https://doi.org/10.26565/2075-1834-2023-35-03
УДК 347.73:336.22

М.Л. РАФАЛЬСЬКИЙ
аспірант юридичного факультету,
адвокат
E-mail: maksimrafalskiy@gmail.com ORCID: https://orcid.org/0000-0001-9016-8613
Академія адвокатури України
м. Київ, 01032, бульвар Тараса Шевченка, 27

МЕТОДИ БОРОТЬБИ З ПРАВОПОРУШЕННЯМИ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

АНОТАЦІЯ. *Вступ.* Ця стаття присвячена дослідженню методів боротьби з правопорушеннями в децентралізованих системах, зокрема в мережах блокчейн. Автор проводить аналіз основних підходів до боротьби з такими правопорушеннями і розглядає різні методи, які можуть бути використані для попередження, виявлення та вирішення вказаних проблем. В статті розглядаються можливі ризики та виклики, пов'язані з боротьбою з правопорушеннями в децентралізованих системах, а також висвітлюються переваги та недоліки різних підходів.

Короткий зміст основних результатів дослідження. Надано роз'яснення особливостей та складності організації роботи децентралізованих мереж таких як блокчейн, і від повідно, складність виявлення та протидії правопорушенням в таких мережах. Також надано роз'яснення щодо різних підходів та методів боротьби із правопорушеннями в децентралізованих системах, а також які є методи боротьби з такими правопорушеннями, та які методи пропонує автор статті.

Висновки. Вперше уніфіковано та надано перелік основних методів із правопорушеннями в децентралізованих мережах таких як блокчейн саме в контексті кримінального права. Також розглянуто методи боротьби та попередження із такими правопорушеннями з точки зору різних підходів, в тому числі, юридичного, технічного, організаційного тощо. В цілому, стаття пропонує висновки щодо різних підходів до попередження та протидії із правопорушеннями в децентралізованих системах, розгляд різних методів боротьби із такими правопорушеннями, а також наголошує на необхідності продовжувати дослідження в цій області.

КЛЮЧОВІ СЛОВА: *децентралізовані мережі, блокчейн, кібербезпека, атаки, кримінальне право.*

Як цитувати: Рафальський М. Л. Методи боротьби з правопорушеннями в децентралізованих системах. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Право».* 2023. Вип. 35. С. 24-34. https://doi.org/10.26565/2075-1834-2023-35-03

In cites: Rafalskyi M. L. (2023). Methods of combating offenses in decentralized systems. *The Journal of V.N. Karazin Kharkiv National University, Series «Law»*, (35), P. 24-34. https://doi.org/10.26565/2075-1834-2023-35-03(in Ukrainian)

Вступ. У сучасному світі децентралізовані мережі стають все більш популярними і поширеними.

Проте разом з їхніми перевагами, такими як відсутність централізованого керівництва, відкритість, ефективність, гнучкість і використання криптографічних протоколів для захисту інформації, з'являються й певні проблеми. Одна з таких проблем - це можливість зловживання децентралізованою мережею для здійснення правопорушень, таких як атаки та шахрайство. Вивчення проблематики боротьби з правопорушеннями в децентралізованих системах має велике значення як для для наукових досліджень, так і практичних застосувань. Оскільки децентралізовані системи стають все більш поширеними, з'являється необхідність розуміти, які виклики та проблеми пов'язані з їх використанням. Наприклад, в сфері фінансів децентралізовані мережі стають все популярнішим засобом здійснення транзакцій Однак, це також призводить до появи нових видів фінансових правопорушень, таких як різні види атак. Вивчення проблематики боротьби з такими правопорушеннями дозволяє розробляти ефективні та безпечні рішення для захисту фінансових транзакцій в

© Рафальський М.Л., 2023
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0

децентралізованих мережах. Крім того, в децентралізованих мережах можуть виникати і інші види правопорушень, наприклад, різні види шахрайства та зловживання довірою. Вивчення таких проблем дозволяє розробляти ефективні механізми контролю та захисту від цих правопорушень. Вивчення проблематики правопорушень у децентралізованих системах може сприяти вирішенню різноманітних завдань, пов'язаних з розробкою ефективних методів виявлення, розслідування та запобігання правопорушень в таких системах, а також стимулювати розвитку нових технологій, які зменшать ймовірність виникнення правопорушень у децентралізованих системах.

Мета дослідження. Опис та аналіз існуючих та потенційних методів виявлення, розслідування та запобігання правопорушень в децентралізованих системах є досить важливим на сьогоднішній день. Таке дослідження дозволяє зрозуміти, які методи використовуються наразі, які є їх переваги та недоліки, а також які можуть бути потенційні шляхи розвитку та вдосконалення таких методів. Результати огляду методів боротьби із правопорушеннями у вказаних системах можуть бути корисними для практичних застосувань в галузі кібербезпеки та правопорядку.

Аналіз останніх досліджень і публікацій. Щодо праць з даної проблематики, то у вітчизняній юридичній літературі саме щодо методів боротьби із правопорушеннми в децентралізованих системах досліджень практично не проводили, особливо в контексті кримінального права. Існують окремі дослідження та статті, які присвячені аналізу правових аспектів децентралізованих систем, включаючи аналіз їхнього впливу на кримінальне право, а також аналіз правопорушень в сфері обігу віртуальних активів. Дослідження в цій сфері проводили Ю.П. Калайда, К.О. Черевко, О.О. Любіч, Т.Л. Дмитренко, В.В. Козій, М.О. Думчиков, Я.А. Шевцов, О.О. Коротка, Д.В. Казначеєва, П.П. Бурдін, В.Д. Іванюк, В. Школьніков, О. Корнейко, Ю. Орлов.

Однією з основних проблем, пов'язаних із правопорушеннями в децентралізованих системах, таких як блокчейн, є те, що вони можуть бути дуже складні для виявлення, розслідування та попередження. Наприклад, у децентралізованих мережах кількість учасників може бути дуже великою, а їх дії можуть бути анонімними. Це робить процес виявлення та розслідування правопорушень надзвичайно складним. Крім того, в децентралізованих системах можуть виникати такі види правопорушень, як атаки, шахрайство, зловживання довірою та інші види кіберзлочинності. Ці правопорушення можуть завдати значної шкоди користувачам децентралізованих мереж, включаючи втрату фінансових активів, викрадення конфіденційної інформації, пошкодження репутації та інші наслідки.

У відкритих мережах атакам протидіють у такі способи, як розробка та запровадження центральним вузлом відповідного захисного програмного забезпечення, адміністративні заходи, наприклад, постійна звітність та централізоване зведення даних. В децентралізованих мережах все складніше, враховуючи особливості функціонування децентралізованих мереж. Наразі боротьба із правопорушеннями вирішується декількома способами. Один із них – це технічний. Наприклад, що в консенсус Proof of stake (PoS) закладений такий механізм, що учасникам невігідно здійснювати атаки. За допомогою proof-of-stake (POS) власники криптовалют перевіряють блокові транзакції на основі кількості поставлених монет. Якщо брати основну ідею, то PoS вносить таку новацію в порівнянні з Proof of Work (PoW), яка полягає в тому, що користувачі, які володіють великою кількістю криптовалюти, зацікавлені в першу чергу в тому, щоб ця система досягала консенсусу серед усіх валідаторів коректним чином, і була невразливою до різних атак, збоїв типу дабл-спендінг (подвійне витрачання монет), атаки на роздвоєння блокчейну, підтвердження неправильних транзакцій, або якесь інше шахрайство в децентралізованій мережі. Відповідно, використовуючи цю ідею, були побудовані такі алгоритми, в яких ймовірність того, що валідатор зможе сформувати правильний блок та підтвердити транзакції, буде пропорційно до кількості його монет у гаманці порівняно з монетами, які беруть участь у PoW. Атака 51% обчислювальної, а саме голосувальної здатності якщо загальними словами, не має сенсу для PoS, тому що власник більшості монет, які беруть участь у PoS, фінансово не зацікавлений проводити таку атаку, тому що якщо це станеться, то сама валюта втратить свою репутацію (за рахунок повторного відтворення або витрати одних і тих самих монет, неконтрольованої емісії). Відповідно, власник цих монет отримає фінансову втрату,

тому що монети фактично знеціняться у всій системі. Підтримка нового вузла в мережі та володіння деякими монетами – це вже достатні умови для того, щоб працювати з PoS. Отже, «атака 51» в PoS немає сенсу, тому одним із варіантів рішення атаки 51 є перехід із PoW в PoS. Враховуючи, що деякі блокчейни і децентралізовані системи на них використовують PoW, тому це питання досі актуально. В свою чергу, у деяких блокчейнах PoW вже розроблені такі алгоритми, що дуже складно або взагалі неможливо змінити правила.

У деяких блокчейнах може бути закладений алгоритм, коли жодна із сторін не може ошукати іншу. Це проявляється в тому, що коли сторони генерують транзакції, вони публікують секретні значення та надсилають один одному. Якщо одна зі сторін захоче ввести в оману іншу, і опублікувати попереднє значення, де вона, наприклад, не відправляла монети другій стороні, алгоритм блокчейна побудований таким чином, що в цьому випадку та сторона, яку намагаються ошукати, може забрати всі монети собі.

Також простим технічним рішенням є такий алгоритм роботи мережі як більшість «чесних вузлів». Так, якщо користувачі будуть підключатися, наприклад, тільки до одного вузла мережі, то жодна перевірка не допоможе захиститися від обману, оскільки вказаний вузол може віддавати користувачам повністю неправильні дані, може віддавати такі заголовки, щоб вони відповідали тому, що він надсилає, і відповідно вводити в оману цих користувачів про реальну ситуацію в мережі блокчейн. Відповідно для того, щоб бути максимально впевненими в тому, що користувачам приходять правильні дані, їм потрібно максимально розподілити ті вузли, з якими вони «спілкуються». У цьому випадку користувачам потрібно «спілкуватися» з якомога більшою кількістю вузлів, і таким чином зловмисникам для того, щоб надсилати користувачам неправильні дані, потрібно буде захопити вже набагато більше вузлів.

Також, в блокчейні захист від обману може бути закладений в Дереві Меркла. Дерево Меркла – це математична структура даних на основі хешу, яка збирає результати всіх транзакцій у блоці. Це метод швидкої перевірки точності даних децентралізованим способом. Завдяки своїм функціональним можливостям Дерево Меркла використовують більш ефективно у плані шифрування даних блокчейну. У Дереві Меркла одна сторона не зможе ошукати іншу через ту властивість хеш-функції, незворотності та стійкості до колізій, які закладені в нього на рівні алгоритму. Дерево Меркла використовується для отримання індифікатора блоку. Отримуючи ідентифікатор блоку, хешується його заголовок, в який і входить значення Дерева Меркла. Коли зловмисник хоче підробити одну транзакцію, змінюється вказане значення, відповідно, Дерево Меркла теж зміниться, і всі верифікатори, валідатори бачитимуть, що зловмисник намагається змінити транзакцію. Також принцип довіри закладено у федеративних сайдчейнах (federated sidechains). Сайдчейн — це незалежний розподілений реєстр із власним алгоритмом консенсусу, типами й правилами транзакцій. Кожен сайдчейн ланцюг керується власним набором серверів (включаючи валідаторів) і не покладається на валідаторів в головній мережі для транзакцій у сайдчейні. У федерейтед сайдчейн працюють з використанням Multisignature address - адреси, до якої прив'язано кілька пар ключів. У цьому випадку виділяється деяка підмножина умовно довірених сторін, яким сторони довіряють, при цьому вони довіряють тому, що всі разом вони не змовляться для того, щоб витратити монети раніше. Вся модель безпеки ґрунтується на наявності достатньо великого набору окремих учасників у групі чи федерації, які розподілені географічно та загальновідомі.

Отже, керівним принципом протидії правопорушенням в децентралізованих мережах є такий алгоритм дії блокчейну, що у її учасників є стимул чесно працювати у мережі. Наприклад, в BFT-протоколах такого стимула немає. Вони розроблені для так званих permissioned ledgers, тобто вони розроблені без урахування самого стимулу для учасників чесно працювати в самій мережі. Передбачається, що такі стимули перебувають поза роботою самого протоколу. Не розглядаються ні нагороди за блок, ні різні стратегії поведінки користувачів. В цьому випадку для сучасних дослідників залишається дуже широка область і з точки зору теорії ігор, і точки зору розробки стратегії винагороди для учасників, для того, щоб повноцінно розгорнути такі протоколи для роботи в децентралізованих мережах. На противагу BFT-протоколам, в PoS є вказаний стимул. У PoS користувачам з великою кількістю монет, які інвестували у криптовалюти, не вигідно робити атаки, тому що у разі успішної атаки відбудеться знецінення криптовалюти, і їх

інвестиції теж знеціняться. Тому найвигідніша стратегія – це чесне дотримання протоколу.

Також можуть бути такі алгоритми, що достатньо тільки одного чесного учасника, щоб система діяла. Так, у протоколах Zero-knowledge proofs (доказ з нульовим розголошенням (інформації)) є властивість, що тільки один учасник повинен бути не скомпрометований, щоб результати обчислень збереглися у безпеці. Zero-knowledge proofs - це метод, за допомогою якого одна сторона (доказуючий) може довести іншій стороні (верифікатору), що щось правдиве, не розкриваючи жодної інформації, окрім факту, що це конкретне твердження є істинним. Інакше кажучи, щоб скомпроментувати генерацію довірених параметрів системи, кожен із учасників має бути скомпроментований. Вся надійність зазначених протоколів повністю залежить від довіри до цієї групи людей, а саме до того, що вони коректно скористалися протоколом формування загальних системних параметрів та знищили використані секрети. Взагалі, такий принцип, як стимул поводити себе чесно в блокчейні, без обману та шахрайства, був закладений розробниками, виходячи з різних теорій математичних моделей прийняття оптимальних рішень в умовах конфлікту. Наприклад, з точки зору теорії ігор, якщо два суб'єкти покладуть у свій платіжний канал по 5 біткоїнів, і якщо кожен з них у будь-який момент часу не обманюватиме, вони залишатимуться при своїх коштах. У одного буде 5 біткоїнів, у іншого буде теж 5 біткоїнів. Якщо ж один із суб'єктів обманюватиме, тоді його 5 біткоїнів дістануться іншому суб'єкту. Тобто, моделюються такі сценарії, що перебувати в ситуації «не обманювати» більш вигідно, і розуміти, що нікому із суб'єктів не вигідно обманювати, і вигідно підтримувати комунікацію між собою, і вигідно зберігати канал у відкритому стані. Хоча теорія ігор знаходить застосування у соціальних, економічних та політичних науках, вона також застосовується до функціонування основних блокчейнів, включаючи Біткойн. Теорія ігор була введена в блокчейн Біткойна для того, щоб передбачити поведінку майнерів і, перш за все, спонукати їх до доброчесної поведінки.

У контексті розподілених технологій питання довіри може мати багато вимірів. Якщо роль розподіленої техно-соціальної системи полягає в тому, щоб з'єднати людей, якщо вона дозволяє або спирається на співпрацю окремих осіб у вимірі міжособистісної довіри, питання полягає в тому, як ми можемо (або: чи потрібно нам) довіряти незнайомцю (часто анонімному), з яким ми використовуємо ту саму розподілену систему. З іншого боку, ми також повинні мати певний рівень довіри до самої системи, і в цьому випадку нам потрібно дивитися на інституційні аспекти довіри. Тут головне питання полягає в тому, чи надійні технології, на які ми покладаємося. Ми можемо визначити технологію у вузькому сенсі, і, отже, питання довіри та надійності технічних систем, і артефактів спрощується до питання технічної надійності: безпека комп'ютерних систем, відсутність у них помилок та вразливостей, чи працює система так, як задумувалась та рекламувалась. Більш широке визначення також враховує людські та інституційні елементи, які розробляють і керують цими технічними системами, а отже, надають їм право власності. У такому підході питання довіри стає більш схожим на більш традиційні форми інституційної довіри. Управління технологіями охоплює ці людські та інституційні елементи, а вплив управління на надійність технічних систем перетворив це питання на галузь досліджень, що швидко розвивається.

Крім атак та шахрайства, передбачені і правомірні дії у децентралізованих мережах, в яких рішення приймаються більшістю користувачів, тобто, передбачається електронне самоврядування або блокчейн-демократія. До речі, вищевказану Концепцію спрощеної верифікації платежів (SPV) можна розглядати як приклад електронної демократії, де вузли самі визначають «правила гри». Важливо враховувати, що від повного вузла мережі SPV відрізняється тим, що користувачі особисто не перевіряють транзакції, тому що в них просто немає всіх даних, щоб їх перевірити. Користувачі по суті перевіряють, щоб дана транзакція була перевірена і підтверджена більшістю вузлів в мережі. Відповідно, в даному випадку користувачі довіряють тому, що більшість вузлів в мережі проводять дану політику, вони дотримуються правил мережі і не проводять будь-яких махінацій. Тобто, відмінність в тому, що користувачі не самі перевіряють транзакції, а довіряють це більшості.

Також актуальним питанням в цій темі є розслідування таких правопорушень та встановлення осіб-правопорушників. Складність розслідування правопорушень в децентралізованих системах, таких як

блокчейн, може бути викликане рядом факторів. По-перше, транзакції у блокчейні анонімні, тому ідентифікація злочинців може бути складною. Хоча у деяких блокчейнах використовуються публічні ключі для ідентифікації користувачів, іноді їх може бути важко пов'язати з реальними особами. По-друге, транзакції у блокчейні є не змінними, тому якщо правопорушення відбулось, воно може бути зафіксоване назавжди. Це може ускладнити процес виправлення такого правопорушення та повернення втрачених коштів. По-третє, децентралізована структура блокчейнів означає, що немає централізованої влади, яка може регулювати транзакції або розслідувати злочини. Це може призвести до того, що учасники мережі повинні взаємодіяти самостійно, щоб виявляти та розслідувати правопорушення. По-четверте, масштабність блокчейнів може призвести до того, що розслідування правопорушень може стати дуже складним завданням. Наприклад, Біткоїн, найбільший блокчейн в світі, має велику кількість користувачів і транзакцій, що ускладнює процес виявлення та розслідування вказаних правопорушень.

На сьогодні є дуже ускладненим вирішення як питання встановлення правопорушників, які «ховаються» в мережі як окремі комп'ютери/вузли, так і питання, а чи дійсно блокчейн є децентралізованим, і рішення в ньому приймаються багатьма фізичними особами, як окремими комп'ютерами/вузлами, а не однією особою, яка є власником десятків різних комп'ютерів/вузлів. На даний час одним із вирішень вказаних проблем є пропозиція відслідковувати весь ланцюжок транзакції конкретної криптовалюти, яка стала предметом правопорушення, які по ідеї на різних етапах можна зв'язати з конкретними особами, наприклад, інтернет-магазинами, криптобіржами, офіційними майнерами. Наприклад, у біткоїні легко відстежити за конкретною адресою всю історію платежів, так як база даних вказаного блокчейну відкрита, а індексація за адресами проводиться доволі легко. Крім того, можна побачити весь ланцюжок повної передачі монет, як вони розподілялися і ходили між різними адресами, це також допоможе зв'язати адреси та їх відповідність між цією адресою та конкретними користувачами. Проте, наявність деанонімізованих осіб надто ускладнює встановлення правопорушників. Наприклад, в мережі Біткоїн все працює без визначення особистості. Тож постає питання, чому не можна персоналізувати гаманець, тобто прив'язати його до конкретної особи. Біткоїн як платіжний протокол не вимагає прив'язки якоїсь особистості, тому що він працює за законами математики, а математика не дозволяє описати людину як особистість. Більше того, це не є необхідною умовою для перевірки транзакцій, тобто тут достатньо просто електронно-цифрового підпису, а щодо того, хто володіє відповідним ключем і може генерувати такі підписи, це вже питання, яким Біткоїн не займається. Відповідно, біткоїнами може володіти якийсь робот, якийсь комп'ютер за певним алгоритмом, може володіти людина, може одним і тим же не витраченим виходом володіти кілька людей, або кілька людей можуть знати один і той самий особистий ключ. Що стосується персоналізації, незважаючи на те, що порушується приватність у плані того, що біткоїн можна деанонімізувати, проте, знаходячи зв'язки того, що певній людині належить певний особистий ключ або певний набір особистих ключів відповідних адрес, з певним ступенем, з певною ймовірністю можна стверджувати, що конкретні монети належать конкретним людям. В загальному плані база даних Біткоїна відкрита, але ніяких даних про конкретних осіб у ній не вказано. Про те, як складно відслідкувати транзакції, можна побачити на прикладі криптобіржі Bitfinex. Так, в 2016 році з однієї з найбільших у світі криптобірж Bitfinex було викрадено біткоїнів на суму 1,33 мільярда доларів. Спочатку пропонували велику винагороду для тих, хто зможе відслідкувати весь ланцюжок транзакцій, куди вивели викрадені кошти. А потім запропонували вже самим хакерам за винагороду повернути викрадені кошти. Сукупна винагорода становила приблизно 400 мільйонів доларів США за поточною ціною BTC, якщо всі біткоїни будуть повністю відновлені.

Іншим важливим в цій частині постає питання, чи можна притягти до відповідальності розробників блокчейнів. Через повну децентралізацію в блокчейні нерідко неможливо дізнатися, хто є розробниками. Як варіант, якщо ці розробники анонімізовані, навіть якщо не безпосередньо. Так, для того, щоб почати роботу в блокчейні, вузлу необхідно зробити запит на один із DNS серверів, які підтримуються розробниками ядра блокчейна або членами комьюніті, і зберігають базу про існуючі активні ноди (вузли). Служби доменних імен (Domain name

Services (DNS)) — це загальнодоступні каталоги, розміщені в мережі комп'ютерів, які приймають вхідні дані від користувачів Інтернету та веб-сайтів, наприклад через браузер, і переводять їх у форми, зрозумілі комп'ютерам. Після запиту на DNS сервер новий вузол дізнається IP-адреси, до яких він хоче під'єднатися. Після цього він підключається до цих вузлів і відбувається протокол звіряння версій. І після цього вузлу потрібно завантажити весь актуальний блокчейн, який активний на даний час. Після того, як існуючі блоки синхронізовані, цей вузол починає брати повну участь у протоколі передачі даних через мережу та обмінюватися новими блоками та транзакціями з іншими вузлами. Якщо за вказаними DNS серверами стоять анонімізовані учасники, тоді є можливість розуміти, яке саме програмне забезпечення було в черговому оновленні, коли відбулася атака, яка стала можлива, наприклад, через вразливість у вказаному оновленому програмному забезпеченні, і з цієї точки вже проводити розслідування, чи було спеціально допущено вказану вразливість, чи це зроблено ненавмисно.

Друге питання, а чи взагалі розробники несуть відповідальність. Насправді будь-яке програмне забезпечення, яке офіційно поширюється, має так звані Terms of use (Умови використання), відповідно в них прописано, що користувачі можуть фактично пред'явити розробникам у випадку, якщо виникли якісь проблеми під час використання їх програмного забезпечення. Ці особливості відрізняються від одного додатка до іншого, і по суті як і завжди, все полягає тільки в тому, наскільки користувачі довіряють розробникам програми. Проте, Terms of use має місце, коли це програмне забезпечення пов'язане офіційно із розробниками. Постає логічне питання, як бути в даній ситуації із програмним забезпеченням, яке розробили анонімні розробники, наприклад, вихідний комп'ютерний код розподіленої де централізованої мережі, де відбуваються транзакції криптовалют. Також один із способів впевнетись, що розробникам можна довіряти – це перевірка на спеціальному вебсервісі для спільної розробки програмного забезпечення GitHub, де розробники можуть викласти свої напрацювання в розробці програмного забезпечення, а інші користувачі можуть виявити помилки, а іноді і спеціальні шпаринини, в програмному коді, які залишають розробники для здійнення майбутніх правопорушень. Далі, треба з'ясувати, а чи дійсно це було правопорушення, тобто дія з явним умислом, недбалість чи просто людський фактор. Наприклад, коли розробники знали, але не уникли прихованих умов у коді, у смарт-контракті, або вважали, що такі приховані умови не є небезпечними. Або, наприклад, у неявному вигляді, через недолік досвіду, були зроблені помилки розробників. Або навмисно були написані програмістами такі приховані умови з метою повного контролю над кодом, наприклад, під час емісії токенів ICO (initial coin offering), або вразливість, яка дозволяє розробникам змінювати ціну токена, знищувати токени, блокувати транзакції. Або використання небезпечних алгоритмів, коли програмісти просто крадуть чужий код і застосовують у проекті, при цьому не знають, які в первинному коді були вразливості. З іншої сторони, розробники блокчейну теж повинні бути захищені від неаргументованих позовів. Так, нещодавно австралійський комп'ютерний вчений Райт подав до суду на 15 розробників блокчейну, намагаючись повернути близько 111 000 біткоїнів – на даний момент вартістю близько 2,5 мільярда доларів – після того, як він втратив зашифровані ключі доступу до них, коли його домашню комп'ютерну мережу нібито зламали. На його думку, розробники блокчейну для мережі біткоїну мали передбачити механізм повернення доступу до гаманців при втраті ключів. В цій ситуації позиція суду повинна бути в тому, що опція повернення доступу до гаманців не передбачалась в самій логіці блокчейну, в іншому випадку губиться сама суть цієї технології, і позитивне рішення у вказаному позові призведе до колапсу ринку криптовалют.

Отже, які можуть бути способи боротьби та попередження вказаних правопорушень. Один із варіантів вирішення проблеми з шахрайством у блокчейні – штраф, який встановлений, наприклад, в системі платіжних каналів Lightning network. Дані платіжні канали необхідні для того, щоб здійснювати транзакції між користувачами розподілених систем швидко, не фіксуючи проміжні стани у головному блокчейні.

Крім цього, це ще спосіб маршрутизації платежів через безліч каналів, об'єднаних однією мережею. Важлива властивість Lightning network платіжних каналів полягає в тому, що вони є trustless, це означає, що два

суб'єкти, які передають один одному цінності всередині цих каналів, можуть не довіряти один одному. Вони можуть не сподіватися на добру волю кожного з них, їм достатньо того, що вони розуміють, що протокол lightning network влаштований таким чином, що за спроби порушити консенсус інша сторона платіжних каналів буде оштрафована. Технологія блокчейн дозволяє користувачам довіряти тому, що всі в системі обмінюються тією ж інформацією. Завдяки переміщенню довірчого елемента до системи, що перевіряється криптографічно, потреба довіряти будь-якій окремій особі зникає. Таким чином, це система «довіри без довіри» («trustless trust»). Також, у децентралізованій біржі на базі atomic swap передбачено штраф за невиконання своїх зобов'язань з виконання ордера з купівлі-продажу монет. Так, коли розміщується заявка на децентралізованій біржі, користувачам необхідна гарантія, що заявку на виконання ордера буде виконано. Тому що якщо немає таких гарантій, тоді це чудовий механізм для маніпуляції ціною, оскільки суб'єкт може скасувати свій ордер. Так, у цьому випадку покупець може виставити ордер, потім у разі чого може його прибрати, хоча він не має такої опції. Саме тому на централізованій біржі є гарантія виконання ордера. Доки ордер існує на децентралізованій біржі, там необхідно ввести штрафи в тій чи іншій валюті, якщо суб'єкти захочуть порушувати дану їм обіцянку і не захочуть виконувати свої власні ордери. Різниця між централізованими та децентралізованими біржами та системою штрафів на останніх в тому, що гарантія виконання ордера у разі централізованих бірж – це весь баланс у бірж, а в децентралізованих біржах необхідні штрафи в межах порушення зобов'язань. Також методом попередження вказаних правопорушень може бути механізм застави. Заставні суми використовуються задля забезпечення виконання зобов'язань. Чим більша застава, тим більша ймовірність виконання. Користувач (трейдер) сам собі будує ймовірності виконання, виходячи із співвідношення застави та суми угоди. Ідеологія заставних сум при використанні децентралізованих бірж полягає в тому, що не обов'язково будувати систему таким чином, щоб у заставу потрапляла вся сума як на централізованих біржах. У деяких випадках користувачеві надається можливість залишати меншу заставу, ніж уся сума угоди. Таким чином кожен користувач самостійно вирішуватиме, які ордери швидше за все будуть виконані, виходячи з розміру заставних сум, тому що чим більше заставна сума, тим більша ймовірність того, що ордер буде виконаний.

Участь медіатора як спосіб протидії шахрайству. Медіатор по суті виступає вирішувачем виконання транзакції.

Наприклад, є два учасники, сторона-1 та сторона-2, і є медіатор між ними. Кожна зі сторін і медіатор має свої особисті відкриті ключі. І, наприклад, сторона-1 заявляє, що монети можуть бути переведені лише якщо дві з трьох сторін підпишуть транзакцію. І таку саму операцію проводить сторона-2. Якщо сторони домовилися між собою, тобто підписали транзакцію удвох, то одразу відбувається переведення коштів, і у зворотний бік теж. Якщо ж ні, тут вступає медіатор, який виконує свою роль, вирішує суперечку між двома сторонами. В цьому випадку сторони надають йому певні докази, і він на підставі цих доказів може підписати транзакцію, яка переведе цінність одній чи іншій стороні. За такої схеми медіатор не може забрати собі монети, але в цьому випадку існує ризик, що він змовиться з однією зі сторін, а друга сторона залишиться ні з чим.

Томудругий спосіб – це збільшити кількість медіаторів.

Аудіт як засіб контролю та протидії правопорушенням. Він може проводитись в централізованих та децентралізованих мережах. Аудитору потрібно підключитися до одного або кількох валідаторів мережі, далі завантажити історію транзакцій і верифікувати її відповідно до правил протоколу. Внаслідок цього аудитор отримує кінцевий стан облікової системи. Цей кінцевий стан він повинен звірити з тими станами, які отримали валідатори чи інші аудитори, які використовують клієнти для своїх цифрових гаманців. Якщо стан аудитора збігається з тим, що бачать клієнти та інший валідатор, значить все в обліковій системі виконано правильно і всі транзакції враховані. Якщо є якісь розбіжності, кінцевий стан не збігається, значить щось у роботі валідаторів було порушено, і треба взяти історію транзакцій і виконати всі транзакції заново. Це не вплине на кінцевих користувачів, але дозволить відновити правильний стан кінцевої облікової системи. У децентралізованому середовищі аудитору фактично потрібно стати частиною мережі, тобто запустити та підтримувати вузол аудитора. У порівнянні з традиційними

обліковими системами, аудит децентралізованих мереж вважається більш автоматизованим і достовірним, в деяких випадках він може виконуватися в режимі реального часу. Якщо аудитор стає частиною мережі, і запускає свій власний вузол, він у режимі реального часу отримує транзакції звичайних користувачів, застосовує їх до свого стану облікової системи та бачить, які вони мають бути у кожний наступний момент часу. Хоча автоматичний аналіз є корисним інструментом для виявлення типових вразливостей, він не може виявити всі недоліки безпеки. Його мета — знайти недоліки безпеки та вразливості в коді. Це необхідний крок у криптобезпеці, оскільки блокчейни працюють на складних наборах самовиконуваного коду, а це означає, що ручна перевірка іноді все ще необхідна. В деяких блокчейн проєктах, які є централізованими, є ті особи, яких можна притягнути до відповідальності за правопорушення. Так, наприклад, якщо схематично розглянути ролі платформи токенізації, то там є розробники програмного забезпечення, є певна спільнота, яка приймає ключові рішення щодо якихось змін у протоколі, є регулятор - це як правило представник якогось політичного характеру, який стежить за виконанням усіх законодавчих норм тощо, далі є облікова система самих вузлів валідаторів, облікова система для вузла аудитора, адміністратори платформи та кінцеві користувачі. Якщо це стосується проєктів, де власники та/або розробники деанонімізовані, то це не тільки як спосіб боротьби із правопорушеннями, а і як важіль контролю на рівні щоденної операційної діяльності. Також протидія шахрайству може бути прописана на рівні алгоритмів. Технологія блокчейн може забезпечити платформі токенізації деякі властивості, залежно від середовища функціонування. Для розподіленого загальнодоступного середовища це такі властивості як перевірка цілісності бази даних, синхронізація в режимі реального часу, консенсус серед валідаторів, прозорість і аудит в режимі реального часу, а також доказ шахрайства. Доказність шахрайства полягає в тому, що якщо всі транзакції зберігаються в ланцюжку блоків, клієнтське програмне забезпечення може зберігати заголовки цих блоків і перевіряти свої транзакції, підтверджені на входження у відповідні блоки. Якщо через якийсь момент часу облікова система заявляє, що частина транзакції не була підтверджена або зникла кудись з історії, або з'явилися інші транзакції, то клієнт може мати доказ, який він отримав у минулому. Це дозволить йому повідомити про це керівникам або регулюючим органам і власне довести шахрайство з боку облікової системи. Тобто в такій системі є доказованість шахрайства, на відміну від розподіленого децентралізованого середовища, тому що децентралізовані системи не піддаються регулюванню, і офіційний регулятор не матиме значення, тому що правила є загальноприйнятими для всіх, і неможливо відкрите співтовариство змусити змінити історію. Тому і придумані різні консенсуси, щоб ця відкрита спільнота сама всередині регулювала підтримку життєдіяльності системи тим, щоб її учасники були чесними.

Підсумовуючи, зазначаємо, що врахочуючи повсюдне розповсюдження децентралізованих мереж і їх широку інтеграцію в фінансові системи, проблема правопорушень у вказаних мережах стає досить актуальною. Методів боротьби із вказаними правопорушеннями є кілька, серед яких виділяємо технічні, на рівні розробки безпеченого програмного забезпечення, розробки нових або удосконалення існуючих консенсусів блокчейнів, вровадження на технічному рівні таких алгоритмів і консенсусів в блокчейнах, щоб мінімізувати саму можливість здійснювати правопорушення, впровадження аудиторів і медиаторів, а також юридичні методи. На нашу думку, дієвим інструментом на сьогодні в децетралізованих мережах є проходження KYC (Know Your Client («Знай свого клієнта»), дана операція проводиться для ідентифікації клієнтів, законності та суті операції) для деанонімізації учасників мережі та надання їм суб'єктності, не тільки нести обов'язки та відповідальність, але і мати права для відшкодування нанесених їм збитків. Також проведення широкої інформаційної роботи на тему того, що учасники самі несуть відповідальність понесення збитків у разі їх діяльності в децентралізованих мережах, де учасники представлені без ідентифікації особи. В розрізі кримінального права, на нашу думку, до вказаних правовідносин необхідно застосовувати міжнародні принципи, угоди, наприклад, стандарти Anti-money laundering (AML), які засновані на процедурах, спрямованих на протидію відмиванню грошей та обмеження правопорушників від перетворення незаконних коштів на законні доходи. Іншим дієвим інтструментом є

моніторинг переведення коштів з криптовалют в фіатні кошти, який може проводитись на рівні банківських установ. Адже, рано чи пізно шахрайські проекти захочуть перевести свої криптокошти в готівку, і на цьому етапі їх можна виявити, наприклад, банк може запросити походження коштів, аж до виписок з транзакціями криптовалют або договір, інший документ, який підтверджує передачу токенів (англ. Token transfering instrument). Що стосується проблем вирішення питань у самоврядуванні у блокчейні, тут можна застосувати аналогію вирішення суперечок на он-лайн маркетплейсах (Alternative Dispute Resolution). Отже, правопорушення є серйозною проблемою в децентралізованих системах, таких як блокчейн, тому необхідно розробляти нові методи боротьби з ними. Важливість цієї проблеми полягає в тому, що вказані правопорушення можуть призвести до великих фінансових втрат, викликати сумніви щодо безпеки і надійності децентралізованих систем та загрожувати їхньому подальшому розвитку. Розробка нових методів боротьби з цією проблемою може значно сприяти забезпеченню ефективної та безпечної роботи децентралізованих систем та підвищити рівень довіри до них. Таким чином, подальші наукові дослідження та практичні застосування в цій сфері є дуже важливими для їхнього розвитку та успішної імплементації у різних галузях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.What Does Proof-of-Stake (PoS) Mean in Crypto? [Інтернет]. Investopedia. [цит. за 21, Лютий 2023]. Доступний у: https://www.investopedia.com/terms/p/proof-stake-pos.asp

2.Синхронизация кошельков с Биткоин сетью [Інтернет]. Хабр. [цит. за 21, Лютий 2023]. Доступний у: https://habr.com/ru/company/distributedlab/blog/416469/

3.What Is a Merkle Tree & What Is Its Role in Blockchain? [Інтернет]. Bybit Learn. 2022 [цит. за 30, Січень 2023]. Доступний у: https://learn.bybit.com/blockchain/what-is-merkle-tree/

4.Federated Sidechains | XRPL.org [Інтернет]. [цит. за 30, Січень 2023]. Доступний у: https://xrpl.org/federated-sidechains.html

5.Shinobi. Federated Sidechains Are Bitcoin's Original Upgradeable Sidechain Implementation [Інтернет]. Bitcoin Magazine - Bitcoin News, Articles and Expert Insights. [цит. за 21, Лютий 2023]. Доступний у:
https://bitcoinmagazine.com/technical/federated-sidechains-bitcoin-original

6.Обзор актуальных протоколов достижения консенсуса в децентрализованной среде [Інтернет]. Хабр. [цит. за 21, Лютий 2023]. Доступний у: https://habr.com/ru/company/distributedlab/blog/419185/

7.Zero-knowledge proofs | ethereum.org [Інтернет]. [цит. за 22, Лютий 2023]. Доступний у: https://ethereum.org/en/zero-knowledge-proofs/

8.Теория игр в криптовалютах [Інтернет]. Decimal. 2022 [цит. за 22, Лютий 2023]. Доступний у: https://decimalchain.com/blog/ru/teoriya-igr-v-kriptovalyutax/

9.Becker M, Bodó B. Trust in blockchain-based systems. Internet Policy Review [Інтернет]. 20, Квітень 2021 [цит. за 30, Січень 2023];10(2). Доступний у: https://policyreview.info/glossary/trust-blockchain

10.Как работает мультиподпись в Биткоине [Інтернет]. Хабр. [цит. за 22, Лютий 2023]. Доступний у: https://habr.com/ru/company/distributedlab/blog/415757/

11.Up to US$400 Million Reward for Return of Stolen 2016 Bitcoin [Інтернет]. [цит. за 04, Лютий 2023]. Доступний у: https://www.bitfinex.com/posts/494

12.Coinscapture. 7 Best Blockchain DNS For 2022 [Інтернет]. Medium. 2022 [цит. за 22, Лютий 2023]. Доступний у: https://medium.com/coinscapture/7-best-blockchain-dns-for-2022-d9645cb80560

13.GitHub: Let's build from here [Інтернет]. GitHub. [цит. за 04, Лютий 2023]. Доступний у: https://github.com/

14.Self-proclaimed bitcoin inventor's $2.5 bln lawsuit can go to trial—London court | Reuters [Інтернет]. [цит. за 08, Лютий 2023]. Доступний у: https://www.reuters.com/legal/self-proclaimed-bitcoin-inventors-25-bln-lawsuit-can-go-trial-london-court-2023-02-03/

15.Summary: Blockchain, The Rise of Trustless Trust? Kevin Werbach, University of Pennsylvania, 2019 [Інтернет]. [цит. за 22, Лютий 2023]. Доступний у: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1002&context=pennwhartonppi_bschool

16.Принципы работы и особенности применения atomic swap [Інтернет]. Хабр. [цит. за 22, Лютий 2023]. Доступний у: https://habr.com/ru/company/distributedlab/blog/417337/

17.Введение в смарт-контракты [Інтернет]. Хабр. [цит. за 22, Лютий 2023]. Доступний у: https://habr.com/ru/company/distributedlab/blog/413231/

Gondek C. What is a Blockchain Security Audit? [Інтернет]. [цит. за 22, Лютий 2023]. Доступний у: https://originstamp.com/blog/what-is-a-blockchain-security-audit/

Стаття надійшла до редакції 11.04.2023
Стаття рекомендована до друку 15.05.2023

M. L. RAFALSKYI
PhD student, Faculty of Law,
Lawyer
E-mail: maksimrafalskiy@gmail.com ORCID: https://orcid.org/0000-0001-9016-8613
The Academy of Advocacy of Ukraine
Kyiv, 01032, Tarasa Shevchenka boulevard, 27

METHODS OF COMBATING OFFENSES IN DECENTRALIZED SYSTEMS

ANNOTATION. *Introduction.* This article is devoted to the study of methods of combating offenses in decentralized systems, in particular in blockchain networks. The author analyzes the main approaches to combating such offenses and considers various methods that can be used to prevent, identify and solve the specified problems. The article examines the potential risks and challenges associated with fighting crime in decentralized systems, and highlights the advantages and disadvantages of different approaches.

Summary of the main results of the study. An explanation of the peculiarities and complexity of organizing the work of decentralized networks such as blockchain, and, accordingly, the complexity of detecting and countering offenses in such networks is provided. Clarification is also provided regarding various approaches and methods of combating offenses in decentralized systems, as well as what methods there are for combating such offenses, and what methods the author of the article proposes.

Conclusions. For the first time, a list of the main methods with offenses in decentralized networks such as blockchain has been unified and provided in the context of criminal law. Methods of combating and preventing such offenses from the point of view of various approaches, including legal, technical, organizational, etc., are also considered. Overall, the article offers conclusions on different approaches to preventing and countering crimes in decentralized systems, reviews different methods of combating such crimes, and emphasizes the need for further research in this area.

KEYWORDS: *decentralized networks, blockchain, cyber security, attacks, criminal law.*

REFERENCES

1.What Does Proof-of-Stake (PoS) Mean in Crypto? [Internet]. Investopedia. [cited for 21, February 2023]. Available at: https://www.investopedia.com/terms/p/proof-stake-pos.asp

2.Synchronization of wallets with the Bitcoin network [Internet]. Habr [cited for 21, February 2023]. Available at: https://habr.com/ru/company/distributedlab/blog/416469// (in Ukrainian)

3.What Is a Merkle Tree & What Is Its Role in Blockchain? [Internet]. Bybit Learn. 2022 [cited for 30, January 2023]. Available at: https://learn.bybit.com/blockchain/what-is-merkle-tree/

4.Federated Sidechains | XRPL.org [Internet]. [cited for 30, January 2023]. Available at: https://xrpl.org/federated-sidechains.html

5.Shinobi. Federated Sidechains Are Bitcoin's Original Upgradeable Sidechain Implementation [Internet]. Bitcoin Magazine - Bitcoin News, Articles and Expert Insights. [cited for 21, February 2023]. Available at: https://bitcoinmagazine.com/technical/federated-sidechains-bitcoin-original

6.Overview of current consensus-building protocols in a decentralized environment [Internet]. Habr [cited for 21, February 2023]. Available at: https://habr.com/ru/company/distributedlab/blog/419185/(in Ukrainian)

7.Zero-knowledge proofs | ethereum.org [Internet]. [cited for 22, February 2023]. Available at: https://ethereum.org/en/zero-knowledge-proofs/

8.Theory of games in cryptocurrencies [Internet]. Decimal. 2022 [cited for 22, February 2023]. Available at: https://decimalchain.com/blog/ru/teoriya-igr-v-kriptovalyutax/ (in Ukrainian)

9.Becker M, Bodó B. Trust in blockchain-based systems. Internet Policy Review [Internet]. 20, April 2021 [cited for 30, January 2023]; 10(2). Available at: https://policyreview.info/glossary/trust-blockchain

10.How multi-signature works in Bitcoin [Internet]. Habr [cited for 22, February 2023]. Available at: https://habr.com/ru/company/distributedlab/blog/415757/ (in Ukrainian)

11.Up to US$400 Million Reward for Return of Stolen 2016 Bitcoin [Internet]. [cited for 04, February 2023]. Available at: https://www.bitfinex.com/posts/494

12.Coincapture. 7 Best Blockchain DNS For 2022 [Internet]. Medium. 2022 [cit. for 22, February 2023]. Available at: https://medium.com/coinscapture/7-best-blockchain-dns-for-2022-d9645cb80560

13. GitHub: Let's build from here [Internet]. GitHub. [cited for 04, February 2023]. Available at: https://github.com/

14. Self-proclaimed bitcoin inventor's $2.5 bln lawsuit can go to trial—London court | Reuters [Internet]. [cited for 08, February 2023]. Available at: https://www.reuters.com/legal/self-proclaimed-bitcoin-inventors-25-bln-lawsuit-can-go-trial-london-court-2023-02-03/

15.Summary: Blockchain, The Rise of Trustless Trust? Kevin Werbach, University of Pennsylvania, 2019 [Internet]. [cited for 22, February 2023]. Available at: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1002&context=pennwhartonppi_bschool

16.Principles of operation and features of the use of atomic swap [Internet]. Habr. [cited for 22, February 2023]. Available from: https://habr.com/ru/company/distributedlab/blog/417337/ (in Ukrainian)

17.Introduction to smart contracts [Internet]. Habr. [cited for 22, February 2023]. Available from: https://habr.com/ru/company/distributedlab/blog/413231/(in Ukrainian)

18.Gondek C. What is a Blockchain Security Audit? [Internet]. [cited for 22, February 2023]. Available from: https://originstamp.com/blog/what-is-a-blockchain-security-audit/

The article was received by the editors 11.04.2023
The article is recommended for printing 15.05.2023