

ВІДПОВІДАЛЬНІСТЬ ЗА ЗЛОЧИНИ, ПОВ'ЯЗАНІ З НЕЗАКОННИМ ОБІГОМ КРИПТОВАЛЮТ

У тезах досліджується проблема злочинів, пов'язаних з незаконним обігом криптовалют, в умовах глобальної цифровізації фінансового сектору. Розглядаються основні ризики, пов'язані з використанням криптовалют у злочинній діяльності, такі як відмивання коштів, фінансування тероризму, ухилення від оподаткування та інші. Аналізуються недоліки існуючих механізмів притягнення до відповідальності за такі злочини та пропонуються шляхи їх удосконалення, включаючи створення чіткої правової бази, посилення цифрової компетентності правоохоронних органів та впровадження спеціалізованих інструментів моніторингу.

Ключові слова: криптовалюта, цифровізація, незаконний обіг, відмивання коштів, фінансування тероризму, правове регулювання, кіберзлочинність, блокчейн, фінансовий моніторинг.

У сучасних умовах глобальної цифровізації фінансового сектору криптовалюти набувають дедалі більшого поширення як альтернативний платіжний засіб, інструмент інвестування та збереження активів. Як зауважує А. Слатюка «криптовалюта — різновид віртуальної валюти, створена за допомогою криптографічних методів та математичних обчислень переважно на базі блокчейну. Це і цифрова, і віртуальна валюта, тому що вона існує в інтернеті та створена за допомогою криптографічних алгоритмів» [1].

Криптовалюти, як новий економічний інструмент викликають підвищений інтерес завдяки своїм унікальним функціям — обміну, накопичення, інвестування та оплати — і характеризуються високим рівнем безпеки, швидкістю транзакцій та анонімністю. Попри це, вони мають низку ризиків, зокрема правову невизначеність, волатильність і використання у злочинній діяльності, що ускладнює їх правове регулювання та інтеграцію в офіційну фінансову систему. У контексті цифровізації криптовалют поступово набувають ваги як альтернатива фіатним валютам, однак залишаються поза ефективним контролем державних органів [2]. Водночас, поряд із легальним використанням віртуальних активів, зростає й кількість правопорушень, пов'язаних з їх незаконним обігом, що створює реальні загрози для економічної безпеки держави, фінансової стабільності та правопорядку. Відсутність чіткого правового статусу криптовалют, а також обмеженість інструментів їхнього регулювання ускладнюють кваліфікацію правопорушень та притягнення винних осіб до відповідальності.

Сучасний ландшафт криптозлочинності характеризується появою нових видів правопорушень, пов'язаних з розвитком децентралізованих фінансів (DeFi) та невзаємозамінних токенів (NFT). До них належать такі явища, як «rug pull» (раптове зникнення ліквідності), NFT-шахрайство (підробка, плагіат) та DeFi-експлуїти (використання вразливостей протоколів). Крім того, необхідно поглибити аналіз зв'язку між криптовалютами та традиційною кіберзлочинністю, зокрема, їх використання у вимогах програм-вимагачів (ransomware), фішингових атаках та інших формах кібершантажу. Важливим аспектом є також оцінка впливу різноманітних підходів до регулювання криптовалют у різних юрисдикціях на їхню привабливість для злочинців, з урахуванням таких факторів, як вимоги KYC/AML, податкове регулювання та загальний правовий статус.

Основні ризики, пов'язані з нелегальним обігом криптовалют, полягають у тому, що віртуальні активи дедалі частіше використовуються як інструмент відмивання коштів, здобутих злочинним шляхом, завдяки своїй високій анонімності, децентралізованій природі та транскордонному характеру транзакцій. Криптовалюти також є ефективним каналом фінансування терористичних організацій через труднощі у відстеженні джерел та напрямів грошових потоків. Крім того, вони створюють широкі можливості для ухилення від оподаткування, оскільки значна частина операцій залишається поза контролем державних податкових та фінансових органів. У сукупності ці загрози становлять серйозний виклик для економічної безпеки держави та вимагають розробки спеціалізованих механізмів правового реагування.

Зважаючи на транснаціональний характер криптовалют, ефективне протидіяння злочинам у цій сфері неможливе без міжнародної координації та правової співпраці. Станом на сьогодні в світі діє низка інституційних, нормативних та оперативних механізмів, спрямованих на виявлення, розслідування та притягнення до відповідальності осіб, причетних до злочинів з використанням криптовалют. Зокрема, міжнародний механізм протидії кримінальним правопорушенням пов'язаним із незаконним обігом

криптовалют включає такі нормативно-інституційні складові, як: Financial Action Task Force, регламент Markets in Crypto-Assets Regulation, Конвенція Ради Європи про кіберзлочинність, Egmont Group, Інтерпол, Європол, Міжнародна правова допомога у кримінальних справах, Egmont Group, UNODC, Міжнародна правова допомога у кримінальних справах (MLA) та європейські ордери на арешт або видачу, Спільні слідчі групи (JITs) та ін.

В Україні, як і в більшості інших країн, законодавство щодо криптовалют лише формується, зокрема, було 2021 р. було прийнято Закон України «Про віртуальні активи», який «регулює правовідносини, що виникають у зв'язку з оборотом віртуальних активів в Україні, визначає права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів» (не набрав чинності) [3]. Окремі положення ККУ України можуть бути застосовані до кримінальних правопорушень, пов'язаних із незаконним використанням криптовалют. До таких злочинів належать: легалізація (відмивання) майна, одержаного злочинним шляхом (ст. 209 ККУ) – використання криптовалют для легалізації незаконно отриманих коштів; шахрайство (ст. 190 ККУ) – маніпуляції з криптовалютами активами для введення в оману інвесторів або споживачів; несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 ККУ) – хакерські атаки, викрадення криптовалют з гаманців або бірж; фінансування тероризму (ст. 258-5 ККУ) – використання криптовалют для підтримки терористичних організацій; маніпулювання на організованих ринках (ст. 222-1 ККУ) – шахрайські схеми із залученням криптовалютних активів; незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (ст. 200 ККУ) – використання криптовалют для ухилення від фінансового моніторингу [4].

Серед основних недоліків механізму притягнення до відповідальності за кримінальні правопорушення в сфері обігу криптовалют:

- невизначеність законодавства, колізії юрисдикцій, відсутність чіткої термінології;
- невизначеність правового статусу криптовалют у багатьох юрисдикціях, що зумовлює складності у визначенні предмету кримінального правопорушення;
- технології блокчейн і криптовалютні платформи дозволяють здійснювати транзакції без розкриття особистих даних, ускладнюючи ідентифікацію злочину;
- складність відстеження транзакцій, анонімність, використання технологій захисту приватності;
- неможливість блокування чи арешту активів у реальному часі без спеціальних інструментів моніторингу та доступу до ключів;
- транзакції часто проходять через юрисдикції з різними або відсутніми регулюваннями, що створює правові «лакуни»;
- юрисдикційні колізії ускладнюють збирання доказів, екстрадицію та правову допомогу між країнами;
- складність збору та подання цифрових доказів, нестача експертизи у правоохоронних органів;
- відсутність у слідчих, прокурорів та суддів необхідних технічних знань про криптовалюту, блокчейн, обмінники, гаманці;
- нестача цифрових криміналістичних інструментів для аналізу криптооперацій та відстеження сліду активів;
- операції з криптовалютами залишають нефізичні цифрові сліди, що складно фіксувати, зберігати та подавати як доказ у суді;
- у багатьох випадках відсутній зв'язок між особою, що контролює гаманець, і конкретним злочинним діянням;
- застосування міксерів, анонімних криптовалют (наприклад, Monero, Zcash), децентралізованих бірж (DEX), які не вимагають KYC (verifying identity), що унеможливило відстеження транзакцій та встановлення сторін операції.

Зауваженні вище недоліки проявляються у конкретних проблемах, з якими стикаються правоохоронці при розслідуванні криптозлочинів, таких як ідентифікація злочинців, відстеження руху коштів через міксери або анонімні криптовалюту, конфіскація криптоактивів. Окремою проблемою є складність міжнародної співпраці у розслідуванні транскордонних злочинів, включаючи питання екстрадиції, обміну інформацією та надання правової допомоги.

Для підвищення ефективності боротьби з криптозлочинністю необхідно розробити конкретні рекомендації щодо удосконалення правової бази, підвищення кваліфікації кадрів та впровадження технологічних інструментів, які включають:

- розробку змін до чинного законодавства з метою чіткого визначення правового статусу криптовалют, встановлення відповідальності за криптозлочини та надання правоохоронним органам необхідних повноважень;

- запровадження детальних програм підвищення кваліфікації для правоохоронців, прокурорів, суддів та інших учасників системи кримінальної юстиції, включаючи навчання основам криптографії, блокчейну, аналізу криптовалютних транзакцій та цифрової криміналістики;
- впровадження спеціалізованих інструментів та технологій для моніторингу та аналізу криптовалютних транзакцій, таких як програмне забезпечення для аналізу блокчейну, інструменти для деанонізації транзакцій та платформи для обміну інформацією між правоохоронними органами.

Отже, криптовалюти поступово інтегруються в глобальну фінансову систему як інструмент інвестування та розрахунків, однак супроводжуються зростанням злочинів, зумовлених їх анонімністю, децентралізацією та відсутністю належного регулювання, основні загрози включають відмивання коштів, фінансування тероризму, ухилення від оподаткування та кіберзлочинність. Правове реагування на такі злочини в Україні є фрагментарним, оскільки чинне законодавство не повною мірою враховує специфіку криптовалют. Водночас міжнародні механізми протидії — такі як FATF, Інтерпол, Європол — демонструють важливість глобального підходу та співпраці. Тому, необхідним є створення чіткої правової бази, посилення цифрової компетентності слідчих органів і впровадження технологічних інструментів моніторингу криптовалют для забезпечення ефективного притягнення до відповідальності за злочини у цій сфері.

References

1. Slatiuk A. Kryptovaliuta: vydy ta yikh osoblyvosti. FinAP. URL: <https://finap.com.ua/kryptovalyuta-vidi-ta-yih-osoblyvosti/> (data zvernennia: 14.03.2025)
2. Stoika M. Kryptovaliuta – vyznachennia, funktsii, perevahy ta ryzyky. Pidpriemnytstvo i torhivlia, 2021. № 30 S. 5-10. URL: <https://doi.org/10.36477/2522-1256-2021-30-01> (data zvernennia: 14.03.2025)
3. Pro virtualni aktyvy: Zakon Ukrainy vid 17.02.2022 r. № 2074-IX URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (data zvernennia: 14.03.2025)
4. Kryminalnyk kodeks Ukrainy vid 05.04.2001 r. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (data zvernennia: 14.03.2025)

DOI 10.34132/mspc2025.01.11.08

Anton Dolhov

LIABILITY FOR CRIMES RELATED TO THE ILLICIT TRAFFICKING OF CRYPTOCURRENCIES

The theses explore the problem of crimes related to the illicit trafficking of cryptocurrencies in the context of the global digitalization of the financial sector. The main risks associated with the use of cryptocurrencies in criminal activities, such as money laundering, terrorist financing, tax evasion, and others, are considered. The shortcomings of the existing mechanisms for bringing to justice for such crimes are analyzed, and ways to improve them are proposed, including the creation of a clear legal framework, strengthening the digital competence of law enforcement agencies, and the introduction of specialized monitoring tools.

Key words: *cryptocurrency, digitalization, illicit trafficking, money laundering, terrorist financing, legal regulation, cybercrime, blockchain, financial monitoring*

Відомості про автора / Information about the Author

Антон Долгов, доктор філософії з права, старший викладач кафедри цивільного та кримінального права та процесу, Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: advokat_dolgov_anton@ukr.net, orcid: <https://orcid.org/0000-0002-0305-363X>.

Dolhov Anton Gennadiyovich, Doctor of Philosophy in Law, Associate Professor at the Department of Civil and Criminal Law and Procedure of the Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: advokat_dolgov_anton@ukr.net, orcid: <https://orcid.org/0000-0002-0305-363X>.

