УДК 347.73:336.22
DOI https://doi.org/10.32782/yuv.v4.2023.28

М. Рафальський,
аспірант кафедри кримінального та адміністративного права
Академії адвокатури України

ПРАВОПОРУШЕННЯ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

Вступ. Проблема правопорушень в децентралізованих мережах, таких як блокчейн, є дуже актуальною в сучасному світі. Зростання популярності блокчейн-технологій та інших децентралізованих мереж призводить до збільшення кількості правопорушень, що відбуваються в цих мережах. Вивчення проблематики таких правопорушень має значення як для практичних застосувань, так і для наукових досліджень. Ця проблема має важливі наслідки для реалізації практичних застосувань блокчейнів у різних галузях, включаючи фінанси, логістику, медицину та інші. Врахочуючи, що децентралізовані мережі є новою технологією, яка ще не повністю зрозуміла та розроблена, це призводить до того, що методи виявлення та розслідування правопорушень в децентралізованих мережах все ще розвиваються та поки що не є настільки ефективними, як традиційні методи виявлення правопорушень. Відсутність ефективної системи виявлення, розслідування та попередження таких правопорушень може призвести до недовіри до децентралізованих мереж, включаючи блокчейни, як інструментів для збереження та передачі цінності. Вирішення цієї проблеми наразі тільки стає предметом наукових досліджень з різних галузей, включаючи право, інформаційну безпеку, криптографію та інші. Дослідження в галузі правопорушень у децентралізованих системах можуть допомогти у вирішенні різних питань, пов'язаних з розробкою ефективних методів виявлення, розслідування та попередження правопорушень у таких системах. Також, ця проблема є важливим стимулом для розвитку нових технологій, що дозволять зменшити можливість правопорушень в децентралізованих системах.

Мета дослідження. Огляд основних видів правопорушень в децентралізованих мережах важливий з кількох причин. По-перше, він допоможе зрозуміти різноманітність можливих способів порушення правил в таких мережах, що може сприяти розробці ефективних стратегій для їх запобігання, виявлення та боротьби з ними. По-друге, огляд правопорушень може допомогти зрозуміти загальну структуру та ризики децентралізованих мереж, що може бути корисним для практикуючих в цій сфері правників, правоохоронних органів. Крім того, здійснення такого огляду може сприяти розумінню технічних аспектів децентралізованих мереж, що може бути корисним для нетехнічних фахівців та дослідників, які працюють в цій галузі.

Аналіз останніх досліджень і публікацій. Щодо праць з даної проблематики, то у вітчизняній юридичній літературі саме щодо правопорушень 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, Іванюк В.Д., 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. Децентралізована система – це система, в якій різні частини мережі (наприклад, комп'ютери, вузли) працюють разом, щоб забезпечити безпеку та ефективність мережі без централізованого управління. У децентралізованих системах можуть відбуватись правопорушення, так само, як і в будь-якій іншій системі, проте, із своїми специфічними особливостями. У цих системах можливі різні види правопорушень, включаючи шахрайство та різні види атак. Тому для об'єктивного огляду цієї частини правопорушень необхідно розглянути всі виміри тих умов, в яких скоюються вказані правопорушення. Зазначемо загальний механізм здійснення транзакцій на прикладі блокчейну мережі Бійткоїн, щоб було зрозуміло, на якій «цифровій території» відбуваються ті чи інші прапопорушення.

Якщо загалом, то блокчейн складається з наборів даних, структура яких складається з ланцюжка пакетів даних (блоків), і кожен блок містить велику кількість транзакцій (ТХ1-n). Цей блокчейн розширюється шляхом додавання кожного нового блоку та представлення повного запису історії транзакцій. Перевірка блоку виконується криптографією [1, ст. 393]. Оскільки кілька людей можуть створювати блоки одночасно, може бути кілька варіантів на вибір, як мережа вирішує питання щодо того, що має бути наступним. Не можна просто покладатися на порядок надходження блоків, оскільки, в транзакціях вони можуть надходити в різному порядку в різні точки мережі. Частина рішення Біткоїн полягає в тому, що кожен блок повинен містити відповідь на дуже особливу математичну задачу. Комп'ютери запускають весь текст блоку плюс додаткове випадкове припущення за допомогою криптографічного хеша, доки результат не стане нижче певного значення. Хеш-функція створює короткий дайджест із будь-якої довжини тексту. Вихід абсолютно непередбачуваний, тому єдиний спосіб знайти конкретне вихідне значення – це зробити випадкові припущення. Це дуже схоже на вгадування комбінації замка. Може пощастити з першою здогадкою, але в середньому потрібно багато спроб. Той, хто першим розв'яже математичну задачу, транслює свій блок і приймає свою групу транзакцій як наступну в ланцюжку. Випадковість, що двоє користувачів розв'яжуть вказану математичну задачу одночасно, є малоймовірною, і той, хто першим розв'язав вказану задачу, передає свій блок, і його група транзакцій приймається як наступна в ланцюжку. Загальне правило полягає в тому, що новий блок завжди відразу переходить до найдовшої доступної гілки. Кінцевим результатом є те, що ланцюжок блоків швидко стабілізується, що означає, що всі погоджуються щодо порядку блоків [2].

Як взагалі влаштовані децентралізованої системи: є основні правила, за якими виконується облік, наприклад, облік фінансів, і існують вузли, які дотримуються цих правил, і за жодних обставин не збираються їх порушити. Також можуть бути зловмисні вузли, які можуть змінити своє програмне забезпечення або здійснити інші дії, та оперувати фінансами вже інакше. Система Біткоїн впорядковує транзакції, розміщуючи їх у групах, які називаються блоками, і з'єднує ці блоки разом у ланцюжок блоків.

Зауважемо, що це відрізняється від ланцюжка транзакцій. Ланцюжок блоків використовується для замовлення транзакцій, тоді як ланцюжок транзакцій відстежує, як змінюється право власності. Кожен блок має посилання на попередній блок, що дає можливість розмістити один блок за іншим у часі. Можна відслідкувати за такими посиланнями історію аж до першої групи транзакцій. Транзакції в одному блоці вважаються такими, що відбулися в один і той же час, а транзакції, які ще не входять до блоку, називаються непідтвердженими або неупорядкованими. Будь-який вузол може зібрати налаштовані непідтверджені транзакції в блок і передати його решті в мережу як пропозицію щодо того, яким має бути наступний блок у ланцюжку [2]. У контексті часу підтвердження транзакцій Bitcoin, він становить приблизно 10-20 хвилин для транзакцій з невеликими сумами та близько години для переказів істотних кількостей монет. Втім, варто зауважити, що ці показники визначає не відправник чи система, а сам одержувач для того, щоб переконатися в успішному отриманні платежу. Оскільки відсутній центральний орган чи суд, який би визначав, чи був платіж проведений чи ні або на якому етапі він знаходиться, відповідальність за підтвердження в цьому випадку покладається на одержувача.

Отже, визначимо, які види правопорушень існують в розподілених децентралізованих системах таких як блокчейн, та які передумови склалися для появлення таких правопорушень. В блокчейні Біткоїн замість права власності на баланс кошти перевіряються через посилання на попередні транзакції. Наприклад, щоб надіслати п'ять біткоїнів користувачу-2, користувач-1 повинен вказати інші транзакції, з яких він отримав певну кількість біткоїнів. Ці довідкові транзакції називаються входами. Інші вузли, які перевіряють цю транзакцію, перевірять ці вхідні дані, щоб переконатися, що користувач-1 справді був одержувачем, а також, що введені дані становлять до п'яти або більше біткоїнів. Надсилання грошей у біткоїнах більше схоже на те, щоб покласти гроші в публічну шафу й прикріпити математичний пазл, який потрібно розгадати, щоб відкрити його. Головоломка визначається за допомогою спеціальної мови сценаріїв і, як правило, розроблена таким чином, що лише один власник іншого відкритого ключа міг її вирішити. Можливі більш складні умови, наприклад, два з трьох підписів можуть знадобитися для здійснення транзакції [2]. Може виявитися що деякі монети намагаються бути витраченими двічі, і верифікація цього вимагає певного процесу для того щоб перевірити, що конкретна монета не намагається бути витраченою більше одного разу. Існує окрема база даних, яку веде кожен вузол мережі Біткоїну, і вона зберігає поточний стан усіх не витрачених виходів транзакцій, тобто серед усіх транзакцій які існують, є безліч виходів, певні з них вже були витрачені, інші ні, і ті які не витрачені, зберігаються окремо. Копії бази або її частини одночасно зберігаються на багатьох комп'ютерах і синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація в блоках не шифрована і доступна у відкритому вигляді, але відсутність змін засвідчується криптографічно через хеш-ланцюжки. Щоб мати змогу обробляти велику кількість блоків за адекватний час, у блокчейн системах використовують дерево Меркла у якості структури збереження даних [3, ст. 20]. Правила Біткоїну вимагають свого роду пароль для розблокування невитрачених коштів, і цей пароль називається цифровим підписом. Відкриті ключі насправді є відправкою на адресу в біткоїнах, тому, коли користувач надсилає комусь гроші, він дійсно надсилає їх на відкритий ключ іншої

особи, і щоб витрачати гроші, користувач повинен довести, що він справжній власник адреси відкритого ключа, куди було надіслано гроші і він робить це, генеруючи цифровий підпис із повідомленням транзакції та його приватного ключа, інші вузли в мережі можуть використовувати цей підпис в іншій функції, щоб перевірити, чи він відповідає його відкритому ключу, за допомогою математики, яка стоїть за цифровим підписом [2]. Транзакції, ініційовані кінцевими користувачами, також перевіряються цими вузлами. Насправді транзакція не відразу додається до блокчейну. Вона додається до блокчейну лише після того, як вузол створив блок, використовуючи значні обчислювальні потужності. В обмін на це вузол винагороджується цифровою валютою. Крім того, транзакції передаються через мережу в реальному часі, тобто кожен комп'ютер у мережі знає про кожну транзакцію, коли вона відбувається. Якщо якийсь зловмисник спробує повідомити фальшиву транзакцію або подвійно витратити ті самі монети через мережу, вона буде відхилена, оскільки інші вузли зроблять її недійсною [4].

Наявність неоднозначності на кінці ланцюжка має певне значення для безпеки транзакцій. Якщо транзакція користувача потрапить у одну з коротших гілок, вона може втратити свою позицію в ланцюжку блоків блокчейні. Зазвичай це призводить до того, що транзакція повертається до пулу непідтверджених транзакцій та буде додана до наступного блоку. Однак така можливість для транзакцій втратити своє місце створює умови для атаки подвійних витрат. Хоча й малоймовірно, що зловмисник зможе вирішити кілька блоків поспіль швидше, ніж інші учасники мережі, це все ж можливо, і ймовірність цього зростає зі збільшенням обчислювальної потужності зловмисника відносно загальної потужності мережі. Насправді, таке може статися для пулів майнерів, які складаються з кількох тисяч комп'ютерів, задіяних у майнінгу та створенні нових блоків транзакцій [2].

Самою відомою атакою в мережі блокчейн є так звана «атака 51%». Д. Ковальчук, Т. Івко, Т. Кузнєцова, О. Наріжний в цій частині вказують, що вузли завжди вважають, що найдовший ланцюжок є правильним і продовжують працювати над його розширенням. Якщо два вузли одночасно транслюють різні версії одного блоку, деякі вузли можуть отримати будь-який з них в першу чергу. У цьому випадку вони працюють над блоком, який був отриманий першим, але зберігають і іншу гілку на випадок, якщо вона стане довшою. При виявленні наступного підтвердження роботи, зв'язок буде розірвано, так як одна гілка стане довшою, а вузли, які «працювали» в іншій гілці, переключаться на довшу гілку. Загроза централізації обчислювальних потужностей, відома як «атака 51%», вважається однією з ключових уразливостей алгоритму консенсусу Proof of Work (PoW). Це відбувається, коли у атакуючої сторони, в ролі якої може виступати порівняно невелика кількість майнерів, знаходиться контрольний пакет хешрейту – обчислювальної потужності мережі. Причиною даної вразливості є той факт, що майнери можуть одночасно пропонувати мережі вірні хеші – рішення, які дозволяють підтверджувати цілісність даних і додавати в мережу нові блоки. І тут у блокчейні відбувається «розгалуження». Алгоритм консенсусу PoW вважає, що решта майнерів визнає вірною ту гілку, яка має найбільшу кількість блоків, і проголосують за її включення до блокчейну. Таким чином, якщо майнер або сукупність майнерів контролюють більше половини хешрейту, то у нього з'являється можливість додавати свої гілки і тим самим маніпулювати двосторонніми операціями і не підтверджувати нові транзакції. Ця атака може призвести до того,

що недобросовісні майнери можуть відкликати вже проведені фінансові транзакції, що називається подвійною тратою (англ. double-spending). При цьому атакуюча сторона не може змінювати інформацію у вже доданих блоках та генерувати нові криптовалюти [5, ст. 35]. Отже, гіпотетична ситуація: користувач-1 за отриманий товар зобов'язаний сплатити користувачу-2 п'ять біткоїнів. Проте, він може вирішити діяти зловмистно і створити паралельно ще одну транзакцію, де вказані п'ять біткоїнів він сплачує вже користувачу-3. Отже, є дві транзакції, які протиріччять одна одній. І якщо далі генеруються блоки в двох ланцюжках транзакцій, то одні користувачі будуть бачити одну історію транзакцій, а інші іншу. Отже, зловмисник або пул зловмисників, який контролює більшу частину обчислювальних ресурсів (51%), може майнити більш довгий ланцюжок блоків, а згодом разом опублікувати її, і всі користувачі повинні будуть переключитися на вказаний ланцюжок блоків. Навіть, якщо користувач не згодний з таким ланцюжком транзакцій, він повинен все-одно переключитися на нього, так як в правилах Біткоїна вказано, що більш довгий ланцюжок блоків є правильним. Правило, згідно з яким вузли приймають найдовший ланцюжок блоків, дозволяє кожному вузлу в мережі домовитися про те, як виглядає блокчейн, і, отже, узгодити ту саму історію транзакцій [6]. Варто зауважити, що причинами, завдяки яким стало можливим проведення «атаки 51», є як відсутність центрального вузла, як в централізованих системах, коли група осіб, які є пулом майнерів, мають у своєму розпjрядженні більше половини обчислювальної потужності мережі або контрольний пакет хешрейту і можуть маніпулювати мережею (здійснювати транзакції, які конфліктують з іншими, продавати одні й ті самі монети кілька разів, зупиняти підтвердження транзакцій інших користувачів тощо), так і сам механізм такої мережі, який дає змогу проведення такої атаки. Щодо методів боротьби та запобігання таким правопорушенням, то вони можуть бути різні за природою, наприклад, технічні, юридичні тощо.

Так, можемо розглянути технічний підхід до вирішення зазначеного питання у контексті альтернативного сценарію "атаки 51%". Це стосується ситуації, коли частка блоків, створених чесними учасниками мережі, відхиляється. Ці блоки, відомі як «сиротські» блоки (англ. orphan block), генеруються паралельно з основним ланцюжком, і значна частка мережі вирішує не продовжувати цей ланцюжок, внаслідок чого відкидаються відповідні блоки. У разі значного збільшення кількості таких блоків через недостатню синхронізацію мережі, обчислювальні потужності чесних користувачів можуть бути втрачені. Це означає, що для зловмисника може бути достатньо контролювати, наприклад, 20% обчислювальних потужностей замість 50% та спричиняти значні затримки доставки повідомлень в мережі для успішного виконання атак подвійних витрат. У даному контексті розробники пропонують технічне рішення для протидії подібним атакам, а саме – збільшення інтервалу між блоками до 10 хвилин, що обмежує пропускну здатність і дозволяє мережі своєчасно синхронізуватися, знижуючи ймовірність виникнення «сиротських» блоків [7].

Схожими є і інші атаки, де в якості інструменту правопорушення застосовується контрольний пакет хешрейту в мережі блокчейн. Припустимо, що в контексті блокчейну Біткоїн сумарна майнінгова потужність складає 100%, а для блокчейну іншої криптовалюти – 45% відповідно до загальної потужності Біткоїну. Якби обидві мережі використовували ідентичний алгоритм майнінгу для генерування блоків, то в певний час деякі

майнери, що працюють з Біткоїном, могли переключитися на мережу альтернативного блокчейну. В результаті, вони створювали б альтернативний ланцюг блоків, котрий за довжиною перевищував би основний ланцюг іншої криптовалюти, через більш високу обчислювальну потужність майнерів Біткоїну. Швидкість створення ланцюжка прямо пропорційна до потужності, що на нього спрямована. Отже, майнери Біткоїну мали б можливість вчинити таку атаку. В результаті, для Біткоїну та альтернативних криптовалют було розроблено різні алгоритми майнінгу, що демонструє технічний підхід до запобігання правопорушенням у цифровому просторі. Розглянемо інші види атак для розуміння специфіки взаємодії між різними суб'єктами в мережі блокчейн.

Атаки в чек-поінті. Такі атаки відбуваються, коли зловмисники надсилають хибні ланцюжки блоків із альтернативними варіантами стану бази даних, в яких у потерпілого від атаки відсутні кошти на рахунку. Чек-поінт (англ. Check Point) відображає відповідність певної висоти блоку до "коректного" хеш-значення блоку на даній висоті. Зазвичай, це використовується для перевірки правильності блоків, які користувачі завантажують під час початкової синхронізації з мережею. Оскільки певний вузол мережі ще не запущений і не має інформації про конкретну базу даних з відповідними транзакціями, він здійснює завантаження всієї історії транзакцій, щоб переконатися у правильності історії та отримати інформацію про невитрачені монети для подальшої роботи з іншими вузлами мережі. На цьому етапі в блокчейні можуть виникати деякі вразливості, що створюють можливість для атак. Однією з таких атак є спам некоректними ланцюжками версій бази даних від зловмисників. Тобто, під час процесу завантаження ланцюжка блоків, користувачеві можуть нав'язати альтернативні варіанти стану бази даних, в яких цей користувач не має монет, але зловмисник має. Також, зловмисник може із запізненням опублікувати недоступні блоки та переконати користувача вивести блоки з верхнього (атакуючого) ланцюжка блоків, спричинивши порушення безпеки [8, ст. 2]. Додатково зазначемо, що вказаний альтернативний ланцюжок теж побудований за правилами протоколу блокчейн, програмне забезпечення вказаного користувача відображатиме, що все коректно, але при цьому він втратить свої кошти. Існує інший сценарій таких атак, коли під час завантаження стану бази даних, вузол користувача опиняється ізольованим від решти чесних вузлів мережі. В результаті, зазначений вузол не має змоги отримати відомий і вже давно підтверджений коректний стан мережі Біткоїн. Натомість вузол користувача отримує альтернативний ланцюжок блоків, який надсилають зловмисники.

Атаки посередників (англ. «Man in the middle»). Сутність цієї атаки полягає в потенційній вразливості системи, що виникає внаслідок використання довірених вузлів мережі Біткоїн з метою спрощення функціонування криптогаманця та уникнення завантаження повного вузла та зберігання інтегральної копії блокчейна. Довірений вузол є стандартним вузлом мережі Біткоїн, якому користувачі довіряють перевірку своїх транзакцій. Зазвичай, такі довірені вузли використовуються різними криптогаманцями, що надаються компаніями-постачальниками криптовалютних гаманців. У даному контексті, користувачам необхідно довіряти компанії-постачальнику криптовалютного гаманця щодо правильності перевірки транзакцій на довірених вузлах. Втім, такий підхід призводить до значної залежності гаманця від довіреного вузла мережі, через що користувачі можуть стати жертвами атаки "Man in the middle". Під час цієї атаки, зло-

вмисник може перехоплювати повідомлення користувача та підміняти їх таким чином, щоб надсилати користувачам хибні дані [9].

Також існують атаки через зміни даних у транзакціях. У Біткоїні через особливості побудови транзакцій є можливість змінити певні дані транзакцій, при цьому залишаючи цю транзакцію цілком правильною. Кошти будуть йти з тієї ж адреси, з якої вони йшли, на ту ж адресу, на яку вони йшли до цього, але при цьому зміниться хеш транзакції, відповідно, це вже буде зовсім інша транзакція, хоча робить вона те саме, що й оригінальна. Існують різні види таких атак:

1) зміна формату підпису: третя сторона може перехопити транзакцію, трохи змінити дані, так щоб підпис залишався валідним, але при цьому хеш транзакції вже зміниться, і відповідно це буде зовсім інша транзакція.

2) атака на scriptSig, яка є набором інструкцій, дозволяючим користувачам підтвердити володіння монетами, полягає в тому, що зловмисники додають додаткові операції, які не мають значення та не впливають на підпис. Проте, додавання нових даних до транзакції призводить до зміни її хешу. В результаті, зловмисники мають змогу створити альтернативну версію транзакції, ідентичну оригіналу, але з іншим хешем. Ця альтернативна транзакція конкурує з оригіналом, заважаючи останньому потрапити до блокчейну. Якщо зловмисники змінюють хеш хоча б однієї транзакції в ланцюжку, усі наступні транзакції стають невалідними. Важливо відзначити, що хеш транзакцій можна змінити без доступу до приватних ключів, що робить цю проблему серйозною для безпеки блокчейну [10].

Грандінг атаки (англ. grinding attacks). Конкретний користувач може перебрати різні варіанти блоків, різні варіанти випадковостей, для того, щоб сформувати той самий ланцюжок, коли він може неправомірно максимізувати свій прибуток. Як вказав лектор Стендфордського університету David Tse «Іншими словами, зловмисник може спробувати зіграти з даними в лотерею, щоб отримати несправедливу перевагу над чесним вузлом» [11].

Лайвнесс атаки (англ. liveness attack). Атака Liveness – це атака, яка може максимально затримати час підтвердження цільової транзакції [12]. Потенційна загроза полягає у можливості непотрапляння нових транзакцій до реєстру транзакцій, особливо при значних затримках у мережі або у випадку, коли зловмисник має змогу видаляти повідомлення, що йому потрібні. У такому сценарії зловмисник не зможе анулювати вже існуючі транзакції, однак він зможе завадити додаванню нових транзакцій до реєстру.

Атаки на DHT. Розподілена хеш-таблиця (англ. Distributed hash table, DHT) – це децентралізована система зберігання, яка забезпечує схеми пошуку та зберігання, подібні до хеш-таблиці, зберігаючи пари ключ-значення. Кожен вузол у DHT відповідає за ключі разом із зіставленими значеннями. Будь-який вузол може ефективно отримати значення, пов'язане з заданим ключем [13]. Найбільш ефективний метод атаки на протокол DHT полягає в тому, що зловмисник може суттєво ускладнити доступ до певного контенту. Для досягнення цього зловмиснику потрібно розгорнути десятки або навіть сотні спеціально модифікованих вузлів. У результаті значна кількість фальшивих учасників оточує цільовий контент, і до них звертаються майже всі користувачі, що шукають зазначений контент. Таким чином, можна тимчасово обмежити доступ до окремого контенту.

Крім атак, є також шахрайство, наприклад, за допомогою маніпуляцій із міткою часу в блокчені та різниці

в часі. Перевіряючи цифровий підпис, відомо, що лише справжній власник міг створити повідомлення про транзакцію. Щоб переконатися, що у відправника дійсно є кошти, можна перевірити кожну довідкову транзакцію, щоб впевнитися, що вона невитрачена. Але в системі все ще є одна велика «діра» в безпеці, і це пов'язано з порядком транзакцій. Враховуючи, що транзакції передаються вузол за вузлом через мережу, немає гарантії, що порядок, у якому користувач їх отримує, відповідає порядку, у якому вони були створені. Крім того, мітка часу теж ненадійна, оскільки зловмисник легко може ввести в оману про час створення транзакції. Тому немає способу визначити, чи одна транзакція відбулася раніше іншої, і це відкриває потенціал для шахрайства. Зловмисний користувач-1 може надіслати транзакцію, надаючи кошти користувачу-2, дочекатися, поки користувач-2 відправить товар в обмін на вказані кошти, а потім надіслати іншу транзакцію, посилаючись на ті самі дані, собі. Через різницю в часі розповсюдження деякі вузли в мережі отримають другу транзакцію подвійних витрат перед транзакцією для користувача-2, і коли транзакція користувача-2 надійде, вона вважатиметься недійсною, оскільки вона намагається повторно використати вхідні дані. Таким чином, користувач-2 втратить і відвантажений товар, і свої гроші. Врешті решт, виникають розбіжності в мережі щодо того, кому мають належати кошти, оскільки неможливо довести, яка транзакція відбулася першою [2].

Також правопорушеннями можуть бути дії валідаторів. Валідатор – це вузол, який має право обробляти операції учасників мережі, створювати нові блоки та додавати їх до блокчейну. Валідатори отримують операції, які хочуть здійснити учасники мережі. Зазвичай валідатори замінюють роль майнерів у блокчейн-мережі Proof of Work (PoW) і отримують стимул діяти чесно в системі, оскільки їх частка заблокована в мережі, поки вони виконують своє завдання. Вони отримують винагороду у вигляді рідного токена мережі за автентичну перевірку, а їхні ставки знижуються, якщо вони діють зловмисно [14]. Проте деякі вразливості все ж таки залишаються. Протокол вибирає випадкового валідатора, щоб він запакував усі отримані операції в блок і додав його до своєї копії блокчейну. Інші валідатори та вузли (ноди) перевіряють блок на можливі помилки, а потім додають його у свої копії блокчейну. Коли більшість вузлів записують новий блок у свою копію блокчейну, операції в ньому вважаються виконаними та необоротними. Виникає питання стосовно порядку формування блоків валідаторами та методу вирішення цього питання. Перш за все, розглядаються деякі вимоги для вирішення цього питання. Основна вимога полягає в тому, що порядок формування блоків має обчислюватися незалежно, без контролю централізованої структури, оскільки це неприпустимо в децентралізованій мережі. Додаткова вимога полягає в тому, що кожний вузол має самостійно визначати порядок, не довіряючи іншим учасникам, і порядок у всіх учасників має бути ідентичним після обчислення. Отже, кожен вузол самостійно розраховує порядок і отримує такий же результат, як і інші учасники. У цьому контексті існують потенційні вразливості, які полягають у можливості змови між валідаторами з метою генерування певної послідовності блоків для впровадження неправомірних дій.

Щодо змови, вона може бути і серед валідаторів в консенсусі Delegated Proof of Stake (DPoS). Щодо змови, вона може бути і серед валідаторів в консенсусі Delegated Proof of Stake (DPoS). У порівнянні з іншими консенсусними механізмами Proof of Stake (PoS), DPoS відрізняється тим, що активніше залучає більшу частку

криптовалюти у процесі досягнення консенсусу. Однак існують користувачі, які з певних причин не беруть активної участі у голосуванні або прийнятті рішень, хоча мають достатній обсяг криптовалюти для цього. Такі обставини можуть створювати ситуації, коли певна підмножина користувачів контролює значну частину голосувальної потужності при створенні блоків. Ця підмножина користувачів може опинитися під впливом зовнішніх чинників, вступити у змову або здійснювати інші недобросовісні дії.

Також шахрайство може відбуватись в оффчейн каналах (англ. Off-chain payment channels). On-chain транзакції відбуваються всередині мережі блокчейну, перевіряються майнерами та записуються в блокчейн. Як тільки транзакції додаються до реєстру, мережа блокчейна оновлюється, і всі дані розподіляються між вузлами. Але враховуючи великі комісії та великий час обробки, транзакції можуть відбуватися і поза блокчейном (off-chain), щоб зменшити навантаження на мережу. Користувачі можуть відкрити канал і обмінюватися приватними ключами гаманців, таким чином можна здійснювати переказ коштів поза блокчейном. Поки канал активний, можна продовжувати обмінювати криптовалюту необмежену кількість часу. Коли користувачі будуть готові завершити угоду, вони закривають канал, і інформація про остаточний розрахунок заноситься до блокчейну. Існує безліч off-chain протоколів, у тому числі Lightning Network, Liquid Network і багато інших [16]. Ситуація, яка створює ризик шахрайства: в рамках відкритого каналу клієнт створює транзакцію, наприклад, номер 3, в якій кошти розподіляються між одержувачами. Сервіс перевіряє відповідність транзакції та підпису, а також приймає платіж. Якщо сервіс планує продовжувати обслуговування клієнта та отримувати оплату в рамках каналу, він зберігає транзакцію номер 3 локально до моменту закриття каналу. Для надсилання всіх подальших платежів клієнт модифікує вихідні дані транзакції номер 3, перепідписує її і передає сервісу лише сам підпис і суму змін. Сервіс перевіряє отримані дані та зберігає оновлену версію транзакції номер 3, оскільки в цій версії він отримує більший обсяг криптовалюти. Закриття каналу також проводиться відповідно. Сервіс має опублікувати останню версію транзакції номер 3 у блокчейні до закінчення терміну дії каналу, інакше відправник може спробувати вчинити шахрайство, допідписавши та оприлюднивши іншу транзакцію, наприклад, номер 2, в якій він забере всю суму на свою адресу.

Атаки, які відбуваються в блокчейні, в якому використовується метод або підхід перевірки транзакцій, який називається Концепція спрощеної верифікації платежів (англ. Simplified Payment Verification (SPV)). Концепція спрощеної верифікації платежів була висвітлена ще в Bitcoin whitepaper [17], опублікованому розробником даної криптовалюти – Сатоші Накамото. Проте, разом із багатьма перевагами данного підходу, використання SPV у мережі повного вузла має недоліки, особливо ті, що стосуються безпеки мережі та даних. Докази SPV більш сприйнятливі до атак 51% і можуть використовуватися для підтвердження фальсифікованих даних транзакцій [18].

Існують і інші атаки в децентралізованих мережах блокчейн, які часто мають свої аналоги в відкритих мережах, де в тому числі діють централізовані криптобіржі, які теж підлягають атакам. Наприклад, Спуфінг ARP (англ. ARP-spoofing) – це тип атаки «Man in the middle», яка дозволяє зловмисникам перехоплювати зв'язок між мережевими пристроями [19]. Орієнтована на використання у локальних мережах, побудованих на комутаторах. Використовує надсилання підроблених ARP-відпові-

дей. Дозволяє зловмиснику направити трафік жертви через себе, далі переглядає та модифікує його. Застосовується також з криптогаманцями. Деяки атаки в цій частині можливі також через вразливість серверу DHCP, який дозволяє зловмиснику направити трафік жертви через себе (Man-in-the-middle), переглядаючи його, і за необхідності також модифікуючи [20].

За результатами проведеного дослідження можна стверджувати, що в децентралізованих мережах, таких як блокчейн, існує значний ризик правопорушень. Блокчейн, як і будь-яка інша технологія, не є повністю невразливим до правопорушень. Хоча блокчейн відомий своєю безпекою і стійкістю до змін, існують деякі сценарії, коли можливі правопорушення, наприклад, здійснення різних атак. Дана стаття детально описує основні види таких правопорушень та їх приклади. Проведене дослідження показало, що найбільші ризики пов'язані з різними атаками на цілісність та доступність коштів та інформації третіх осіб. Крім атак та шахрайства в самих децентралізованих мережах, існують правопорушення поза ними, але із застосуванням таких мереж. Наприклад, введення в оману власника приватного ключа за допомогою соціальної інженерії через електронну пошту або соціальні мережі, заволодіння таких ключем, і вже за допомогою такого приватного ключа здійснюється викрадення криптовалюти. Для зменшення ризику правопорушень в децентралізованих мережах необхідно розробляти та використовувати відповідні технічні, юридичні та організаційні заходи безпеки, а також регулювати юридичний аспект використання таких мереж. Дана стаття може бути корисною для фахівців з кримінального права, які займаються науковою та практичною діяльністю в сфері децентралізованих мереж, а також для розробників технічних засобів та алгоритмів, що забезпечують безпеку в мережах блокчейн. Отже, проблема правопорушень у децентралізованих системах є важливою для практичних застосувань, наукових досліджень та розвитку нових технологій. Розв'язання цієї проблеми може внести вагомий внесок у забезпечення ефективної та безпечної роботи децентралізованих систем таких як блокчейн.

Статтю присвячено дослідженню проблеми правопорушень в децентралізованих системах, зокрема в мережах блокчейн. Автор аналізує основні види правопорушень, які можуть виникнути в цих системах, такі як шахрайство, різноманітні атаки та інші. Оскільки децентралізовані мережі не мають централізованого контролю, вони стають більш вразливими до різних видів атак та зловживань. Розуміння природи децентралізованих мереж може допомогти вирішити проблему правопорушень в цих системах більш ефективно, а розуміння принципів вказаних мереж може допомогти розробити ефективні та прозорі методи вирішення таких правопорушень.Зважаючи на результати проведеного дослідження,надано роз'яснення як влаштовані децентралізовані мережі такі як блокчейн, які є правопорушення в таких мережах, що таке атаки в децентралізованих системах. Також надано детальний перелік основних видів атак, інших видів правопорушень та зловживань в децентралізованих системах, до кожного виду надано опис та роз'яснення, до деяких надані також конкретні приклади.Зроблено висновок, що в децентралізованих мережах, таких як блокчейн, існує значний ризик правопорушень. Блокчейн, як і будь-яка інша технологія, не є повністю невразливим до правопорушень. Хоча блокчейн відомий своєю безпекою і стійкістю до змін, існують деякі сцена-

рії, коли можливі правопорушення, наприклад, здійснення різних атак. Дана стаття детально описує основні види таких правопорушень та їх приклади. Проведене дослідження показало, що найбільші ризики пов'язані з різними атаками на цілісність та доступність коштів та інформації третіх осіб. Крім атак та шахрайства в самих децентралізованих мережах, існують правопорушення поза ними, але із застосуванням таких мереж. Наприклад, введення в оману власника приватного ключа за допомогою соціальної інженерії через електронну пошту або соціальні мережі, заволодіння таких ключем, і вже за допомогою такого приватного ключа здійснюється викрадення криптовалюти. Для зменшення ризику правопорушень в децентралізованих мережах необхідно розробляти та використовувати відповідні технічні, юридичні та організаційні заходи безпеки, а також регулювати юридичний аспект використання таких мереж.

Ключові слова: децентралізовані мережі, блокчейн, кібербезпека, атаки, кримінальне право.

Rafalskyi M. Offenses in decentralized systems

The article is devoted to the study of the problem of offenses in decentralized systems, in particular in blockchain networks. The author analyzes the main types of offenses that can occur in these systems, such as fraud, various attacks, and others. Since decentralized networks have no centralized control, they become more vulnerable to various types of attacks and abuses. Understanding the nature of decentralized networks can help to solve the problem of crimes in these systems more effectively, and understanding the principles of these networks can help to develop effective and transparent methods of solving such crimes.Taking into account the results of the research, an explanation is provided as to how decentralized networks such as blockchain are organized, what are the offenses in such networks, what are attacks in decentralized systems. A detailed list of the main types of attacks, other types of offenses and abuses in decentralized systems is also provided, a description and explanation is provided for each type, and specific examples are also provided for some of them. It is concluded that there is a significant risk of wrongdoing in decentralized networks such as blockchain. Blockchain, like any other technology, is not completely invulnerable to wrongdoing. Although the blockchain is known for its security and resistance to change, there are some scenarios where offenses are possible, such as various attacks. This article describes in detail the main types of such offenses and their examples. The conducted research showed that the greatest risks are associated with various attacks on the integrity and availability of funds and information of third parties. In addition to attacks and fraud in the decentralized networks themselves, there are crimes outside them, but with the use of such networks. For example, misleading the owner of a private key with the help of social engineering through e-mail or social networks, taking possession of such a key, and using such a private key to steal cryptocurrency. To reduce the risk of offenses in decentralized networks, it is necessary to develop and use appropriate technical, legal and organizational security measures, as well as to regulate the legal aspect of the use of such networks.

Key words: decentralized networks, blockchain, cyber security, attacks, criminal law.

Література

1. BLOCKCHAIN TECHNOLOGY ON THE DEMOCRATIC CHOICE. 2020. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=pnwJInEAAAAJ&citation_for_view=pnwJInEAAAAJ:d1gkVwhDpl0C (date of access: 03.02.2023)

2. Driscoll S. How Bitcoin Works Under the Hood.ImponderableThings (Scott Driscoll's Blog).URL: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html(date of access: 21.02.2023)

3. Черніков М.Ю. Методи захисту транзакцій в блокчейн системах :пояснювальна записка до атестаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 125 – Кібербезпека / М-во освіти та науки України ; Харків. нац. ун-т радіоелектроніки. Харків, 2021. 81 с. URL: https://openarchive.nure.ua/handle/document/19433(date of access: 21.02.2023)

4. Double-Spending Problem and Byzantine General's Problem in Relation to Cryptocurrency. Freeman Law. URL: https://freemanlaw.com/double-spending-problem-and-byzantine-generals-problem-in-relation-to-cryptocurrency-2/ (date of access: 03.02.2023)

5. Kovalchuk D., Ivko T., Kuznetsova T., Nariezhnii O. Огляд протоколів консенсусу, що застосовуються в технологіях блокчейн. CS&CS E-journal. 2019.Issue 1(13). P. 30–43. URL: https://periodicals.karazin.ua/cscs/article/view/13081 (date of access: 03.02.2023)

6. The Longest Chain–Blockchain Guide. URL: https://learnmeabitcoin.com/technical/longest-chain(date of access: 21.02.2023)

7. Кучковський В. В. Алгоритми консенсуса блокчейн-систем. Herald of Khmelnytskyi national university. 2021. Issue 3. P. 30–33. URL: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/08/7-2.pdf (date of access: 21.02.2023)

8. Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities. Ertem Nusret Tas, David Tse, Fangyu Gai, Sreeram Kannan, Mohammad Ali Maddah-Ali, Fisher Yu.URL:https://eprint.iacr.org/search?q=Bitcoin-Enhanced+&title=&authors=&category=&submittedafter=&submittedbefore=&revisedafter=&revisedbefore(date of access: 21.02.2023)

9. Мандела Амуссу. Чому впровадження оновлень мережі біткойн, як-от SegWit і Taproot, є плодом? Securities : [сайт]. URL: https://www.securities.io/uk/%D1%87%D0%BE%D0%BC%D1%83 (date of access: 21.02.2023)

10. Andrushchenko D. Технічні виклики блокчейну. 5 задач, які потребують розв'язання. DOU.ua : [сайт]. URL: https://dou.ua/forums/topic/33464/ (date of access: 21.02.2023)

11. Tse D. Bribery and stake grinding attacks. Scaling Blockchains, Stanford University. 2020. 374 p. URL: https://web.stanford.edu/class/archive/ee/ee374/ee374.1206//downloads/l18_notes.pdf (date of access: 23.01.2023)

12. Liveness–an overview. ScienceDirect. URL: https://www.sciencedirect.com/topics/engineering/liveness(date of access: 23.01.2023)

13. What is a distributed hash table? Educative: Interactive Courses for Software Developers. URL: https://www.educative.io/answers/what-is-a-distributed-hash-table(date of access: 23.01.2023)

14. Thellman P. Validators Create New Attack Vectors for Decentralized Systems. 2019. URL: https://www.coindesk.com/markets/2019/02/24/validators-create-new-attack-vectors-for-decentralized-systems/ (date of access: 23.01.2023)

15. What Is Delegated Proof of Stake? URL: https://crypto.com/university/what-is-dpos-delegated-proof-of-stake(date of access: 21.02.2023)

16. Crypto Off-Chain vs. On-Chain Transactions: What Are They? Bybit Learn. 2021. URL: https://learn.bybit.com/blockchain/off-chain-vs-on-chain-transactions/ (date of access: 29.01.2023)

17. Bitcoin White Paper. URL: https://bitcoinwhitepaper.co/ (date of access: 03.02.2023)

18. What is Simplified Payment Verification (SPV)? Definition & Meaning / Crypto Wiki. BitDegree.org: [сайт]. URL: https://www.bitdegree.org/crypto/learn/crypto-terms/what-is-simplified-payment-verification-spv(date of access: 20.01.2023)

19. What is ARP Spoofing. ARP Cache Poisoning Attack Explained.Imperva. Learning Center. URL: https://www.imperva.com/learn/application-security/arp-spoofing/ (date of access: 23.01.2023)

20. DHCP Starvation Attack. 2022. GeeksforGeeks. URL: https://www.geeksforgeeks.org/dhcp-starvation-attack/ (date of access: 21.02.2023)