування підтримки; їх одержання здійснюється через процесуальні запити, у т. ч. транскордонні канали (EIO/MLAT), а для юрисдикцій загального права – також через судові виклики/субпоени до провайдерів; ключову роль відіграють вимоги FATF R.15/INR.15 та «подорожуючої інформації» TFR, що зобов'язують VASPs зберігати і передавати ідентифікаційні дані, корисні для атрибуції бенефіціара [7; 14; 21–23; 29].

Як засвідчує практика тимчасового доступу, зволікання з ухвалою та слабка примусовість її виконання прямо підвищують ризики втрати логів / технічних записів; отже, запити до постачальників послуг у сфері віртуальних

активів (VASP) мають ініціюватися без зволікань і супроводжуватися заходами збереження: журналів доступу та сесій (IP-адреси, агент користувача, «відбиток» пристрою, файли cookie, маркери сесії), пакетів KYC/AML (ідентифікаційні дані клієнта, дати й часи верифікації, ризиковий профіль), біржових записів і технічних журналів (залишки на рахунках, ордери, зарахування / виведення, адреси та ідентифікатори транзакцій, маршрути переказів), а також судово-технічних (комп'ютерно-технічних) знімків і експорту даних через програмні інтерфейси прикладних систем (API) із фіксацією використаних інструментів, їхніх версій, конфігурацій, часових міток і часового поясу; обов'язковим є хешування «сирих» і робочих копій, зазначення строків зберігання у провайдера та визначення відповідальної особи за збереження документів; паралельно необхідно надіслати звернення про замороження рахунків / адрес і продублювати запити каналами Європейського ордера на розслідування та міжнародної правової допомоги для підтвердження консервації даних і недопущення їх ротації чи втрати [53].

Судова практика підтверджує можливість і належність використання даних бірж і графового аналізу для встановлення контролю над гаманцем, а також формує підходи до конфіскації цифрових активів (Gratkowski; Ulbricht; Sterlingov), тоді як матеріали справ щодо провайдерів (у т. ч. OKX/OKEx) демонструють доказове значення комплаєнс-політик, логів і KYC-пакетів [1; 28; 31–33]. *OSINT і відкриті цифрові сліди* потребують суворого дотримання правил автентичності та цілісності: Збирання цифрових джерел здійснюється шляхом виконання скрінкастів та судово-технічних (форензійних) знімків із обов'язковою фіксацією першоджерела (URL), часової мітки (дата-час) та часового поясу, збереженням повного набору метаданих і негайним хешуванням «сирих» і робочих копій у межах ланцюга збереження доказів. Верифікація отриманих матеріалів передбачає встановлення автентичності, атрибуції й контексту їх виникнення; методика збору й аналізу має бути описана таким чином, щоб стороні захисту та суду була забезпечена можливість незалежної перевірки (відтворення) результатів (з урахуванням орієнтирів Berkeley Protocol, ENFSI, NIST та відповідних настанов Європарламенту й ОБСЄ) [2; 9; 10; 12; 16; 21].

Враховуючи підхід ЄСПЛ до якості закону й пропорційності, а також національні вимоги до процесуальних документів, рекомендована послідовність дій для оперативних підрозділів і слідчих/детективів така: «виявлення → збереження → перевірка → протоколювання». *На етапі виявлення* здійснюється швидке картографування on-chain руху вартості з виявленням «критичних вузлів» (біржі, шлюзи, VASPs) та паралельний OSINT-збір; *на етапі збереження* здійснюється створення судово-технічних (комп'ютерно-технічних) знімків екрана та скрінкастів, експорт даних із блокчейн-оглядачів *(explorers)* та програмних інтерфейсів прикладних систем (API) із детальним описом використаних інструментів, їхніх версій і конфігурацій; формується хеш-таблиця відповідності між «сирими» та робочими копіями даних; ініціюються термінові процесуальні запити до провайдерів послуг у сфері віртуальних активів (VASPs) щодо замороження активів *(freeze-звернення)* та збереження журналів доступу і матеріалів KYC/AML-ідентифікації; *на етапі перевірки* – здійснюється дублювання експорту даних альтернативними інструментами та незалежна верифікація отриманих результатів; проводиться перехресна перевірка висновків, отриманих із блокчейна (on-chain), із позаблокчейновими матеріалами (off-chain) шляхом зіставлення транзакційних графів із KYC / логами доступу, платіжними слідами й іншими позаблокчейновими джерелами; фіксуються розбіжності, їхня інтерпретація та оцінка ризику хибнопозитивних інференцій; *на етапі протоколювання* – у процесуальному документі детально описуються джерела даних, застосовані алгоритми й евристики трасування, параметри інструментів (назва ПЗ, версія, конфігурація), методи експорту й трансформації даних, часові мітки, середовище збору та відповідальні особи; окремим додатком до протоколу додаються хеш-таблиці «сирі ↔ робочі копії», контрольні логи, конфігураційні файли та вказівки щодо меж технічної похибки й процедур незалежної перевірки (реплікації) отриманих результатів [2; 9; 12; 21; 44; 54–56].

Залежно від складу злочину, підвідомчості та підслідності, а також форми провадження дії з документування і збереження цифрових слідів здійснюють працівники оперативних і контррозвідувальних підрозділів під час ОРД/КРД, чи слідчі / детективи під час досудового розслідування; у всіх випадках потрібні чітка процесуальна форма й дотримання стандартів прав людини та транскордонної співпраці [7; 44; 55; 56].

Ланцюг збереження доказів *(chain of custody)* вимагає фіксації першоджерела (URL, хеші

сторінок / файлів, час / часовий пояс), середовища збору жоказів (ОС, мережеві параметри), інструментів і їх версій / конфігурацій, а також контрольних логів; незмінність забезпечується створенням «сирих» і робочих копій та збереженням їх хеш-значень у протоколі [2; 9; 10; 12; 16].

Для *відтворюваності (reproducibility)* методика має описувати алгоритми трасування, застосовані евристики, межі похибки та процедури незалежної перевірки стороною захисту (повторний експорт, альтернативні інструменти, звірка хешів «сирих» і робочих копій) [2; 9; 10; 12]. *Протокольні рішення* при роботі з «живими» вебджерелами, сторінками бірж і API-викликами передбачають скрінкасти або форензійні знімки із фіксацією метаданих, журналів мережевих запитів і часу, додаванням до протоколу хеш-таблиць і конфігурацій; за потреби доступу до захищених даних або приватних записів провайдерів слідчий / детектив забезпечує належну авторизацію (судовий дозвіл) та відображає її реквізити у процесуальному документі [2; 9; 12; 44]. Окремі процесуальні акти щодо осіб зі спеціальним статусом здійснюються *лише* суб'єктами з виключною компетенцією; делегування таких повноважень *не допускається*, а *порушення порядк*у нівелює правові наслідки процесуального акту [57].

Транскордонне одержання позаблокчейнових матеріалів *(off-chain)* (KYC/AML-пакети, журнали доступів, записи рахунків, договори, кореспонденція підтримки) здійснюється через Європейський ордер на розслідування або інші канали міжнародної допомоги; при цьому дотримуються вимоги законності, необхідності й пропорційності втручання, визначені практикою ЄСПЛ [7; 55; 56]. Для провайдерів діють стандарти FATF щодо віртуальних активів і VASP (R.15/INR.15), а також правила «подорожуючої інформації» TFR; їх виконання створює структуровану доказову базу (ідентифікаційні дані відправника/одержувача, маршрути, провайдери), яку потрібно своєчасно консервувати [14; 22].

Особливості так званого «невідкладного збереження» цифрових даних зумовлені високим ризиком їх швидкої втрати, що потребує негайної фіксації цифрових слідів із дотриманням вимог щодо забезпечення їх цілісності та достовірності (видалення акаунтів, ротація логів, зміна конфігурацій сервісів). У таких випадках ініціюються звернення про тимчасове збереження даних (freeze-запити) до постачальників послуг у сфері віртуальних активів (VASPs) чи криптовалютних бірж, фіксуються контрольні знімки та експорти з інструментів із негайним хешуванням, а в протоколі зазначаються часові межі зберігання даних у провайдерів і здійснені дії щодо їх продовження [2; 9; 10; 21].

Судова й відомча практика деталізує допустимість використання даних бірж і блокчейн-трасування (ідентифікація контролю над гаманцем, кореляція адрес з особою) та підходи до конфіскації / спеціальної конфіскації цифрових активів; ці орієнтири слід відтворювати у протоколі описуються методика та параметри збору, забезпечуючи відтворюваність і можливість незалежної перевірки результатів стороною захисту та судом [28; 29; 31; 32; 33].

Нарешті, у національному контексті документування має відповідати вимогам КПК України та узагальненням щодо цифровізації провадження, а процесуальний контроль суду – перевіряти ланцюг збереження, прозорість методики та відповідність зібраних матеріалів стандартам належності й допустимості [44; 54].

Ідентифікацію суб'єкта та ланцюга бенефіціарів здійснюють, залежно від складу злочину, підвідомчості та підслідності, як працівники оперативних і контррозвідувальних підрозділів органів правопорядку, так і слідчі / детективи; базовим є дотримання KYC/AML-стандартів провайдерів віртуальних активів та вимог до «подорожуючої інформації», що задають мінімальний доказовий набір: установчі та верифікаційні дані клієнта (ID), реєстраційні й платіжні атрибути, журнали доступу та IP/пристроїв, історія транзакцій, ризик-профілі й журнали комплаєнс-перевірок [12; 14; 21; 22].

Повнота таких пакетів перевіряється через внутрішні політики VASP і державний нагляд, а у транскордонних епізодах – через інструменти міжнародної допомоги (Європейський ордер на розслідування) та канали взаємодії з іноземними провайдерами [7; 12; 21]. Встановлення відповідності («люстра») між блокчейн-адресами та конкретними фізичними або юридичними особами досягається шляхом поєднання кластеризації на основі даних, зафіксованих у блокчейні (on-chain), і графового аналізу з інформацією поза межами блокчейна (off-chain), зокрема матеріалами ідентифікації клієнтів (KYC), журналами доступу криптовалютних бірж, платіжними слідами та службовою кореспонденцією із сервіс-провайдерами. При цьому необхідно враховувати поширені схеми ухилення від ідентифікації, зокрема

використання мікшерів та «тумблерів», криптовалют із підвищеним рівнем конфіденційності (privacy-coins), практики переходу між ланцюгами блокчейнів (chain-hopping) і застосування міжланцюгових (крос-чейн) мостів. Важливо документувати не лише сам трансформаційний маршрут криптоактивів, а й точки їх входу та виходу через регульовані сервіси [3; 4; 21; 25; 26].

Судова практика підтверджує як можливість, так і належність використання даних криптовалютних бірж та результатів блокчейн-трасування з метою доведення фактичного контролю особи над криптогаманцем і встановлення зв'язку між конкретною адресою та її користувачем (справи *Gratkowski, Ulbricht, Sterlingov*). У цих рішеннях також формуються підходи до правового механізму конфіскації цифрових активів, а також до застосування судових викликів (subpoena) та запитів до постачальників цифрових послуг у поєднанні з міжнародними запитами про правову допомогу [7; 28; 29; 31–33].

Показові кримінальні провадження щодо діяльності криптовалютних провайдерів демонструють істотну доказову вагу досьє з ідентифікації клієнтів (KYC), журналів доступу, матеріалів щодо санкційного статусу, реєстрації та внутрішніх політик з дотримання вимог фінансового моніторингу (комплаєнсу) для атрибуції бенефіціарних власників і встановлення ролі постачальників віртуальних активів (VASPs) як посередників. Також вказані провадження виявляють тісний взаємозв'язок між доказуванням та режимами ринкового нагляду й державної реєстрації суб'єктів [1; 11; 13; 34–36].

У підсумку, належна ідентифікація особи як учасника правовідносин з криптоактивами спирається на триєдину методологію: (1) технічно верифіковані висновки, отримані з блокчейн-аналізу (on-chain); (2) повні та автентичні масиви даних KYC і логів доступу (off-chain); (3) матеріали міжнародної правової взаємодії, здобуті з дотриманням процесуальних гарантій і принципу відтворюваності (реплікативності) методики, необхідної для перевірки стороною захисту [2; 7; 12; 21].

У транскордонних кримінальних епізодах базовими інструментами отримання позаблокчейнових (off-chain) матеріалів – таких як журнали доступу, ідентифікаційно-фінансові пакети KYC/AML, виписки з рахунків, копії договорів та службова кореспонденція провайдерів – є механізми міжнародної правової допомоги та адресні запити до постачальників послуг, пов'язаних із віртуальними активами (VASPs) і криптовалютних бірж. З метою оперативної та формалізованої передачі електронних доказів активно застосовується Європейський ордер на розслідування (EIO). Одночасно використовуються термінові канали збереження даних (preservation / freeze-requests), які спрямовані на попередження втрати журналів доступу та технічних записів [7; 11; 12; 21].

Додатковий регуляторний контур формують стандарти Групи розробки фінансових заходів боротьби з відмиванням грошей (FATF) щодо віртуальних активів і постачальників відповідних послуг (рекомендація 15 та її тлумачення – R.15/INR.15), а також правила «подорожуючої інформації» (Travel Rule), передбачені Регламентом ЄС про перекази коштів (TFR). Вказані акти покладають на провайдерів обов'язок зберігати та передавати ідентифікаційні дані, що супроводжують транзакції, що, у свою чергу, істотно підвищує доказову цінність отриманих інформаційних пакетів [14; 22].

Для забезпечення допустимості таких даних в українському кримінальному провадженні необхідне чітке узгодження формальних вимог іноземної юрисдикції з процесуальною формою українського права. Це передбачає процесуальну перевірку достовірності та належності отриманих доказів шляхом належного опису джерела й каналу передачі, підтвердження автентичності, повноти та цілісності інформації, документування застосованих інструментів, версій програмного забезпечення, конфігурацій, а також хешування як «сирих» копій, так і робочих екземплярів файлів відповідно до вимог Берклійського протоколу, настанов Європейської мережі судово-експертних установ (ENFSI) та орієнтирів Європейського парламенту [2; 9; 10; 12]. Усі ці дії забезпечують відтворюваність цифрового доказу та його подальшу перевірюваність у суді.

Додаткові орієнтири для формування запитів, процесуального впорядкування доказової інформації та її подальшого використання у кримінальному провадженні містяться в практичних керівництвах для правоохоронних органів, зокрема у матеріалах Організації з безпеки і співробітництва в Європі (OSCE), а також у судових та координаційних оглядах Євроюсту (Eurojust), які дають змогу конкретизувати адресність вимог до постачальників послуг у сфері віртуальних активів (VASPs) і криптовалютних бірж, а також визначити очікуваний «мінімальний набір» технічних полів у відповідях [11; 21].

З урахуванням притаманних міжнародному обміну ризиків – таких як відмова у наданні інформації, часові затримки, фрагментарні відповіді – доцільним є проведення попередньої кореляції запитуваної інформації з відкритими джерелами (OSINT) та результатами аналізу блокчейнових транзакцій *(on-chain)* ще на етапі ініціювання запиту, що дозволяє обґрунтувати його релевантність і підвищити його ефективність. Крім того, рекомендується дублювати канали звернення – зокрема, шляхом одночасного направлення запиту у формі Європейського ордера на розслідування (EIO) та прямого запиту до провайдера (за наявності відповідної договірної чи процесуальної можливості), а також максимально конкретизувати у запиті предмет дослідження, часові рамки, технічні атрибути і поля. Для цього варто спиратися на аналітику ризиків, типові практичні кейси та профільні методичні матеріали [3; 4; 12; 30].

Усі дії, пов'язані з отриманням і подальшим використанням цифрових доказів, мають здійснюватися з дотриманням стандартів верховенства права, законності, необхідності та пропорційності втручання у приватне життя, сформульованих у практиці Європейського суду з прав людини. Це вимагає чіткої фіксації підстав і меж доступу до інформації, а також наявності ефективного процесуального контролю на національному рівні [44; 54; 55; 56].

Нарешті, з урахуванням нормативно визначених обов'язків провайдерів послуг, закріплених у Регламенті ЄС про ринки криптоактивів (MiCA) та Регламенті щодо передавання супровідної інформації про перекази коштів і криптоактивів (TFR), а також наглядових очікувань до їхньої діяльності, у змісті міжнародних і процесуальних запитів доцільно прямо посилатися на їхні обов'язки щодо ведення обліку, зберігання та забезпечення передачі «подорожуючої інформації»[1]. Це полегшує встановлення бенефіціарної приналежності транзакцій і дозволяє здійснити подальшу інтеграцію отриманих позаблокчейнових матеріалів з висновками, сформованими на основі блокчейнового аналізу (on-chain) [22; 23].

Судова практика Сполучених Штатів Америки підтверджує допустимість використання даних криптовалютних бірж і результатів графового аналізу для доведення фактичного контролю особи над криптогаманцем і подальшої конфіскації цифрових активів, що засвідчено, зокрема, у справах *Gratkowski, Ulbricht, Sterlingov*. Водночас політики Міністерства юстиції США щодо конфіскації цифрових активів містять структуровані вимоги до їх збереження, атрибуції та фіксації доказового ланцюга. У справах, пов'язаних із ринковим наглядом і регуляторним статусом криптоактивів *(SEC v. Coinbase, Kraken, Ripple)*, суди додатково конкретизують юридичні ознаки, що породжують похідні джерела доказів – документи розкриття, ліцензійні матеріали, комплаєнс-звіти тощо [28; 29; 31; 32–36].

У національному контексті питання належності цифрових доказів охоплює також необхідність звірки з даними декларування та оподаткування – зокрема, встановлення походження й вартості активів – що є ключовим для розслідування злочинів, пов'язаних із незаконним збагаченням, одержанням неправомірної вигоди та іншими корупційними правопорушеннями. Додатково потребується узгодження з вимогами кримінального процесуального законодавства України та антикорупційної правозастосовної практики [18; 20; 41; 44; 54].

У підсумку, цифровий доказ визнається одночасно належним і допустимим, якщо він отриманий із дотриманням принципу законності доступу, забезпечує процесуальну відтворюваність та криміналістичну перевірюваність результатів фіксації, узгоджується з іншими джерелами доказової інформації як у межах ланцюга транзакцій (on-chain), так і поза ним (off-chain), а також надає суду можливість здійснити повноцінну, всебічну та мотивовану оцінку з урахуванням стандартів Європейського суду з прав людини щодо права на приватність, змагальності та процесуальної справедливості [2; 7; 9; 10; 12; 44; 54–56].

Алгоритм доказової інтеграції в подібних справах доцільно реалізовувати поетапно. Сама логіка комплексних актів (складання, вручення,

[1] У процесуально-криміналістичному розумінні йдеться про нормативно регламентований обіг даних, що супроводжують фінансові або криптоактивні трансакції, зокрема ідентифікаційні відомості про відправника, отримувача, мету операції та пов'язані KYC/AML-атрибути. Така інформація, що «подорожує» разом із транзакцією через мережу постачальників послуг віртуальних активів, становить *частину ланцюга доказового походження електронних даних*, з огляду на її роль у відтворенні фактичного шляху активів, зв'язків між учасниками та джерела фінансування.

Посилання на ці обов'язки у запитах – як до постачальників послуг (VASPs), так і до компетентних органів держав-членів ЄС – надає процесуальному зверненню *юридично обґрунтованого характеру* та підсилює його доказову вагу, оскільки забезпечує прив'язку вимоги до встановлених регуляторних стандартів належного зберігання й передачі «подорожуючої інформації» у межах контролю за фінансовими потоками та запобігання легалізації злочинних доходів.

роз'яснення прав, внесення до ЄРДР) демонструє, що *кожен елемент* має бути *окремо зафіксований* у протоколах/додатках [57, с. 59]. *На першому* етапі слід сформулювати фабулу правовідносин і чітко визначити процесуальну роль криптовалюти в межах провадження – як об'єкта, предмета чи засобу вчинення злочину, з подальшим закріпленням наслідків для кваліфікації, визначенням елементів предмета доказування та типових джерел інформації [42; 43; 48; 49]. *Далі* вибудовується план збирання доказів за логікою *"on-chain → off-chain → OSINT"*, із картографуванням критичних вузлів цифрової інфраструктури (біржі, платіжні шлюзи, VASP-провайдери, криптосервіси) та визначенням першочергових дій для їх швидкої консервації [3; 21; 25; 26].

Наступний крок передбачає консервацію, протоколювання та хешування цифрових слідів: створення «сирих» і робочих копій, побудову хеш-таблиць, фіксацію джерела, часу та середовища збору, а також повний опис інструментів, версій і конфігурацій, які були використані під час добування інформації – що є передумовою відтворюваності результатів [2; 9; 10; 12; 16]. *Далі* здійснюється одержання позаблокчейнових *(off-chain)* матеріалів – KYC/AML-пакетів, журналів доступу, біржових записів, договорів і службового листування – шляхом належних процесуальних запитів, зокрема транскордонних (через Європейський ордер на розслідування або MLAT), з урахуванням положень стандарту FATF R.15/INR.15 та правил зберігання і передавання ідентифікаційних даних у межах «подорожуючої інформації» (Travel Rule), передбачених Регламентами TFR та MiCA. Зібрані таким чином матеріали співставляються з висновками блокчейн-аналізу з метою підтвердження релевантності й належності інформації [7; 14; 21–23; 29].

На наступному етапі виконується експертна перевірка застосованої методики: здійснюється повторне відтворення результатів за допомогою інших інструментів, звіряються хеш-значення «сирих» і робочих копій, фіксуються межі технічної похибки та описуються застосовані евристики графового аналізу [2; 9; 10; 12; 16]. *Далі* готується доказовий блок для судової презентації: логічно структурований масив доказів із пояснювальними таблицями та схемами, що містить чіткі відповіді на контрольні питання суду – щодо джерела, законності доступу, авторизації, прозорості методики, відтворюваності та пропорційності втручання. На цьому етапі можуть бути корисними методичні рекомендації для суддів, координаційні огляди, а також національні процесуальні приписи й стандарти захисту прав людини [11; 28; 44; 55; 56].

Завершальним етапом є перевірка можливості перевірки доказу стороною захисту, що передбачає надання їй доступу до «сирих» даних, хеш-сум, конфігурацій інструментів та протоколів збору. Забезпечення такого доступу дозволяє стороні захисту поставити обґрунтовані контрекспертні питання, повторити аналітичні дії й здійснити перевірку достовірності доказів, що є ознакою дотримання принципу змагальності та підвищує доказову спроможність усього зібраного матеріалу як на досудовому слідстві, так і в суді [2; 9; 10; 12].

З урахуванням того, що дії з виявлення, документування та фіксації цифрових слідів у кримінальному провадженні здійснюються не лише слідчими, детективами та прокурорами, але й працівниками оперативних підрозділів у межах здійснення оперативно-розшукової діяльності, а у провадженнях щодо злочинів проти основ національної безпеки – також співробітниками підрозділів контррозвідувальної діяльності, доцільним є запровадження уніфікованого набору інструментів для всіх зазначених суб'єктів.

По-перше, це стандартизовані контрольні переліки, що охоплюють повний цикл роботи з цифровими слідами: від аналізу блокчейн-даних *(on-chain)*, позаблокчейнових джерел (off-chain) та відкритих джерел розвідки (OSINT) до фіксації джерела, метаданих, часу, опису інструментів та їхніх версій, побудови хеш-таблиць для «сирих» і робочих копій. Такі переліки повинні також передбачати дотримання вимог законності доступу, зокрема з урахуванням механізмів транскордонної взаємодії (EIO/MLAT), принципу пропорційності втручання у приватність, забезпечення супровідної ідентифікаційної інформації щодо переказів *(Travel Rule)*, а також відповідність доказовим критеріям допустимості та належності, сформульованим як на національному, так і на міжнародному рівнях [2; 7; 9; 10; 12; 21–23; 44; 54–56].

По-друге, мають бути передбачені шаблони процесуальних і відомчих документів, адаптовані до різних стадій збору й використання цифрових слідів. Зокрема:

– *«Протокол (акт) огляду веб-ресурсу / API-ендпойнту»* – з полями для зазначення URL, дати й часу огляду, часової зони, мережевих журналів, параметрів запитів/відповідей, скрінкастів або форензійних знімків та їхніх хеш-значень;

– *«Додаток із хеш-таблицями»* – для документування ідентичності «сирих» і робочих копій;

– *«Опис інструментів і методики»* – з обов'язковим зазначенням програмного забезпечення, його версії, налаштувань, меж технічної похибки, застосованих евристик та результатів перевірки відтворюваності;

– *«Запит про міжнародну правову допомогу (EIO/MLAT)»* – з конкретизованими полями для KYC-даних, логів, записів рахунків і посиланням на регуляторні зобов'язання за MiCA/TFR;

– *"Freeze-request"* – запит про замороження активів, адресований криптобіржі чи VASP-провайдеру;

– *«Супровідний рапорт (ОРД/КРД)»* – документ, що забезпечує належну інтеграцію інформації, отриманої в межах оперативно-розшукової чи контррозвідувальної діяльності, у кримінальне процесуальне провадження [2; 7; 12; 21; 22; 23; 44].

По-третє, доцільним є формування мінімального пакета для судової перевірки та доступу сторони захисту, який забезпечує можливість незалежної реплікації отриманих результатів. Такий пакет має включати: сирі експорти (raw-exports) та контрольні знімки з хешами; журнали доступу та технічні логи; повний опис застосованих інструментів, версій та конфігурацій; опис методики аналізу; документи комплаєнсу провайдера (KYC/AML-пакети, внутрішні політики, підтвердження дотримання Travel Rule); реквізити авторизації доступу (ухвали слідчого судді, EIO/MLAT); підтвердження дотримання стандартів прав людини щодо законності, необхідності та пропорційності втручання. У справах із ризиками відмивання доходів або фінансування тероризму додатково мають бути враховані посилання на виконання рекомендацій FATF R.15/INR.15 та дотримання національного режиму протидії легалізації (відмиванню) доходів [14; 21; 22; 23; 51], а за наявності – також матеріали щодо конфіскації або спеціальної конфіскації та збереження цифрових активів [28].

Для визначення пріоритетності дій оперативних, контррозвідувальних, слідчих і процесуальних підрозділів доцільно орієнтуватися на оновлені кримінологічні та комплаєнс-звіти, аналітичні матеріали й координаційні огляди, підготовлені провідними міжнародними інституціями – зокрема *Chainalysis* (аналітична платформа з розслідування блокчейн-транзакцій), *TRM Labs* (система моніторингу ризиків у сфері віртуальних активів), Програмою співпраці в галузі боротьби з наркотиками та відмиванням коштів (COPOLAD), Програмою співпраці в галузі боротьби з наркотиками та відмиванням коштів (COPOLAD), Європейським координаційним центром з питань правосуддя (Eurojust), Європейським парламентом та Організацією з безпеки і співробітництва в Європі (ОБСЄ). Зазначені документи містять практичні рекомендації щодо обґрунтування релевантності запитів до постачальників послуг у сфері віртуальних активів (VASP), ідентифікації критичних вузлів криптоекосистеми та мінімізації ризиків втрати доказової інформації на всіх етапах її збирання й фіксації [3; 4; 11; 12; 21; 25; 26].

Межі допустимих інтерпретацій результатів аналізу даних у блокчейні *(on-chain)* визначаються публічним характером самого реєстру та природою застосованих евристик. Зокрема, графові методи дозволяють виявляти кореляції між окремими адресами або кластерами, однак самі по собі не забезпечують достовірної особистої атрибуції без незалежних позаблокчейнових *(off-chain)* підтверджень – таких як досьє клієнта *(KYC)*, журнали доступу, платіжні сліди. Саме тому сучасні стандарти належності цифрових доказів вимагають не лише доказової надмірності *(redundancy of proof)*, але й прозорого опису застосованих припущень, меж технічної похибки та методологічних обмежень [2; 8–11; 21].

За умов використання мікшерів, протоколів з підвищеним рівнем конфіденційності, децентралізованих фінансових сервісів *(DeFi)* або у разі багаторазових транзакцій між різними блокчейнами *("chain-hopping")*, істотно зростає ризик формування хибнопозитивних зв'язків, що потребує попередньої валідації шляхом співставлення з даними, отриманими від постачальників послуг у сфері віртуальних активів, та обов'язкового дотримання вимог щодо збереження і передачі супровідної ідентифікаційної інформації відповідно до правила «подорожуючої інформації» *(Travel Rule)* [3; 4; 22–26].

У транскордонному вимірі стандарти доказової достатності ґрунтуються на комбінації формалізованих інструментів доступу до цифрових даних, зокрема Європейського ордера на розслідування (EIO), дотримання процесуальної форми національного законодавства, а також вимог до цифрової криміналістики (форензіки): чітка ідентифікація джерела, збереження метаданих, хешування «сирих» і робочих копій, опис використаних інструментів, їхніх версій та конфігурацій [2; 7; 9; 10; 12; 16; 44; 54].

Європейський суд з прав людини у своїй усталеній практиці сформулював імперативні процесуально-правові межі допустимого втручання держави у сферу приватного життя, які охоплюють критерії законності, необхідності у демократичному суспільстві та пропорційності поставленій меті. Ці межі визначають не лише формальні умови легітимності втручання, а й обсяг обов'язку держави забезпечити його процесуальну перевірюваність.

У контексті кримінального провадження це означає, що сторона обвинувачення зобов'язана довести не лише техніко-процесуальну коректність способу одержання цифрових доказів, а й наявність реального та ефективного судового контролю, який забезпечує передбачуваність, підзвітність і можливість перевірки втручання у приватність. Одночасно суд має надати вмотивовану оцінку кожному випадку обмеження прав людини, засвідчивши, що таке втручання було обґрунтованим, пропорційним і невід'ємним від завдань кримінального правосуддя, а не здійснювалося з надмірним чи дискреційним відхиленням від принципу верховенства права [50; 52; 55].

Узгодження технічних та процесуальних вимог проявляється в трьох ключових аспектах. *По-перше, відтворюваність (reproducibility):* методика збору й аналізу цифрових доказів має бути описана таким чином, щоб сторона захисту могла здійснити незалежну перевірку результатів. Це зумовлює обов'язковість ведення хеш-таблиць, журналів дій та детального опису параметрів інструментів і середовища збору [2; 9; 10; 12; 16].

По-друге, належність: будь-які аналітичні висновки, зроблені на основі on-chain аналізу, повинні бути підтверджені незалежними off-chain джерелами, отриманими в установленому законом порядку, у тому числі через механізми міжнародної правової допомоги (EIO/MLAT) [7; 11; 21].

По-третє, регуляторний контур: обов'язки постачальників послуг у сфері віртуальних активів (VASP) щодо збереження й передачі ідентифікаційних атрибутів переказів відповідно до Регламенту TFR та вимоги щодо ринкового комплаєнсу, закріплені в Регламенті MiCA, формують структуровані масиви даних. Проте процесуальна якість таких даних безпосередньо залежить від правильності формулювання запитів, дотримання встановлених процедур нагляду та наявності судового контролю [22; 23].

Ризики використання автоматизованих інструментів аналізу без належного судового контролю полягають у непрозорості алгоритмів обробки даних, прихованих евристичних припущеннях та використанні так званих «чорних скриньок» візуалізації графових зв'язків. За таких умов суди вимагають забезпечення пояснюваності результатів, опису джерел потенційних похибок, меж застосовності інструментів та можливості незалежної перевірки отриманих висновків.

Судова практика Сполучених Штатів демонструє, що дані криптовалютних бірж і результати блокчейн-трасування можуть визнаватися належними доказами лише за умови дотримання процесуальної дисципліни, наявності чіткої атрибуції та забезпечення прозорої методології фіксації цифрових слідів [28; 29; 31–33]. Водночас регуляторні провадження, зокрема у справах *SEC v. Coinbase, Kraken та Ripple*, ілюструють, що віднесення токенів до категорії цінних паперів породжує низку похідних джерел доказової інформації – документи про розкриття інформації, матеріали ліцензування, комплаєнс-політики, – які підлягають інтеграції у кримінальні провадження із дотриманням вимог автентичності та належного ланцюга збереження *(chain of custody)* [34–36].

Національний правовий контекст зумовлює додаткові процесуальні та криміналістичні вимоги до встановлення фактичних обставин, пов'язаних із володінням і використанням цифрових активів. Податкові та деклараційні обов'язки осіб виступають істотним елементом доказування, оскільки вони безпосередньо впливають на правову кваліфікацію походження активів, визначення їх законного статусу, а також оцінку вартості в аспекті можливого незаконного збагачення, одержання неправомірної вигоди чи зловживання службовим становищем.

У кримінальному процесі ці дані мають доказове значення для встановлення відповідності майнового стану суб'єкта його офіційним доходам, ідентифікації джерел формування цифрових активів, а також розмежування законних і тіньових фінансових потоків, що використовуються у схемах легалізації чи приховування неправомірних доходів. Такий підхід забезпечує не лише економічно-фінансову, але й процесуально-правову атрибуцію цифрових активів, перетворюючи їх на предмет об'єктивного аналізу у доказуванні корупційних злочинів.

При цьому судова практика України характеризується підвищеними вимогами до фіксації цифрових слідів, обґрунтування їх належності та допустимості, а також до мотивування

процесуального рішення щодо визнання таких даних доказами [18; 20; 38–41; 44; 54].

Узагальнюючи, межі допустимих інференцій (висновків) у кримінальному провадженні визначаються тим, наскільки прозоро, обґрунтовано та відтворювано сторона обвинувачення поєднує висновки блокчейн-аналізу *(on-chain)* з незалежними позаблокчейновими джерелами (off-chain), дотримується процедур міжнародного правового доступу (зокрема через Європейський ордер на розслідування або MLAT), а також відповідає вимогам законності, необхідності та пропорційності втручання, сформульованим у практиці Європейського суду з прав людини.

Доказова достатність у таких справах досягається не візуальною переконливістю графів, а якістю зібраного ланцюга збереження цифрових доказів і можливістю їх незалежної реплікації стороною захисту. Автоматизовані інструменти аналізу можуть застосовуватись виключно як частина відкритої методики, яка передбачає опис меж похибки, фіксацію всіх параметрів аналізу та підлягає процесуальному й судовому контролю. Отже, саме процесуальна форма є необхідною умовою трансформації технічних артефактів цифрового середовища у належні й допустимі докази в кримінальному судочинстві.

Таким чином криптовалюта як *об'єкт, предмет та засіб* вчинення злочину це не лише теоретичні категорії: воно детермінує структуру предмета доказування, допустимі процесуальні інструменти доступу, джерела on-/off-chain та модель судового контролю. Для всіх категорій справ обов'язковими є: (1) *прозора методика* (опис інструментів/версій, межі евристик, параметри збору); (2) *відтворюваність* (хеш-таблиці «сирі ↔ робочі копії», журнали мережевих звернень, конфігурації); (3) *легітимні канали доступу* (EIO/MLAT, процесуальні ухвали, Travel Rule/MiCA-зобов'язання провайдерів) із дотриманням тестів законності, необхідності та пропорційності. Усі аналітичні висновки on-chain підлягають *верифікації незалежними off-chain джерелами* (KYC/лог-дані/комплаєнс-матеріали) і включаються до процесуальних документів так, щоб сторона захисту мала *реальну можливість незалежної реплікації.*

Зазначені гарантії не є «надмірним формалізмом»: за відсутності належної суб'єктності /процедури доступу або дефектів у ланцюгу збереження ризик недопустимості даних зростає кратно. Саме тому поряд із технічною коректністю техніко-криміналістичних дій вирішального значення набуває процесуальний механізм – від обґрунтованого вибору належного інструмента міжнародної правової допомоги та визначення адресності запиту до послідовної фіксації кожного етапу збирання, перевірки й аналітичної обробки даних.

Запропонована методична конструкція «роль → наслідки → стратегія доказування» у поєднанні зі стандартизованими протоколами фіксації цифрових слідів забезпечує перетворення технічних артефактів цифрового середовища на належні й допустимі докази, придатні для судової оцінки.

Висновки. Стаття окреслює цілісний цикл роботи з криптоактивами в оперативно-розшуковій, контррозвідувальній діяльності та у кримінальному провадженні – від виявлення і документування до доказування на досудовій та судовій стадіях, з повноважень оперативних і контррозвідувальних підрозділів та процесуального статусу слідчих (детективів), прокурорів, захисників і суддів.

По-перше, Ефективне реагування органів правопорядку на вчинення кримінальних правопорушень з використанням криптовалюти розпочинається з належного виявлення інформаційних слідів події. На початковому етапі ОРД чи досудового розслідування ключовим є формування структурованої карти джерел відомостей за логікою послідовності: *внутріш-ньоланцюгові дані (on-chain) – позаланцюгові джерела (off-chain) – відкриті розвідувальні відомості (OSINT).* Такий підхід забезпечує комплексне охоплення інформаційного простору та своєчасне виявлення взаємозв'язків між учасниками транзакцій. Важливо оперативно ідентифікувати критичні вузли цифрової інфраструктури – криптовалютні біржі, платіжні шлюзи, постачальників послуг у сфері віртуальних активів (VASP), а також невідкладно здійснити консервацію релевантних цифрових слідів та ініціювати термінові канали їх збереження (freeze / preservation), що гарантує цілісність і доказове значення даних у подальшому процесуальному використанні.

По-друге, документування цифрових слідів має здійснюватися з дотриманням принципів цифрової криміналістики, відтворюваності та процесуальної надійності, що забезпечує їх належність, допустимість і достовірність у структурі доказування. Така діяльність вимагає суворої фіксації джерела, часу, способу та середовища отримання даних; здійснення хешування

«сирих» і робочих копій з відповідним зазначенням алгоритму; детального опису застосованих інструментів, версій програмного забезпечення, параметрів конфігурацій і технічних протоколів. Обов'язковим є протокольне оформлення API-запитів, звернень до вебджерел і службової кореспонденції, що підтверджують процес збору та передачі інформації. Безперервність і простежуваність ланцюга збереження цифрових слідів (майбутніх цифрових доказів у кримінальному провадженні – *(chain of custody)* мають гарантувати неможливість модифікації чи втрати даних, а також забезпечувати автентичність цифрового доказу на всіх етапах його кримінального процесуального доказування.

По-третє, доказування на стадії досудового розслідування має здійснюватися на основі інтеграції аналітичних висновків, отриманих із блокчейна *(on-chain)*, із незалежними позаланцюговими джерелами *(off-chain)* – такими як KYC/AML-досьє, журнали доступу, банківські виписки, договори, платіжні сліди, – що одержані у спосіб, передбачений законом, зокрема через механізми міжнародної правової допомоги. Така інтеграція спрямована на формування цілісної системи доказів, у якій цифрові відомості підтверджуються матеріальними чи документальними даними, отриманими з офіційних джерел. Водночас необхідним є чітке розмежування між фактичними даними, які становлять об'єктивну основу доказування, та аналітичними або експертними судженнями, що мають оцінювальний характер. Забезпечення можливості незалежної перевірки, відтворення та експертної перевірки результатів стороною захисту є проявом дотримання принципів змагальності, рівності процесуальних прав сторін і забезпечення справедливості кримінального провадження.

По-четверте, на судовій стадії визначального значення набувають відкритість та верифікованість застосованої методики, її наукова обґрунтованість, технічна відтворюваність і дотримання принципу пропорційності втручання у права та свободи особи. Судова оцінка цифрових доказів має спиратися на достовірні дані, перевірюваність способів їх одержання та суворе дотримання процесуальної форми. Суд повинен встановити джерело походження інформації, спосіб і умови її отримання, межі допустимої технічної похибки, а також виявити наявність кореляційного зв'язку між внутрішньоланцюговими *(on-chain)* та позаланцюговими *(off-chain)* даними, що гарантує системність і цілісність доказової бази. Водночас стороні захисту має бути забезпечене право на незалежну перевірку, повторне відтворення та експертну оцінку результатів на підставі наданих матеріалів, що становить необхідну передумову реалізації принципів змагальності, рівності процесуальних можливостей і справедливого судового розгляду.

До практичних пропозицій для вдосконалення нормативних актів та відомчих методик належать такі положення:

1. *Закріплення у відомчих нормативних актах класифікації ролей криптовалюти – як об'єкта посягання, предмета злочину та засобу його вчинення* – є необхідною умовою формування єдиної методичної бази для документування та доказування кримінальних правопорушень у сфері обігу віртуальних активів. Така класифікація має бути доповнена визначенням орієнтирів предмета доказування для типових складів злочинів, у яких криптовалюта виступає ключовим елементом кримінально-правового механізму – зокрема шахрайства, легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування забороненої чи терористичної діяльності, порушення вимог фінансового моніторингу та корупційних кримінальних правопорушень. Такий підхід забезпечує уніфікацію оперативно-розшукових та криміналістично-процесуальних підходів до виявлення, фіксації, вилучення та оцінки цифрових активів як доказових об'єктів, що сприяє підвищенню ефективності досудового розслідування та забезпеченню принципу правової визначеності у сфері доказування, законності та верховенства права.

2. *Уніфікація контрольних переліків дій* для оперативних, контррозвідувальних підрозділів, слідчих (детективів) та прокурорів на всіх стадіях цифрового документування – від виявлення і фіксації до перевірки достовірності, автентичності та процесуального протоколювання – має на меті забезпечення послідовності, повноти й відтворюваності процесу отримання цифрових доказів. Такі переліки повинні включати стандартизовані поля для фіксації звернень щодо тимчасового збереження даних *(preservation / freeze requests)*, оформлення міжнародних запитів про правову допомогу та виконання вимог правила «подорожуючої інформації» *(Travel Rule)*, яке регламентує передачу ідентифікаційних відомостей про ініціатора й одержувача транзакцій із віртуальними активами. Запровадження єдиних

контрольних форм забезпечує належний відомчий контроль та прокурорський нагляд, мінімізує ризики втрати цифрових доказів, підвищує доказову цінність зібраних матеріалів і сприяє дотриманню принципів законності, пропорційності та процесуальної узгодженості дій усіх суб'єктів доказування.

3. *Стандартизація методик і шаблонів документування* передбачає уніфіковане оформлення процесуальних і техніко-криміналістичних матеріалів, зокрема: протоколів огляду вебресурсів та API-ендпойнтів, додатків із хеш-таблицями, описів застосованих інструментів, їх версій і конфігурацій, а також оперативно-службових рапортів, призначених для подальшої процесуальної інтеграції у матеріали кримінального провадження.

До таких шаблонів належать і типові форми Європейського ордера на розслідування (EIO), запити про міжнародну правову допомогу (MLAT), а також звернення про тимчасове збереження даних (freeze-запити) до постачальників послуг, пов'язаних із віртуальними активами (VASP) чи криптовалютних бірж, що забезпечує належне документування цифрових доказів і їх подальшу допустимість у судовому доказуванні.

4. *Визначення мінімального пакета розкриття* для судової перевірки та сторони захисту має забезпечувати можливість незалежного відтворення результатів і перевірки достовірності цифрових доказів. До такого пакета доцільно включати: сирі *(raw)* експорти даних, контрольні хеш-значення, журнали доступу, методику дослідження з описом меж технічної похибки, підтвердження авторизованого доступу до джерел інформації, а також процесуальні гарантії збереження автентичності та цілісності цифрових слідів.

Такий підхід відповідає принципам змагальності, рівності сторін і належного судового контролю, забезпечуючи можливість самостійної криміналістичної перевірки кожного етапу отримання, фіксації та оцінки доказової інформації.

5. *Інтеграція до національних відомчих інструкцій* регуляторних вимог, визначених Регламентом ЄС про ринки криптоактивів (MiCA), Регламентом щодо передавання ідентифікаційних атрибутів (TFR), а також положень KYC/AML для постачальників послуг, пов'язаних із віртуальними активами (VASP), має на меті забезпечення процесуальної сумісності та уніфікації процедур ідентифікації учасників цифрових транзакцій.

Таке нормативне узгодження сприятиме спрощенню встановлення бенефіціарів операцій, підвищенню доказової спроможності отриманих позаланцюгових *(off-chain)* матеріалів, а також формуванню якісних доказових пакетів, придатних для процесуальної перевірки, експертного дослідження та судової оцінки відповідно до стандартів допустимості і достовірності цифрових доказів.

6. *Розроблення суддівського довідника (benchbook)* із системою контрольних запитань має на меті забезпечення єдності судової практики та підвищення якості судової оцінки цифрових доказів у кримінальному провадженні. Такий довідник покликаний слугувати інструментом практичного орієнтування суддів під час аналізу цифрових доказів, визначення їх належності, допустимості та достовірності. У його змісті доцільно передбачити контрольні запитання, спрямовані на з'ясування законності джерела походження доказу та дотримання процесуальних умов його одержання, пропорційності втручання у приватне життя та обґрунтованості обмеження прав людини, прозорості, відтворюваності й наукової обґрунтованості застосованої методики фіксації й аналізу цифрових слідів, а також кореляції та узгодженості між внутрішньоланцюговими *(on-chain)* і позаланцюговими *(off-chain)* даними, що формують сукупність доказової інформації. Упровадження такого довідника сприятиме належній процесуальній мотивації судових рішень, гармонізації підходів до оцінки цифрових доказів і реалізації принципів верховенства права, змагальності та справедливості судового розгляду.

7. *Запровадження міжвідомчих навчальних модулів і практичних симуляцій* для всіх суб'єктів кримінального провадження – працівників оперативних та контррозвідувальних підрозділів, слідчих (детективів), прокурорів, адвокатів і суддів – є необхідною умовою підвищення ефективності роботи з цифровими доказами у кримінальному процесі.

Такі програми мають бути орієнтовані на оперативну консервацію цифрових слідів, дотримання вимог міжнародної взаємодії, застосування інструментів блокчейн-трасування для виявлення та простеження руху активів, а також на підготовку процесуально повноцінного доказового пакета, придатного для судового розгляду та перевірки у межах змагальної процедури.

Комплексна реалізація цих заходів сприятиме уніфікації практики збирання й оцінки цифрових доказів, зміцненню гарантій їх допустимості

та формуванню належної професійної компетентності суб'єктів доказування відповідно до сучасних криміналістичних і процесуальних стандартів.

Запропонована нормативно-методична модель забезпечує інкорпорацію операційно-технічних дій у процесуальну форму та перетворює дані блокчейна і комплаєнс-масиви провайдерів на належні, допустимі, достовірні й відтворювані докази, що відповідають вимогам змагального кримінального процесу на досудовій і судовій стадіях.

Список використаної літератури:

1. Aux Cayes FinTech Co. Ltd. (d/b/a "OKEx," "OKX"). United States v. Aux Cayes FinTech Co. Ltd., No. 25-cr-00069 (S.D.N.Y.). Plea Agreement (Rule 11 (c) (1) (C)). URL: https://www.lit-wc.aoshearman.com/siteFiles/50508/%5BEnforcement%202%5D%20U.S.%20v.%20OKX%20Plea%20Agreement.pdf ; Statement of Facts (USAO-SDNY, PDF). URL: https://www.justice.gov/usao-sdny/media/1390641/dl?inline=
2. Berkeley Protocol on Digital Open Source Investigations. Geneva: OHCHR & UC Berkeley, 2020. URL: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source
3. Chainalysis. The 2025 Crypto Crime Report. 2025. URL: https://go.chainalysis.com/2025-Crypto-Crime-Report.html
4. COPOLAD. Financial Investigations and Analysis for Emerging Money Laundering Risks Related to Cryptoassets. 2025. URL: https://copolad.eu/wp-content/uploads/2025/02/COPOLAD_Publicaciones_Criptoactivos_English-1.pdf
5. Court of Justice of the European Union. Case C-264/14 Skatteverket v David Hedqvist. Judgment of 22.10.2015. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0264
6. DLA Piper. Blockchain and Digital Assets News and Trends – March 2025. 2025. URL: https://www.dlapiper.com/en/insights/publications/blockchain-and-digital-assets-news-and-trends/2025/blockchain-and-digital-assets-news-and-trends-march-2025
7. Directive 2014/41/EU of the European Parliament and of the Council regarding the European Investigation Order in criminal matters. OJ L 130, 01.05.2014, P.1–36. URL: https://eur-lex.europa.eu/eli/dir/2014/41/oj/eng
8. Dudani S. The current state of cryptocurrency forensics. Forensic Science International: Digital Investigation. 2023. URL: https://www.sciencedirect.com/science/article/pii/S2666281723000859
9. ENFSI. Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI-BPM-FIT-01).2015. URL: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf
10. ENFSI. Best Practice Manuals – Digital Forensics (index). 2015–2025. URL: https://enfsi.eu/documents/best-practice-manuals/
11. Eurojust. Cybercrime Judicial Monitor – Issue 9. July 2024. URL: https://www.eurojust.europa.eu/sites/default/files/assets/cybercrim-judicial-monitor-issue-9.pdf
12. European Parliament. Access to data for law enforcement: Digital forensics (EPRS Briefing 775879). 2025. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775879/EPRS_BRI(2025)775879_EN.pdf
13. Europol. Programming Document 2024–2026. 2024. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Programming_Document_2024-2026.pdf
14. FATF. Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (R.15/INR.15). 2024. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html
15. Katten Muchin Rosenman LLP. Crypto in the Courts: Five Cases Reshaping Digital Asset Regulation in 2025. 2025. URL: https://katten.com/crypto-in-the-courts-five-cases-reshaping-digital-asset-regulation-in-2025
16. Kent K., Chevalier S., Grance T., Dang H. Guidelines on Mobile Device Forensics (NIST SP 800-101, Rev. 1). Gaithersburg, MD: NIST, 2014. DOI: 10.6028/NIST.SP.800-101r1 URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf
17. Merkle Science. The DOJ's Most Important Crypto Prosecution Cases. 2025. URL: https://www.merklescience.com/blog/the-dojs-most-important-crypto-prosecution-cases
18. National Agency on Corruption Prevention (NACP). Cryptocurrency declaration: amounts and detected violations. 2025. URL: https://nazk.gov.ua/uk/novyny/deklaruvannya-kryptovalyuty-sumy-ta-vyyavleni-porushennya/
19. National School of Judges of Ukraine. Подкаст «Криптоактиви і суд. Як це працює?». 2025. URL: https://court.gov.ua/archive/1827380/
20. National Securities and Stock Market Commission of Ukraine. Матриця оподаткування віртуальних активів. 2025. URL: https://www.nssmc.gov.ua/wp-content/

uploads/2025/04/matrytsia-opodatkuvannia-va-1.pdf
21. OSCE. Decoding Crypto Crime – A Guide for Law Enforcement. 2025. URL: https://www.osce.org/oceea/587475 PDF: https://www.osce.org/files/f/documents/2/1/587475.pdf
22. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets (TFR). OJ L 150, 09.06.2023, P. 1–39. URL: https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng
23. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets (MiCA). OJ L 150, 09.06.2023, P. 40–205. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng
24. Sezonov V. The role of forensic expertise in the investigation of crimes related to forgery of digital documents and cryptocurrencies. *Juridica.* 2025. URL: https://revistas.rcaap.pt/juridica/article/view/40167
25. TRM Labs. 2025 Crypto Crime Report: Trends and Analysis. 2025. URL: https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report
26. TRM Labs. Now Live: The 2025 Crypto Crime Report. 2025. URL: https://www.trmlabs.com/resources/blog/now-live-the-2025-crypto-crime-report
27. TRM Labs. FATF updates on Recommendation 15 implementation (analytics). 2025. URL: https://www.trmlabs.com/resources/blog/fatf-updates-on-recommendation-15-implementation-in-jurisdictions-with-materially-important-virtual-asset-sectors
28. U. S. Department of Justice. *Asset Forfeiture Policy Manual.* 2025. URL: https://www.justice.gov/criminal/criminal-afmls/file/839521/dl?inline=
29. U. S. Department of Justice. Cryptocurrency: An Enforcement Framework (Cyber-Digital Task Force). 2020/2021. URL: https://www.justice.gov/d9/pages/attachments/2021/01/20/cryptocurrency_white_paper.final_.pdf
30. U. S. Department of the Treasury. *National Money Laundering Risk Assessment 2024.* 2024. URL: https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf
31. United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020). Opinion. URL: https://law.justia.com/cases/federal/appellate-courts/ca5/19-50492/19-50492-2020-06-30.html
32. United States v. Sterlingov (Bitcoin Fog), No. 1:21-cr-00399 (D.D.C.). Memorandum Opinions & Orders. GovInfo forfeiture opinion (04.11.2024): URL: https://www.govinfo.gov/content/pkg/USCOURTS-dcd-1_21-cr-00399/pdf/USCOURTS-dcd-1_21-cr-00399-2.pdf ; Memo Opinion & Order (29.02.2024, hosted): URL: https://www.moneylaunderingnews.com/wp-content/uploads/sites/12/2024/03/District_of_Columbia_USA_v._STERLINGOV_Memo_Opinion_and_Order.pdf ; Docket: URL: https://www.courtlistener.com/docket/59988850/united-states-v-sterlingov/
33. United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017). Opinion. URL: https://law.justia.com/cases/federal/appellate-courts/ca2/15-1815/15-1815-2017-05-31.html
34. Securities and Exchange Commission v. Coinbase, Inc. and Coinbase Global, Inc., No. 1:23-cv-04738 (S.D.N.Y.). Opinion & Order (denying in large part Defendants' Rule 12 (c) motion), 27.03.2024, Dkt. 105. PDF: https://cases.justia.com/federal/district-courts/new-york/nysdce/1%3A2023cv04738/599908/105/0.pdf ; Compiled record (incl. Dkts. 105, 175): https://business.cch.com/srd/SECvCoinbase.pdf
35. Securities and Exchange Commission v. Payward, Inc. (Kraken), No. 3:23-cv-06003-WHO (N.D.Cal.). Order Denying Motion to Dismiss, 23.08.2024 (Re: Dkt. 25). PDF (hosted copy): https://www.skadden.com/-/media/files/publications/2024/11/inside-the-courts/sec-v-payward-inc.pdf ; GovInfo docket PDF: https://www.govinfo.gov/content/pkg/USCOURTS-cand-3_23-cv-06003/pdf/USCOURTS-cand-3_23-cv-06003-2.pdf
36. Securities and Exchange Commission v. Ripple Labs, Inc., No. 1:20-cv-10832 (S.D.N.Y.). Order & Final Judgment materials, 2025 (Doc. 989, 26.06.2025). PDF: https://www.nutter.com/assets/htmldocuments/SEC%20v%20Ripple%20Labs%202025.06.26.pdf ; SEC Litigation Release (08.07.2025): URL: https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26369
37. Yatsyk T. P., Shkelebey V. A. Розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2023. Вип. 80. Ч. 2. С. 219–223. URL: https://ekmair.ukma.edu.ua/bitstreams/aa91d8f5-a50f-49e6-9497-a9e4923e44f3/download
38. Вирок у справі № 569/10875/19 (провадження № 1-кп/569/876/19) / Рівненський міський суд Рівненської області. Повний текст. URL: https://reyestr.court.gov.ua/Review/82846071
39. Вирок у справі № 638/14394/18 (провадження № 1-кп/638/1276/18) від 05.10.2018 / Дзержинський районний суд м. Харкова. Повний текст. URL: https://reyestr.court.gov.ua/Review/76978584

40. Вирок у справі № 755/17724/17 (провадження № 1-кп/755/1227/17) від 08.12.2017 / Дніпровський районний суд м. Києва. Повний текст. URL: https://reyestr.court.gov.ua/Review/70845302
41. Вирок у справі № 991/1512/23 (провадження № 1-кп/991/25/23) від 27.11.2024 / Вищий антикорупційний суд. Повний текст. URL: https://iplex.com.ua/doc.php?regnum=123349217&red=100003508b6a1068a6e52617075203562acc4f&d=5
42. Казначеєва Д. В., Дорош А. О. Кримінальні правопорушення у сфері обігу криптовалюти. *Вісник Кримінологічної асоціації України.* 2021. № 2 (25). С. 149–157. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/10969
43. Каменський Д. В., Титаренко С. С. Віртуальні активи як інструмент легалізації майна, одержаного злочинним шляхом: порівняльно-правовий аспект. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2023. Вип. 80. Ч. 2. С. 41–52. DOI: https://doi.org/10.24144/2307-3322.2023.80.2.6 PDF: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/01/80_part_2.pdf
44. Кальман О. Г., Погорецький М. А. Рейдерство: причини та заходи протидії. *Вісник Запорізького юридичного інституту ДДУВС.* 2009. № 3. С. 150–160.
45. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/go/4651-17
46. Національна школа суддів України. *Подкаст «Криптоактиви і суд. Як це працює?».* 2025. URL: https://court.gov.ua/archive/1827380/
47. Огляд законодавства щодо регулювання віртуальних активів у сфері боротьби з відмиванням коштів та фінансуванням тероризму. Київ : Держфінмоніторинг за сприяння Координатора проєктів ОБСЄ в Україні, 2022. 587 с. URL: https://https://fiu.gov.ua/assets/userfiles/310/Різне/VirtualAssets.pdf
48. Пашко Д. В., Омельчук Л. В. Потреба визначення статусу криптовалют в Україні: економічні та кримінальні процесуальні аспекти. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2018. № 1. С. 173–179. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA%3D&2_S21STR=muvnudp_2018_1-2_31
49. Погорецький М. А. Нова концепція кримінального процесуального доказування. Вісник кримінального судочинства України. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf
50. Погорецький М. А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. Аналітично-порівняльне правознавство. 2025. № 4 (3). С. 269–279. DOI: https://doi.org/10.24144/2788-6018.2025.04.3.40. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42-2.pdf
51. Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів. Вісник кримінального судочинства. 2023. № 3–4. С. 84–102. DOI: 10.17721/2413-5372.2023.3-4/84-102. URL: https://vkslaw.knu.ua/wp-content/uploads/2025/05/visnyk_krim_sud_3-4_23_v2_250425_avt2-84-102.pdf
52. Погорецький М. А., Гринюк В. О. Повідомлення судді про підозру: проблемні питання правового регулювання, теорії та практики. Вісник кримінального судочинства. 2018. № 2. С. 58–71.
53. Погорецький М. А., Коровайко О. І. Застосування тимчасового доступу до речей і документів у справах організованих злочинних угруповань. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 1. С. 234–241.
54. Погорецький М. А., Шеломенцев В. Поняття кіберпростору як середовища вчинення злочинів. *Інформаційна безпека людини, суспільства, держави.* 2009. № 2. С. 77–81.
55. Погорецький М. А. Захисник – суб'єкт доказування на досудовому провадженні за чинним КПК України: проблемні питання. *Актуальні питання державотворення в Україні* : матеріали міжнародної науково-практичної конференції (м. Київ, 23 травня 2014 р.). Київ : Прінт-Сервіс, 2014. С. 480-482.
56. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 № 361-IX. URL: https://zakon.rada.gov.ua/go/361-20
57. Регламент (ЄС) 2023/1113 Європейського Парламенту і Ради від 31 травня 2023 р. про інформацію, що супроводжує перекази коштів та певних криптоактивів (TFR). OJ L 150, 09.06.2023, С. 1–39. URL: https://eur-lex.europa.eu/eli/reg/2023/1113/oj
58. Регламент (ЄС) 2023/1114 Європейського Парламенту і Ради від 31 травня 2023 р. Про ринки криптоактивів (MiCA). OJ L 150, 09.06.2023, С. 40–205. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj
59. European Court of Human Rights (Grand Chamber). Big Brother Watch and v. the United Kingdom. Judgment of 25.05.2021. URL: https://hudoc.echr.coe.int/eng?i=001-203614
60. European Court of Human Rights (Grand Chamber). Roman Zakharov v. Russia. Judgment of 04.12.2015. URL: https://hudoc.echr.coe.int/eng?i=001-159324

Pohoretskyi M. A. Cryptocurrency as an object, subject, and means of committing a crime: issues of detection, documentation, and proof in pre-trial and court proceedings

The article is devoted to the development of a systematic procedural approach to working with crypto-assets in criminal proceedings – from detection to judicial review. A model for the integration of digital evidence is proposed, which takes into account the functional participation of operational and counterintelligence units, investigators, prosecutors, and the court.

The purpose of the study is to define the legal classification of cryptocurrency roles (object, subject, instrument) and to elaborate a procedural and forensic framework ensuring the relevance, admissibility, and reproducibility of digital evidence at all stages of criminal proceedings. Special attention is given to the coordination of results of operational-search and counterintelligence activities with materials of the pre-trial investigation, the verification of their authenticity, and compliance with the chain of custody.

The methodological basis combines formal-legal and comparative-legal methods, involving the provisions of EU Regulations MiCA and TFR, the mechanisms of the European Investigation Order, and international treaties on mutual legal assistance. The research relies on international standards for the preservation and documentation of digital traces developed in the Berkeley Protocol, ENFSI and NIST guidelines, adapted to a triangulation model for verifying data from blockchain, off-chain, and open sources.

The scientific novelty lies in combining the classification "object – subject – instrument" with a step-by-step procedural algorithm for integrating digital evidence ("detection → fixation → verification → documentation → judicial assessment") and in constructing a legal correlation scheme "role of cryptocurrency – legal implications – evidentiary strategy."

The practical significance of the study consists in the development of unified checklists and documentation templates (protocols for inspecting web resources/API, hash tables, descriptions of tools, acts of operational-search and counterintelligence measures), a minimum disclosure package for judicial verification and the defence, as well as guidance for judges on assessing methodological transparency, reproducibility, and correlation between blockchain and off-chain data (on-chain ↔ off-chain).

The proposed procedural and criminalistic model ensures the transformation of technical and departmental information arrays – in particular, blockchain data, providers' compliance information, and the results of operational-search and counterintelligence measures – into a procedural form of evidence that meets the criteria of relevance, admissibility, and reliability, in accordance with the standards of a fair trial.

Key words: *cryptocurrency, blockchain, object of a crime, subject (corpus) of a crime, means of committing a crime, European Investigation Order (EIO), operational and investigative activity, pre-trial investigation, judicial proceedings, digital evidence, digital forensics.*

Дата першого надходження рукопису до видання: 25.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 30.09.2025