«Travel Rule» у дії: прозорість криптотранзакцій як інструмент протидії відмиванню коштів

Думчиков М.О.[1]

Опубліковано	Секція	УДК
30.10.2025	Право	343.2.

DOI: https://doi.org/10.5281/zenodo.17936741

Анотація. Стаття присвячена комплексному аналізу сучасних тенденцій розвитку кіберзлочинності у сфері віртуальних активів, а також дослідженню механізмів відмивання коштів із використанням криптовалют та інших цифрових фінансових інструментів.

Актуальність теми зумовлена тим, що упродовж останнього десятиліття віртуальні активи, насамперед криптовалюти, перетворилися на важливий елемент глобальної фінансової системи, який створює нові можливості для інноваційного розвитку економіки і водночас, значні ризики у сфері фінансової безпеки.

Враховуючи глобальний характер цифрових транзакцій, відсутність єдиних стандартів контролю та псевдоанонімність криптовалютних операцій, що ускладнює ідентифікацію суб'єктів правопорушень, проблема протидії кібервідмиванню набуває міждисциплінарного характеру, охоплюючи як кримінально-правову, так і фінансово-економічну складову.

У статті здійснено порівняльний аналіз рекомендацій та стандартів FATF, положень нормативного регулювання Європейського Союзу, зокрема, Регламент MiCA та П'ята директива ЄС з протидії відмиванню коштів, а також законодавство FinCEN, Bank Secrecy Act США. Виокремлено ключові проблеми імплементації міжнародних стандартів у національні правові системи, зокрема у частині забезпечення прозорості транзакцій, ідентифікації кінцевих бенефіціарів та контролю діяльності посередників віртуальних активів.

Зроблено висновок, що комплексне посилення нормативно-правового регулювання у поєднанні з міжнародною взаємодією, цифровізацією процесів фінансового моніторингу та впровадженням інноваційних технологічних рішень є ключовими передумовами підвищення ефективності протидії відмиванню коштів у кіберпросторі. На нашу думку, саме поєднання правових, технічних та інституційних інструментів створює підґрунтя для формування глобальної системи кіберфінансової безпеки нового покоління.

Ключові слова: віртуальні активи, криптовалюта, відмивання коштів, кіберзлочинність, фінансова безпека, цифрова економіка.

«The Travel Rule» in Action: Transparency of Crypto Transactions as a Tool to Counter Money Laundering

Abstract. The article provides a comprehensive analysis of current trends in the development of cybercrime in the sphere of virtual assets and examines the mechanisms of

[1] Д.ю.н., доцент, доцент кафедри кримінально правових дисциплін та судочинства Навчально-наукового інституту права СумДУ , https://orcid.org/0000-0002-4244-2419

money laundering through cryptocurrencies and other digital financial instruments. The relevance of the topic is driven by the fact that over the past decade, virtual assets—primarily cryptocurrencies—have become a significant component of the global financial system, creating new opportunities for economic innovation while simultaneously posing substantial risks to financial security. Given the global nature of digital transactions, the absence of unified control standards, and the pseudo-anonymity of cryptocurrency operations that complicate the identification of offenders, the issue of combating cyber–money laundering acquires an interdisciplinary character, encompassing both criminal law and financial–economic dimensions. The article conducts a comparative analysis of the FATF recommendations and standards, the regulatory framework of the European Union—including the MiCA Regulation and the Fifth Anti-Money Laundering Directive—as well as U.S. legislation such as the FinCEN regulations and the Bank Secrecy Act. It identifies the main challenges in implementing international standards into national legal systems, particularly regarding transaction transparency, beneficial ownership identification, and the supervision of virtual asset intermediaries. The study concludes that the comprehensive strengthening of legal regulation, combined with enhanced international cooperation, the digitalization of financial monitoring processes, and the adoption of innovative technological solutions, are key prerequisites for improving the effectiveness of anti–money laundering efforts in cyberspace. In our view, the integration of legal, technological, and institutional tools forms the foundation for building a new-generation global system of cyber-financial security.

Keywords: virtual assets, cryptocurrency, money laundering, cybercrime, financial security, digital economy.

Вступ

Постановка проблеми. Постійний розвиток фінансових технологій та зростання популярності віртуальних активів створюють нові можливості не лише для інвесторів і бізнесу, але й для злочинців. Сьогодні, кіберзлочинність дедалі частіше охоплює сегмент віртуальних активів, що проявляється у численних випадках шахрайства, зломів криптобірж, вимагань з використанням програм-вимагачів, а також відмивання незаконно отриманих коштів через криптовалютні транзакції [1].

Масштаб проблеми ілюструють дані аналітичних досліджень, так зокрема, з 2019 року зі «злочинних» криптогаманців було переведено у конверсійні служби майже 100 млрд. доларів США, причому пік обсягів в $30 млрд. припав на 2022 рік [2].

У 2023 році сума виплат криптовалютних викупів від атак програм-вимагачів сягнула рекордних 1 млрд доларів, що майже вдвічі більше, ніж попереднього року [2]. Ми переконані, що ці факти підтверджують, що віртуальні валюти активно використовуються злочинцями різних категорій – від хакерських угруповань до наркоторговців та терористичних фінансистів – для легалізації доходів і приховування слідів злочинної діяльності.

Стан наукової розробки теми свідчить про підвищену увагу міжнародних організацій та науковців до ризиків відмивання коштів через криптоактиви. Зокрема, FATF ще у 2019 році поширила стандарти боротьби з відмиванням коштів (AML) на віртуальні активи і постійно моніторить їх впровадження [3].

У доктринальних дослідженнях наголошується на ускладненні відстеження нелегальних операцій у криптовалютах через використання технологій приховування транзакцій, а також на тому, що децентралізовані фінансові моделі та нерегульовані юрисдикції створюють значні прогалини для правозастосування [4].

Водночас законодавці багатьох країн тільки нещодавно почали запроваджувати комплексні правила для цього сектора, і їх ефективність потребує перевірки часом. Існує потреба в систематизації сучасних знань про тенденції кіберзлочинності, пов’язаної з віртуальними активами, та оцінці адекватності заходів протидії.

Метою статті є здійснення глибокого аналізу міжнародних та зарубіжних тенденцій кіберзлочинності у сфері віртуальних активів, зокрема практик відмивання коштів, а також нормативного реагування і механізмів протидії.

Методи дослідження включають аналіз міжнародних нормативно-правових актів і рекомендацій, огляд статистичних даних про кіберзлочини з криптовалютами, а також узагальнення досвіду правоохоронної діяльності у різних країнах.

Результати

Сьогодні ми беззаперечно можемо акцентувати, що віртуальні активи стали невід'ємною частиною екосистеми транснаціональної злочинності. Ми переконані, що їх привабливість для злочинців пояснюється такими властивостями, як децентралізований характер, відносна анонімність транзакцій, швидкість переказів та глобальна доступність без посередників [2].

Первинно злочинна активність у криптосекторі асоціювалася з кіберзлочинами «у чистому вигляді», зокрема хакерськими крадіжками з криптобірж, атаками програм-вимагачів, шахрайськими ICO тощо. З часом криптовалюти почали використовувати й для відмивання грошей, здобутих від традиційних злочинів, таких як торгівля наркотиками або фінансові махінації [2]. Варто зауважити, що відповідно даним компанії Chainalysis, у 2024 році спостерігалася тенденція розширення спектру злочинів, доходи від яких відмиваються через криптоактиви, що вимагає від правоохоронців відповідного розширення експертизи. Фахівці з аналізу блокчейну потрібні тепер не тільки кіберпідрозділам, а й підрозділам по боротьбі з наркоторгівлею, фінансовим злочинам тощо [2]. На наше переконання, позитивним моментом є те, що прозорість публічних блокчейнів за наявності сучасних інструментів аналітики може слугувати правоохоронцям для відстеження злочинних потоків і збирання доказів, чого складніше досягти у традиційній банківській системі.

Серед найпоширеніших злочинів, пов'язаних із віртуальними активами, виділяються: крадіжки та зломи на криптовалютних платформах, шахрайства і скам-проєкти, вимагання та незаконна торгівля у даркнеті. Так, у 2023 році суттєво потерпали децентралізовані фінансові платформи, які за оцінками втратили близько $2 млрд внаслідок зломів смарт-контрактів і експлойтів, що вказує на вразливість DeFi-сектору [5].

Варто зауважити, що відмивання коштів через віртуальні активи часто є продовженням зазначених вище злочинів: отримані злочинні доходи (в криптовалюті чи конвертовані у неї) проходять подальшу «очистку» через численні транзакції.

Злочинці використовують для цього різноманітні інструменти. По-перше, онлайн-обмінники і криптобіржі, особливо зареєстровані у країнах з поблажливим регулюванням, слугують «конверсійними сервісами» для обміну «брудних» активів на фіат або інші активи [4]. По-друге, зловмисники вдаються до «мікшируючих» сервісів – спеціальних платформ, що змішують кошти багатьох користувачів з метою ускладнення прослідковування їхнього походження. Яскравим прикладом є сервіс Tornado Cash, через який було відмито понад $1 млрд, у тому числі сотні мільйонів для північнокорейської хакерської групи Lazarus [6].

По-третє, все більшою проблемою стає використання децентралізованих фінансів (DeFi) для відмивання грошей. У ризиковій оцінці DeFi, оприлюдненій Міністерством фінансів США у 2023 році, прямо зазначено, що кіберзлочинці, шахраї, хакери з КНДР та інші зловмисники активно "експлуатують вразливості" DeFi-протоколів для переміщення і легалізації нелегальних коштів [7].

На нашу думку, особливої уваги заслуговує роль віртуальних активів у фінансуванні кіберзлочинних угруповань та санкційних режимів. Так, сьогодні, КНДР перетворилася на одного з найбільших «спонсорів» незаконної криптовалютної

діяльності: державні хакери регулярно здійснюють зломи криптовалютних бірж і платформ з метою викрадення коштів для фінансування ракетної програми. У 2023 році відбувся найбільший в історії криптовалют пограбунок – хакери, пов'язані з КНДР, викрали з біржі ByBit близько $1,46 млрд, і лише менш як 4% цих активів вдалося відстежити та повернути [8].

Варто зазначити, що за даними FATF, зараз стейблкоїни дедалі частіше використовуються злочинцями, зокрема північнокорейськими хакерами, терористичними фінансистами та наркокартелями. Ми переконані, що масове впровадження стейблкоїнів без належного глобального контролю може суттєво підвищити ризики відмивання коштів, особливо якщо регулятивні режими різних країн залишатимуться нерівномірними.

Ми переконані, що ключовим джерелом міжнародних стандартів у сфері протидії відмиванню коштів є Рекомендації FATF. У відповідь на появу криптовалют цей орган у червні 2019 року оновив Рекомендацію 15, поширивши вимоги AML/CFT на діяльність з віртуальними активами та провайдерів таких послуг.

Було запроваджено поняття «virtual asset service providers», до яких віднесено: платформи обміну, передачі, зберігання криптоактивів тощо, які мають бути ліцензовані або зареєстровані та виконувати вимоги фінансового моніторингу [9].

Одним із центральних нововведень на нашу думку, стала вимога так званого «правила подорожі» (Travel Rule), аналогічна до банківських переказів: при переміщенні криптоактивів між платформами повинна передаватися інформація про відправника та одержувача, зокрема, ім'я, адреса, номер рахунку, тощо. FATF рекомендувала встановити поріг для застосування цієї вимоги (еквівалент 1000 євро), однак країни можуть запроваджувати і повне охоплення без порогів [10].

На практиці впровадження глобальних стандартів стикається з суттєвими затримками та нерівномірністю. FATF регулярно здійснює моніторинг виконання країнами цих вимог і публікує *Targeted Update* – цільові огляди прогресу. За даними шостого такого огляду який відбувся у червні, хоча ситуація покращилась порівняно з попередніми роками, багато юрисдикцій досі мають прогалини у ліцензуванні та нагляді за VASP, а також труднощі з ідентифікацією осіб, що здійснюють діяльність з віртуальними активами [2].

Водночас, позитивною зміною є те, що станом на червень 2025 року вже 99 країн запровадили або завершують законодавче впровадження «правила подорожі» для криптовалют [2]. На наше переконання, рівень фактичної відповідності залишається недостатнім, так, зоакрема у 2024 році FATF встановила, що 75% оцінених країн були лише частково або зовсім не сумісні з вимогами щодо віртуальних активів [11].

Не можемо не згадати про одних із лідерів у впровадженні комплексного регулювання ринку криптоактивів та протидії їхньому нелегальному використанню – ЄС в рамках регламентів. Так, зокрема, В червні 2023 року на рівні ЄС було остаточно прийнято два взаємопов'язаних акти: Регламент (ЄС) 2023/1113 та Регламент (ЄС) 2023/1114, які разом формують нову регуляторну рамку. Регламент 2023/1113 встановлює вимоги щодо супровідної інформації при переказах коштів і криптоактивів, фактично впроваджуючи правило «travel rule» у праві ЄС [12].

Відповідно до нього, оператори криптообміну та інші постачальники послуг з криптоактивами (CASP) зобов'язані збирати і передавати дані про платників та одержувачів при будь-яких переказах криптоактивів незалежно від суми транзакції [10]. Варто зауважити, що ЄС пішов навіть далі за рекомендації FATF, повністю скасувавши мінімальний поріг: нові правила вимагають здійснювати ідентифікацію для всіх переказів, у тому числі дрібних, якщо транзакція відбувається між провайдерами. Також правило поширюється на операції з «нехостингованими» (самостійними) гаманцями,

якщо такі гаманці взаємодіють з регульованими провайдерами і сума переказу перевищує 1000 євро [10].

Другий документ – Регламент 2023/1114, більш відомий як MiCA (Markets in Crypto-Assets Regulation), ухвалений водночас, встановлює всеосяжні правила обігу криптоактивів у ЄС. MiCA вперше запроваджує уніфіковані вимоги до випуску криптоактивів, діяльності криптобірж, провайдерів гаманців тощо, а також передбачає ліцензування CASP у межах ЄС [12]. Хоча MiCA націлений передусім на захист прав інвесторів і цілісність ринків, він має й важливий компонент запобігання фінансовим злочинам. Так, зокрема, регламент зобов'язує провайдерів дотримуватися вимог фінансового моніторингу нарівні з банками, в тому числі виконувати вимоги Регламенту 2023/1113 щодо передачі інформації про транзакції.

MiCA також покликаний усунути прогалини у нагляді: він підпорядковує великі платформи нагляду з боку Європейського органу з цінних паперів та ринків або національних регуляторів, встановлює вимоги до капіталу та управління ризиками для емітентів стейблкоїнів. Водночас, аналізований Регламент встановлює механізм «паспортизації» ліцензій, тобто, отримавши дозвіл в одній державі-члені, криптокомпанія зможе надавати послуги по всьому ЄС. На нашу думку такий підхід з одного боку, спрощує ведення бізнесу, а з іншого – підвищує вимоги до заявників, які мусять продемонструвати відповідність високим стандартам.

Крім того, Європейський Союз просуває створення окремого органу – Європейського органу з боротьби з відмиванням коштів (AMLA). Нагадаємо, що ця ініціатива є частиною пакету реформ ЄС у сфері AML, презентованого у 2021 році [10].

Новий орган матиме повноваження координації і прямого нагляду за найбільш ризиковими фінансовими установами в державах-членах, включно з великими постачальниками послуг віртуальних активів. Очікується, що AMLA розпочне роботу у 2026 році, і до його компетенції входитиме, зокрема, моніторинг виконання вимог щодо криптоактивів по всьому ЄС та гармонізація практики застосування санкцій за порушення.

Розглянувши основні міжнародні стандарти в сфері протидії легалізації віртуальних активів, пропонуємо визначити основні прогалини та виклики у протидії. На наше переконання, незважаючи на активізацію регуляторних зусиль, протидія відмиванню коштів через віртуальні активи залишається надзвичайно складним завданням. Серед основних проблем ми вбачаємо: 1) Анонімність та технології маскування. Анонімність блокчейн-транзакцій і використання змішувачів, coinjoin-сервісів та приватних монет (Monero, Zcash) ускладнюють розслідування фінансових злочинів, потребують просунутих аналітичних інструментів, які відсутні в багатьох країнах; хоча у випадку Tornado Cash блокчейн-аналіз виявив зв'язки з гаманцями Lazarus Group, сотні менших сервісів залишаються неконтрольованими [6]; 2) Децентралізація та відсутність посередника. На відміну від традиційних фінансових установ із визначеною відповідальністю, протоколи DeFi діють без чітких суб'єктів нагляду, що дозволяє злочинцям переміщувати кошти через смарт-контракти поза правовим контролем, оскільки чинні норми не охоплюють децентралізовані сервіси, які часто уникають вимог AML під приводом децентралізації [7]; 3) Юрисдикційний арбітраж. Віртуальні активи мають транснаціональний характер, тож злочинці переміщують операції в юрисдикції з м'яким регулюванням або слабким наглядом, через що клієнти з високим ризиком йдуть з бірж із жорстким KYC на офшорні платформи і злочинні потоки концентруються в уразливих країнах; FATF попереджає, що регуляторні провали в одній державі мають глобальні наслідки, тому головне завдання полягає у забезпеченні однорідного застосування стандартів; 4) Ідентифікація. Навіть у випадку, якщо виявлено підозрілий криптогаманець, встановити реальну особу без співпраці платформ складно, а слабкі процедури KYC у близько 56% глобальних VASP

станом на 2024 рік створюють прогалини у системі, через які банки іноді змушені блокувати перекази на біржі, щоб захистити клієнтів, що підриває прозорість [9]; 5) Обмежені ресурсу правоохоронних органів. Розслідування криптозлочинів потребує спеціалізованих навичок і інструментів, які мають переважно провідні країни, тоді як багато держав не володіють експертним потенціалом, що дозволяє злочинцям переміщувати кошти через менш ризикові юрисдикції і робить міжнародну координацію та оперативний обмін інформацією критично важливими.

Ми переконані, що для ефективної протидії відмиванню коштів через віртуальні активи необхідний комплексний підхід, що поєднує удосконалення правових норм, розвиток технологічних рішень та розширення міжнародної взаємодії.

Так, зокрема, впровадження правила передачі даних про відправника й отримувача транзакції є наріжним каменем для забезпечення прозорості криптоплатежів. Як вже було зазначено, ЄС вже закріпив цю вимогу законодавчо з датою застосування з кінця 2024 року [12]. Інші країни також ухвалюють аналогічні норми, станом на 2025 р. практично всі юрисдикції з найбільшими крипторинками перебувають у процесі імплементації Travel Rule [2]. Наступним кроком на нашу думку, має стати налагодження обміну даними між провайдерами з різних країн. Варто зауважити, що тут важливі саме технічні рішення, зокрема створення стандартизованих безпечних протоколів передачі інформації між VASP.

Однією з важливих складових протидії є використання передових технологічних рішень. Так, наприклад, служби фінансових розслідувань активно співпрацюють з компаніями, що спеціалізуються на блокчейн-аналізі, такими як Chainalysis, TRM Labs, Elliptic. В майбутньому штучний інтелект може ще більше посилити можливості моніторингу, виявляючи складні багатокрокові схеми відмивання. Проте злочинці теж застосовують нові технології, наприклад, Bridge-агрегатори для автоматизованого розподілення коштів між блокчейнами, або AI-інструменти для генерування фішингових схем, тому технологічна гонка триває.

Варто наголосити, що жодна країна не може самостійно ефективно протидіяти транскордонним криптозлочинам, тому правоохоронні органи розвивають міжнародну співпрацю. Під егідою Інтерполу діє Глобальна група з боротьби з фінансовими злочинами, що об’єднує зусилля проти відмивання коштів, пов’язаного з кіберзлочинами. Інтерпол, Європол і Базельський інститут управління щорічно проводять конференції з питань криптовалют і фінансових розслідувань, під час яких країни обмінюються досвідом та формують спільні методики. Серед результатів такої взаємодії варто виділити операцію «Haechi» у 2023 році, у межах якої заарештовано понад 3000 осіб і вилучено понад $100 млн, а також «Operation Destabilise» у Великій Британії, що дозволила завдяки міжнародній координації заморозити значні обсяги криптоактивів, пов’язаних з організованою злочинністю [13].

Водночас, міжнародна спільнота стимулює криптоіндустрію до саморегулювання, зокрема організації Global Digital Finance, CryptoUK та інші розробляють кодекси поведінки, а великі біржі впроваджують «travel rule» у межах проєкту TRISA, обмінюючись даними про транзакції понад $1000 [14].

Міжнародні ініціативи, зокрема програми UNODC із розбудови систем фінансових розслідувань і аналітичні огляди щодо конвергенції кіберзлочинності та відмивання коштів, сприяють включенню компоненту віртуальних активів до національних оцінок ризиків. Паралельно на платформах G7 і G20 провідні економіки світу узгоджують спільну політику проти використання криптовалют для обходу санкцій та формують глобальний консенсус у боротьбі з цифровим відмиванням коштів [15].

Висновки

Кіберзлочинність, пов'язана з віртуальними активами, становить одну з найдинамічніших загроз фінансовій безпеці у світі. Аналіз показав, що злочинці швидко освоїли сферу віртуальних активів як інструмент для відмивання доходів, користуючись їх транскордонністю та частковою анонімністю. Сучасні тенденції включають зростання масштабів криптовалютних крадіжок і вимагань, активне використання міксерів та DeFi-протоколів для приховування слідів, а також залучення до схем легалізації доходів нових категорій злочинців.

У дослідженні виявлено низку проблем, зокрема недостатньо ефективне впровадження правил у багатьох юрисдикціях, технічні складнощі ідентифікації зловмисників в децентралізованому середовищі та постійне виникнення нових схем відмивання. Протидія потребує підвищення глобальної координації: взаємного визнання і виконання правил, на кшталт Travel Rule, створення спільних платформ для обміну розвідувальною інформацією, а також узгодженого тиску на «безпечні гавані» для фінансових злочинців. Перспективним напрямом вбачається використання штучного інтелекту та машинного навчання у моніторингу транзакцій, що може виявляти приховані зв'язки і аномалії у потоках коштів.

На наше переконання, подальші дослідження в цій галузі мають бути спрямовані на пошук оптимального балансу між інноваціями і безпекою. Також перспективним є порівняльний аналіз ефективності різних національних моделей регулювання криптоіндустрії та вироблення рекомендацій щодо кращих практик. Ми переконані, що лише комплексний підхід, який об'єднає правові, технічні та організаційні заходи на національному й міжнародному рівнях, здатен забезпечити дієву протидію відмиванню коштів через віртуальні активи та сприяти безпечному функціонуванню цифрової економіки.

Список використаних джерел

1. Crypto ransom attack payments hit record $1 billion in 2023 — Chainalysis. Website: Reuters. URL: https://www.reuters.com/technology/cybersecurity/crypto-ransom-attack-payments-hit-record-1-billion-2023-chainalysis-2024-02-07, (Дата звернення 07.10.2025)
2. Money Laundering and Cryptocurrency. URL: https://airant.org/wp-content/uploads/2024/07/Report_-Money_laundering_and_Cryptocurrency.pdf#:~:text=As%20shown%20below%2C%20since%202019%2C,2024%20%28YTD, (Дата звернення 07.10.2025)
3. Financial Action Task Force (FATF). Virtual Assets: Sixth Targeted Update on Implementation of the FATF Standards on VAs and VASPs (Paris, 2025). 26.06.2025. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html#:~:text=The%20report%20assesses%20jurisdictions%E2%80%99%20compliance,taking%20supervisory%20and%20enforcement%20actions, (Дата звернення 07.10.2025)
4. Gabbiadini, Romina and Gobbi, Lorenzo and Rubera, Eugenio, Money Laundering and Blockchain Technology: Can you Follow the Trail of Cryptocurrency Transactions? (November 14, 2024). Bank of Italy Occasional Paper No. 893, Available at SSRN: https://ssrn.com/abstract=5247949 or http://dx.doi.org/10.2139/ssrn.5247949, (Дата звернення 07.10.2025)
5. A Pivotal Year for Virtual Assets. A Review of 2023 Highlights. URL: https://finintegrity.org/a-pivotal-year-for-virtual-assets-2023 highlights/#:~:text=Immunefi's%20in,the%20stolen%20funds a%20whopping%2017, (Дата звернення 07.10.2025)

6. Tornado Cash Founders Charged With Money Laundering And Sanctions Violations. Website: US Attorney's Office. URL: https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations#:~:text=business,SEMENOV%20remains%20at%20large, (Дата звернення 07.10.2025)
7. Treasury Releases 2023 DeFi Illicit Finance Risk Assessment. Website: U.S. Department of the Treasury. URL: https://home.treasury.gov/news/press-releases/jy1391#:~:text=illicit%20actors%2C%20including%20criminals%2C%20scammers%2C," , (Дата звернення 07.10.2025)
8. FATF urges stronger global action to address Illicit Finance Risks in Virtual Assets. Website: FATF. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html#:~:text=,address%20asset%20recovery%20challenges%20and, (Дата звернення 07.10.2025)
9. Financial Crimes in Digital Assets and Cryptocurrencies. URL: https://kpmg.com/us/en/articles/2023/financial-crimes-in-digital-assets.html#:~:text=Per%20the%20Action%20Plan%2C%20FATF," , (Дата звернення 07.10.2025)
10. EU passes landmark crypto regulation, MiCA, in lock step after cementing decried, dreaded virtual value AML 'travel rule'. URL: https://www.acfcs.org/eu-passes-landmark-crypto-regulation#:~:text="All%20CASPs%20will%20need%20to,analysis%20of%20the%20new%20rules, (Дата звернення 07.10.2025)
11. FATF Updates on Recommendation 15 Implementation in Jurisdictions With Materially Important Virtual Asset Sectors. URL: https://www.trmlabs.com/resources/blog/fatf-updates-on-recommendation-15-implementation-in-jurisdictions-with-materially-important-virtual-asset-sectors#:~:text=FATF%20requirements%20on%20virtual%20assets,which%20a%20jurisdiction%20is%20exposed, (Дата звернення 07.10.2025)
12. Dr. Anna Pingen. New Rules for Crypto-Assets in the EU. Eucrim. 2023. № 2. P. 143. URL: https://eucrim.eu/news/new-rules-for-crypto-assets-in-the-eu/#:~:text=,beneficiary%20of%20transfers%20of%20crypto, (Дата звернення 07.10.2025)
13. Fighting money laundering goes hand in hand with investigating the crimes it is linked to. Website: INTERPOL. URL: https://www.interpol.int/en/Crimes/Financial-crime/Money-laundering#:~:text=Our%20initiative%20against%20money%20laundering,Forestry%20crime, (Дата звернення 07.10.2025)
14. TRISA - Travel Rule Information Sharing Alliance. URL: https://notabene.id/travel-rule-messaging-protocols/trisa, (Дата звернення 07.10.2025)
15. Cryptocurrency investigations. Website: United Nations. URL: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/investigation/cryptocurrency.html,(Дата звернення 07.10.2025)