

УДК 343.13:343.9.024:336.744

DOI 10.33244/2617-4154.2(23).2026.330-340

Т. П. Яцик,*кандидат юридичних наук, доцент,**доцент кафедри фінансових розслідувань та економічної безпеки**Навчально-наукового інституту економічної безпеки та митної справи,**Державний податковий університет***T. P. Yatsyk,***Candidate in Law Sciences (Ph.D), Docent,**Associate Professor of the Department of Financial Investigations and Economic Security**of the Educational and Scientific Institute of Economic Security and Customs,**State Tax University**email: zvezda171088@gmail.com***ORCID 0000-0003-4207-4633;****Т. В. Черненко,***здобувачка освіти першого (бакалаврського) рівня**Навчально-наукового інституту економічної безпеки та митної справи,**Державний податковий університет***T. V. Chernenko,***Bachelor Student of the Educational and Scientific**Institute of Economic Security and Customs,**State Tax University**email: tannybs2005@gmail.com***ORCID 0009-0003-6158-162X**

ПРАВОВА ПРИРОДА ТА ОСОБЛИВОСТІ ПРОЦЕСУАЛЬНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З КРИПТОВАЛЮТОЮ

THE LEGAL NATURE AND CHARACTERISTICS OF PROCEDURAL SUPPORT FOR THE INVESTIGATION OF CRIMINAL OFFENSES RELATED TO CRYPTOCURRENCY



Ця робота ліцензується відповідно до [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

© Яцик Т. П., Черненко Т. В., 2026

Стаття спрямована на комплексне дослідження правової природи віртуальних активів у контексті кримінального судочинства України. Основна увага приділяється розмежуванню понять «віртуальний актив», «криптоактив» та «криптовалюта», а також розробці практичних рекомендацій щодо подолання процесуальних перешкод у разі накладення арешту на цифрові активи та їх визнання речовими доказами. Проведено критичний аналіз відповідності національного законодавства міжнародним стандартам, який висвітлює прогалини у вітчизняному правовому полі, що перешкоджають повноцінному використанню цифрових активів як об'єктів доказування.

У процесі дослідження використано сукупність загальнонаукових і спеціальних методів пізнання. Формально-логічний метод застосовано для уточнення понятійно-категоріального апарату. Порівняльно-правовий метод дав змогу зіставити українське законодавство з міжнародними стандартами (Регламент MiCA, Рекомендації FATF). Метод системно-структурного аналізу використано для вивчення технічної складової блокчейну та смарт-контрактів, а аналіз судової практики – для виявлення типових помилок слідства під час доведення контролю над активами.

Встановлено, що ключовою проблемою правозастосування є «нематеріальність» криптовалюти, яка стає підставою для відмов у накладенні арешту. Доведено, що для ефективного розслідування фокус доказування має зміститися з права власності на факт ексклюзивного володіння ключами доступу. Виокремлено основні методи ідентифікації власників активів: від аналізу електронних декларацій до використання спеціалізованого програмного забезпечення для деанонізації транзакцій. Розкрито роль смарт-контрактів як інструментів автоматизації злочинної діяльності та джерел доказової інформації.

Зроблено висновок про потребу в адаптації КПК України до цифрових реалій через визнання специфічної форми матеріальності віртуальних активів. Обґрунтовано, що подолання транскордонності криптозлочинів можливе лише через імплементацію міжнародних стандартів прозорості та розширення інструментарію блокчейн-аналітики в роботі правоохоронних органів. Уніфікація підходів до розуміння технічної та юридичної природи криптовалют є запорукою мінімізації процесуальної невизначеності та забезпечення невідворотності покарання.

Ключові слова: блокчейн, смарт-контракт, кримінальне провадження, речовий доказ, арешт майна, приватний ключ.

The article is aimed at a comprehensive study of the legal nature of virtual assets in the context of the criminal justice system of Ukraine. The primary focus is on distinguishing the concepts of "virtual asset," "crypto-asset," and "cryptocurrency," as well as developing practical recommendations for overcoming procedural obstacles when seizing digital assets and recognizing them as physical evidence. A critical analysis of the compliance of national legislation with international standards was conducted, highlighting gaps in the domestic legal framework that prevent the full utilization of digital assets as objects of evidence.

In the course of the study, a set of general scientific and special methods of cognition were employed. The formal-logical method was applied to clarify the conceptual and categorical apparatus. The comparative-legal method allowed for the comparison of Ukrainian legislation with international standards (MiCA Regulation, FATF Recommendations). The

Яцик Т. П., Черненко Т. В. Правова природа та особливості процесуального забезпечення розслідування кримінальних правопорушень, пов'язаних з криптовалютою

system-structural analysis method was used to study the technical components of blockchain and smart contracts, while the analysis of judicial practice served to identify typical errors made by investigation authorities in proving control over assets.

It has been established that the key problem of law enforcement is the "immateriality" of cryptocurrency, which serves as a basis for refusals to impose seizure. It is proven that for an effective investigation, the focus of evidence must shift from ownership rights to the fact of exclusive possession of access keys. The main methods for identifying asset owners are identified: from the analysis of electronic declarations to the use of specialized software for de-anonymizing transactions. The role of smart contracts as tools for automating criminal activity and as sources of evidentiary information is revealed.

The conclusion is drawn regarding the necessity of adapting the Criminal Procedure Code of Ukraine to digital realities by recognizing a specific form of materiality for virtual assets. It is substantiated that overcoming the trans-border nature of crypto-crimes is possible only through the implementation of international transparency standards and the expansion of blockchain analytics tools in the work of law enforcement agencies. Unifying approaches to understanding the technical and legal nature of cryptocurrencies is a prerequisite for minimizing procedural uncertainty and ensuring the inevitability of punishment.

Keywords: blockchain, smart contract, criminal proceedings, physical evidence, seizure of property, private key.

Постановка проблеми. Стрімкий розвиток фінансових технологій і глобальна цифровізація економічних відносин призвели до появи та масового використання віртуальних активів, серед яких ключове місце посідає криптовалюта. Станом на 2025 рік Україна демонструє досить високий рівень інтеграції цифрових активів у повсякденне життя, посідаючи восьме місце в Глобальному індексі криптоадаптації та четверте місце за кількістю роздрібних операцій. Така популярність, з одного боку, відкриває нові економічні можливості, а з іншого – створює безпрецедентні виклики для правоохоронної та судової систем.

Криптовалюти завдяки своїм особливостям, як-от анонімність (псевдонімність), транскордонність, висока швидкість транзакцій і відсутність централізованого контролю, стали ефективним інструментом для реалізації різних видів кримінальних правопорушень. Вони широко застосовуються для легалізації (відмивання) доходів, отриманих незаконним шляхом, фінансування тероризму, торгівлі забороненими товарами в даркнеті, а також слугують предметом неправомірної вигоди в корупційних схемах.

Отже, потреба у виробленні єдиного науково обґрунтованого підходу до визначення правового статусу криптовалюти в кримінальному провадженні є критичною для забезпечення правопорядку та економічної безпеки держави.

Аналіз останніх досліджень і публікацій. Питання правового регулювання віртуальних активів наразі перебуває на етапі активного наукового аналізу. Теоретичні основи обігу криптовалют та їхній захист у межах кримінального права досліджують провідні українські вчені, серед яких можна виділити Т. П. Овсійчука, О. В. Кременського, К. В. Шустрову, Є. В. Лашука, А. А. Музику, Л. В. Омельчук, В. А. Шкелебей, Т. П. Яцик, І. І. Румик та інших.

Яцик Т. П., Черненко Т. В. Правова природа та особливості процесуального забезпечення розслідування кримінальних правопорушень, пов'язаних з криптовалютою

На міжнародному рівні ключовими є напрацювання експертів FATF і положення європейського Регламенту MiCA, які визначають глобальні стандарти прозорості та фінансового моніторингу віртуальних активів.

Водночас, попри значну кількість публікацій, низка питань усе ще залишається предметом дискусій. Зокрема, немає єдиної позиції щодо юридичної природи криптовалют: чи потрібно її вважати майном, інформацією або цифровим кодом.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на значний масив наукових напрацювань щодо правової природи криптовалют, поза увагою дослідників залишається низка критичних аспектів, що зумовлюють розрив між теорією та практикою кримінального судочинства. Зокрема, залишається нерозв'язаним питання розробки уніфікованого алгоритму процесуального закріплення «факту контролю» над приватними ключами, що в умовах децентралізації є важливішим за встановлення класичного права власності. Більшість наявних досліджень фокусуються на правовому статусі активу, ігноруючи методику документування транзакцій, проведених через сервіси анонімізації (міксері), та джерела доказової інформації, що містяться в коді смарт-контрактів. Причиною такого стану є надмірна консервативність кримінальної доктрини, яка не встигає за динамічним розвитком блокчейн-технологій, і відсутність міждисциплінарного підходу, що поєднував би юриспруденцію із цифровою криміналістикою. Дослідження цих аспектів є фундаментальним для розуміння загальної проблеми, оскільки без подолання «бар'єра матеріальності» та визначення чітких критеріїв ідентифікації користувача будь-які заходи кримінально-правового впливу втрачають реальну перспективу виконання. Авторський внесок у цій статті спрямований на заповнення вказаних прогалин через обґрунтування концепції «цифрової матеріальності» та формування прикладних рекомендацій щодо фіксації електронних слідів у розподілених реєстрах, що дасть змогу мінімізувати процесуальну невизначеність під час арешту та конфіскації віртуальних активів.

Формулювання цілей статті (постановка завдання). Основним завданням дослідження є обґрунтування методики залучення віртуальних активів до доказової бази кримінального провадження за рахунок подолання колізії між їхньою цифровою природою та процесуальними вимогами щодо речових доказів. Для реалізації цієї цілі передбачається вирішення таких конкретних завдань: усунення термінологічної неоднозначності понять «віртуальний актив» і «криптовалюта» в слідчій практиці; розробка алгоритму доведення факту контролю над активами через володіння криптографічними ключами; обґрунтування концепції «цифрової матеріальності» для забезпечення правомірності арешту активів згідно зі ст. 170 КПК України. Дослідження також спрямоване на розробку прикладних рекомендацій щодо ідентифікації транзакцій у блокчейні та нейтралізації інструментів анонімізації. Виконання цих завдань дасть змогу трансформувати теоретичні знання про блокчейн у дієвий криміналістичний інструментарій, що забезпечить невідворотність покарання за правопорушення у сфері цифрової економіки.

Виклад основного матеріалу. У системі кримінального судочинства критично важливим є чітке термінологічне розмежування об'єктів цифрового світу, оскільки помилкова кваліфікація активу може призвести до процесуальних помилок під час визначення обсягу завданих збитків або природи вчиненого правопорушення.

Яцик Т. П., Черненко Т. В. Правова природа та особливості процесуального забезпечення розслідування кримінальних правопорушень, пов'язаних з криптовалютою

У сучасній вітчизняній літературі досить часто спостерігається ототожнення понять «віртуальні активи», «криптоактиви» та «криптовалюта». Проте ці терміни мають принципово різні значення, а розуміння їхніх відмінностей є надзвичайно важливим.

Базовою категорією, що існує родовим поняттям у вітчизняному та міжнародному законодавстві, є «віртуальний актив». В українському законодавстві віртуальний актив визначається як «нематеріальне благо, що є об'єктом цивільних прав, має вартість і виражене сукупністю даних в електронній формі» [1]. Це найширша дефініція, яка охоплює будь-яке цифрове вираження вартості, незалежно від технології його створення, за умови, що воно може бути об'єктом цивільних прав. До віртуальних активів належать не лише криптовалюти, але й токени, внутрішньоігрові валюти, скіни в певних іграх тощо.

Відповідно до Закону України «Про віртуальні активи», який станом на 14.04.2026 все ще не набрав чинності, віртуальний актив не є засобом платежу, а його правовий статус ототожнюється зі статусом рухомого майна в цивільному праві [1].

Термін «криптоактив» все ще немає законодавчого визначення, хоча й згадується в офіційних документах.

ЄС у своєму Регламенті MiCA надає таке визначення криптоактиву: «цифрове вираження вартості або права, яке можна передавати та зберігати в електронній формі за допомогою технології розподіленого реєстру або схожої технології» [2].

До криптоактивів Регламент MiCA відносить токени електронних грошей (electronic money tokens), токени, прив'язані до активу (asset-referenced tokens) та інші криптоактиви.

Зі свого боку поняття «криптовалюта» є ще вужчим і має суто фінансове спрямування. Це специфічний вид криптоактива, основною функцією якого є роль універсального засобу обміну, накопичення та розрахунку. До криптовалюти належать Bitcoin, Ethereum, Litecoin тощо.

Для належного визначення самої правової природи криптовалюти, на наше переконання, є встановлення її технічної складової, зокрема розуміння принципу функціонування блокчейну. За своєю сутністю блокчейн є децентралізованою цифровою базою або реєстром, що складається з постійно зростаючого списку упорядкованих записів, які називаються блоками; і який зберігає записи в мережі комп'ютерів прозорим, незмінним і стійким до втручання способом [3].

Інакше кажучи, блокчейн ніби цифровий журнал, який неможливо підробити і який зберігається одночасно на тисячах комп'ютерів. Кожна сторінка журналу – це окремий блок, а всі сторінки разом утворюють ланцюг (chain). Після того як сторінка заповнюється, її «запечатують» або ж хешують. Кожен блок має свій унікальний хеш – довгий рядок символів, який створюється на основі даних усередині самого блоку. Кожен наступний блок містить хеш попереднього, тому якщо хтось спробує втрутитись і змінити хоча б один символ у старому блоці, його хеш повністю зміниться. Саме цим способом забезпечується незмінність і стійкість до втручання, про яку згадувалося раніше.

Варто звернути увагу на те, що блокчейн є специфічним реєстром порівняно з тим самим реєстром транзакцій банку. Його функціональне наповнення давно вийшло за межі фіксації звичайних монетарних транзакцій. Якщо банківський реєстр фактично є як список змін у балансах рахунків із прив'язкою до ідентифікованих клієнтів, то блокчейн охоплює значно ширший спектр цифрових подій. Наприклад, у блокчейнах

Яцук Т. П., Черненко Т. В. Правова природа та особливості процесуального забезпечення розслідування кримінальних правопорушень, пов'язаних з криптовалютою

другого та третього поколінь, як-от Ethereum, до реєстру вносяться не лише транзакції з передачі активів, але й дані про створення та виконання смарт-контрактів.

Смарт-контрактом є автоматичний контракт із вбудованими умовами та правилами, який виконується без потреби в посереднику [3, с. 13]. Інакше кажучи, це програмний код, який діє за простою логікою «Якщо – то».

У контексті кримінального провадження смарт-контракти можуть бути як знаряддям вчинення кримінальних правопорушень (наприклад, у децентралізованих фінансових пірамідах), так і джерелом доказової інформації, а їхня автономність створює окремий виклик для правоохоронних органів: оскільки смарт-контракт є незмінним після розгортання в блокчейні, технічно неможливо «скасувати» чи «зупинити» його дію звичайним способом. Отже, цей механізм створює систему, де безпосередня фізична або цифрова участь особи в момент розподілу злочинних активів стає не обов'язковою.

До того ж саме функціональні можливості смарт-контрактів дають змогу реалізувати складну ієрархію цифрових об'єктів, що знову повертає нас до потреби в їхньому суворому розмежуванні. Варто підкреслити, що блокчейн є технологічною основою, а криптовалюта – лише одним із варіантів її застосування і є нативним активом блокчейн-протоколу, який слугує засобом обміну для всіх транзакцій усередині цієї мережі. Токени ж зі свого боку є активами, які створюються «поверх» наявного блокчейну.

Однак для правової кваліфікації кримінального правопорушення недостатньо розуміти лише природу самого активу; критично важливим є встановлення механізму контролю над ним. У світі віртуальних активів такий контроль реалізується через криптографічні ключі, які зберігаються в криптогаманцях.

Часто в цифровій економіці криптогаманець розглядається як такий собі сейф, де зберігаються певні віртуальні активи, проте насправді криптогаманець не є гаманцем за своєю суттю і не містить валюти як такої. Усі записи про активи існують виключно в блокчейні, тоді як гаманець є лише інструментом взаємодії з ним і містить криптографічні ключі [4].

Сутність роботи гаманця базується на асиметричному шифруванні, де ключову роль відіграють публічний і приватний ключі. Публічний ключ є основою для генерування адреси гаманця й він відкритий для всіх учасників мережі та використовується для ідентифікації отримувача коштів. Приватний ключ виконує роль такого собі цифрового підпису, без якого доступ до коштів у блокчейні стає технічно неможливим. Відновити доступ до активів навіть за умови втрати приватного ключа можна за допомогою seed-фрази – послідовності із 12 або 24 випадкових слів.

Саме така специфічна технічна архітектура, де володіння активом зводиться до володіння інформацією (ключами), а не фізичним об'єктом – зумовлює складність правової інтерпретації цього явища. Адже криптовалютні активи є багатоаспектним об'єктом і, з одного боку, являють собою сукупність даних в електронній формі, а з іншого – актив, що має реальну економічну цінність і може бути конвертований у фіатну валюту.

Варто зазначити, що рівень складності правової інтерпретації та подальшого накладення арешту значною мірою залежить від способу зберігання активів, зокрема від їхнього кастодіального статусу.

У разі кастодіального зберігання, як-от на централізованих біржах Binance або WhiteBIT, приватними ключами керує платформа-кастодіан. У такому разі об'єктом арешту є майнові права на обліковий запис, і юридичний обов'язок виконання ухвали суду лягає саме на юридичну особу, яка керує такою платформою.

Однак під час некастодіального зберігання підозрюваний є одноосібним власником ключів. У такій ситуації просте вилучення гаджета не гарантує збереження активів, оскільки підозрюваний може скористатися seed-фразою для відновлення доступу до гаманця з іншого пристрою та перевести кошти за лічені секунди. Доцільним у такій ситуації є негайне переміщення активів на підконтрольні державі адреси.

Проте реалізація такої тактичної дії впирається у фундаментальну законодавчу неврегульованість, адже в кримінальному судочинстві й досі відсутні конкретні норми, які б визнавали криптовалюту об'єктом або предметом кримінального правопорушення. Наразі в Кримінальному кодексі України відсутні положення, які б прямо встановлювали кримінальну відповідальність за незаконне заволодіння криптовалютою, а норми Кримінального процесуального кодексу (далі – КПК України) не повною мірою пристосовані до розслідування кримінальних правопорушень у сфері криптовалют. Унаслідок цього питання подальшої правової долі вилучених криптоактивів залишається не повністю врегульованим і вирішується ситуативно [5, с. 197].

Ситуативність та процесуальна невизначеність особливо яскраво проявляються у спробах визначити правовий статус криптовалюти в контексті доказового права. Основною перешкодою водночас є питання щодо визнання криптовалюти як майна. Як зазначає А. О. Воронкін, КПК України, а саме ст. 170 передбачено накладення арешту на криптовалютні активи з метою збереження речових доказів [6]. Проте криптовалюту важко визнати саме речовим доказом, оскільки вона не має тієї ключової ознаки, яка впливає із самого визначення речового доказу, наданого тим самим процесуальним законодавством – матеріальності [7].

Матеріальним об'єктом є фізично наявна річ або предмет, який існує об'єктивно; він існує незалежно від свідомості людини та здатен фіксуватись у просторі. Криптовалюта ж за своєю суттю позбавлена таких ознак і є нематеріальним благом, цифровим записом у розподіленому реєстрі (блокчейні), який не має фізичного втілення.

Саме ця невизначеність створює неоднозначність судової практики, коли в одному випадку слідчий суддя задовольняє клопотання про накладення арешту на криптовалютні активи й погоджується з позицією прокурора [8], а в іншому – навпаки, відмовляє [9].

Якщо проаналізувати схожі судові рішення Печерського суду, простежується чітка тенденція: якщо прокурор у клопотанні про арешт майна вказує метою лише «збереження речових доказів», ризик відмови через нематеріальність об'єкта наближається до абсолютного.

Відмови в арешті часто обумовлені не лише теоретичними суперечностями, але й тим, що слідство не завжди може довести володіння конкретною особою певним активом. На відміну від нерухомості, яка зареєстрована в державному реєстрі, право власності на віртуальні активи підтверджується загалом контролем над ключами доступу.

Якщо право власності на ту саму нерухомість підтверджується відповідним записом у реєстрі, то в світі віртуальних активів діє принцип «Not your keys, not your

coins» (не твої ключі – не твої монети). Оскільки право розпоряджатися активом має лише той, хто володіє приватним ключем (сид-фразою), слідству потрібно довести не те, що актив «належить» особі, а те, що особа має ексклюзивний доступ до нього.

Відповідно, щоб навіть накласти той самий арешт, слідчий або прокурор мають довести причетність підозрюваного до нього. Це складно через декілька аспектів.

По-перше, якщо криптовалютні активи були отримані незаконним способом, власники часто звертаються до використання міксерів або тумблерів – спеціалізованих сервісів на кшталт Tornado Cash, які розривають зв'язок між відправником і отримувачем, роблячи неможливим відстеження ланцюжка транзакцій [10].

Саме процесуальне доведення є теж однією із проблем. Суди часто відмовляють в арешті, оскільки слідство не надає доказів «контролю». Для суду «скріншот з екрана монітора» не завжди є достатнім доказом, тому слідству потрібно встановити IP-адреси, пристрої, на яких зберігаються ключі, або встановлені застосунки та зв'язок з фіатними грошима.

З урахуванням викладеного вище доцільно запропонувати такий алгоритм дій, спрямований на запобігання подальшим відмовам у задоволенні клопотань про накладення арешту:

1. Надання декларацій як факту підтвердження володіння віртуальними активами. Згідно із Законом України «Про запобігання корупції» суб'єкти декларування зобов'язані вказувати криптовалюти, які їм належать [11]. Запис у декларації є самостійним доказом володіння, хоча він часто потребує підтвердження через фіксацію публічної адреси гаманця.

2. Вилучення особистих гаджетів. Найбільш вагомими доказами є вилучені смартфони та ноутбуки, де виявляють встановлені додатки (Trust Wallet, Binance), скріншоти seed-фраз, листування в месенджерах про транзакції та історію входу в акаунти.

3. Блокчейн-аналітика. Слідчі судді ВАКС усе частіше приймають результати технічних експертиз, які пов'язують активність за публічними адресами блокчейну з фізичними діями підозрюваного.

4. Пошук фізичних носіїв і паролів. Якщо під час обшуку не вдалося виявити фізичних носіїв або паролів, накладення арешту на умовну чи «абстрактну адресу» часто розцінюється судом як надмірне втручання в право власності без реальної перспективи виконання ухвали. Це стає додатковим аргументом для відмови: суд не хоче ухвалювати рішення, яке залишиться лише «на папері».

Потрібно також змінити й сам підхід під час формування клопотань про накладення арешту. Ситуативність судової практики часто зумовлена тим, що слідство намагається накласти арешт на криптовалюту як на «річ», що суперечить її технічній природі.

Натомість юридично коректним і технічно обґрунтованим є підхід, за якого об'єктом процесуального примусу існують майнові права на віртуальний актив. Така зміна юридичної техніки дає змогу змістити акцент у судовому засіданні з дискусії про фізичне існування об'єкта на обговорення його економічної вартості та можливості відчуження.

Водночас подолання проблеми «нематеріальності» криптоактивів можливе через переосмислення їхньої правової природи. Зокрема, деякі науковці, серед яких О. В. Кришевич, акцентують увагу на специфічних ознаках криптовалюти, які забезпечують

ту саму матеріальність і дають віднести криптовалютні активи до предмета кримінального правопорушення. До фізичних ознак відносять можливість вимірювати їх у певних одиницях, здатність торгувати на електронній біржі або можливість вилучення. О. В. Кришевич наводить й інші ознаки криптовалюти як предмета кримінального правопорушення проти власності: соціально-економічні (певна мінова й споживча вартість) та юридичні (гаманець комусь належить, а якщо ні, то це не є власністю цієї конкретної особи) [12, с. 172].

У деяких випадках криптовалюта може бути не лише об'єктом посягання, а й знаряддям вчинення кримінального правопорушення. Наприклад, коли вона використовується як інструмент для вчинення іншого злочину. Вона не є ціллю, а лише полегшує злочинний намір. У такому контексті криптовалюта полегшує реалізацію злочинного наміру, забезпечуючи зловмиснику анонімність і можливість дистанційного впливу.

Важливим питанням, яке потребує з'ясування під час розгляду кримінальних правопорушень, пов'язаних із криптовалютою, є саме місце вчинення кримінального правопорушення. Традиційний територіальний принцип, закріплений у ст. 6 КК України, виходить із того, що кримінальне правопорушення вважається вчиненим на території України, якщо його було почато, продовжено, закінчено або припинено на її території [13]. Проте децентралізована природа блокчейну фактично нівелює поняття державних кордонів.

У випадку із криптовалютами правопорушення часто має розподілений і транскордонний характер. Розподілений характер блокчейну означає, що кримінальне правопорушення може бути ініційоване в одній країні, сервери біржі розташовані в іншій, а виведення коштів відбувається в третій. До того ж, незважаючи на те, що всі транзакції в блокчейні є відкритими для перегляду, вони пов'язані з адресами (публічними ключами), а не з конкретними іменами осіб.

У такому разі доцільно використовувати спеціалізоване програмне забезпечення (наприклад, Chainalysis, Elliptic або TRM Labs), які об'єднують тисячі адрес в одну групу, що належить одному серверу або особі. Сучасні алгоритми та програми дають змогу впоратись і з міксерами, про які згадувалось раніше.

Оскільки схожі правопорушення часто мають транскордонний характер, найчастіше слідчі подають запити про надання міжнародної правової допомоги. Однак, як свідчить практика, такі запити рідко дають якісь результати. Не багато країн готові надавати таку інформацію, до того ж дотримання всіх процедур, передбачених законом, вимагає часу, якого в роботі з криптовалютою немає – зловмиснику потрібно лише кілька хвилин, щоб прогнати активи через десятки «міксерів».

Світова спільнота вже давно розробляє уніфіковані правила для боротьби з використанням криптовалют у злочинних цілях. І хоча в більшості країн питання правового регулювання криптовалют залишається все ще невирішеним, міжнародні організацій повільно рухаються в напрямі створення єдиного стандарту прозорості та транскордонного нагляду, який би поєднував децентралізовану природу блокчейну з вимогами класичного фінансового моніторингу.

Ключову роль тут відіграє FATF (Financial Action Task Force). 2025 року FATF оновила свої рекомендації, зосередивши увагу на ефективності повернення активів. Згідно з Рекомендацією 15 країни повинні ідентифікувати й оцінювати ризики, пов'язані з віртуальними активами, а також ліцензувати VASPs (постачальників послуг) [14].

Відповідно до останніх звітів FATF понад 80 % юрисдикцій усе ще демонструють низький або помірний рівень ефективності в процесах повернення віртуальних активів. Водночас блокчейн за належної підготовки правоохоронців та використання сучасних аналітичних інструментів може виявитися навіть простішим для відстеження, ніж традиційні активи. Рекомендується активніше впроваджувати державно-приватні партнерства, що даватиме змогу оперативно реагувати на криптозлочини в режимі реального часу [15].

Висновки. Підсумовуючи результати дослідження, варто зазначити, що ефективність протидії злочинності у сфері віртуальних активів безпосередньо залежить від здатності кримінального процесуального законодавства адаптуватися до нематеріальної природи цифрових об'єктів. Ключовим висновком є потреба в переході від класичного доказування права власності до встановлення факту ексклюзивного контролю особи над приватними ключами, що дасть змогу мінімізувати процесуальну невизначеність під час накладення арешту на активи. Доведено, що подолання «бар'єра матеріальності» можливе через імплементацію концепції «цифрової матеріальності», де криптовалюта визнається специфічним видом майна, що має реальну економічну цінність і технічну вимірюваність у розподіленому реєстрі. Встановлено, що інтеграція інструментів блокчейн-аналітики та дотримання міжнародних стандартів FATF є обов'язковою умовою для нейтралізації методів анонімізації транзакцій і забезпечення невідворотності покарання. Отже, лише уніфікація технічних алгоритмів і правових норм дасть змогу трансформувати віртуальні активи з об'єктів процесуальних труднощів у повноцінну джерельну базу доказової інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX : станом на 15 листоп. 2024 р. URL : <https://zakon.rada.gov.ua/laws/show/2074-20#Text>
2. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. URL : <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>
3. Румик І., Ковальчук Ю. Управління фінансами та процесами з використанням криптовалютних технологій. *Вчені записки Університету «КРОК»*. 2024. № 2 (74). С. 11–21. DOI : <https://doi.org/10.31732/2663-2209-2024-74-11-21>
4. Ковтонюк І. В., Марчук Д. К. Криптогаманці та їх типи. *Комп'ютерні технології: інновації, проблеми, рішення* : тези V Всеукраїнської науково-технічної конференції, м. Житомир, 01–02 грудня 2022 р. Житомир : Житомирська політехніка, 2022. С. 20.
5. Кузьменко О. В., Кравчук П. Ю. Віртуальні активи як предмет кримінального правопорушення: проблеми визначення та доказування. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. № 6 (3). С. 194–198.

Яцик Т. П., Черненко Т. В. *Правова природа та особливості процесуального забезпечення розслідування кримінальних правопорушень, пов'язаних з криптовалютою*

6. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 1 квіт. 2026 р. URL : <https://zakon.rada.gov.ua/laws/show/4651-17#Text>

7. Воронкін А. О. Арешт як різновид обмеження права власності на криптовалютні активи у кримінальному провадженні. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. № 5 (3). С. 137–145.

8. Ухвала від 05.03.2025 № 757/10299/25-к / Печерський районний суд м. Києва. URL : https://verdictum.ligazakon.net/document/125727992?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01

9. Ухвала від 04.03.2025 № 757/5200/25-к / Печерський районний суд м. Києва. URL : https://verdictum.ligazakon.net/document/125727992?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01

10. Криптоміксери та обфускатори / Trustee. URL : <https://trusteeglobal.com/academy/crypto-mixers/>

11. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII : станом на 7 лют. 2026 р. URL : <https://zakon.rada.gov.ua/laws/show/1700-18#Text>

12. Кришевич О. В., Рощина І. О. Криптовалюта, як предмет кримінального правопорушення проти власності: національне та міжнародне законодавство. *Вісник мариупольського державного університету. Серія: право*. 2022. № 23–24. С. 168–175.

13. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р. URL : <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

14. Рекомендації FATF міжнародні стандарти боротьби з відмиванням коштів, фінансуванням тероризму і розповсюдженням зброї масового знищення. URL : <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf>

15. Asset Recovery Guidance and Best Practices / FATF. Paris, 2025. URL : <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/asset-recovery-guidance-best-practices-2025.html>

16. Яцик Т. П., Шкелебей В. А. Розслідування кримінальних правопорушень, пов'язаних з обігом віртуальних активів. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2023. № 80 (2). С. 219–223.

Дата надходження 26.03.2026

Дата прийняття 23.04.2026

Дата рекомендації 28.05.2026

Дата публікації 30.06.2026