https://doi.org/10.26565/2075-1834-2022-34-03
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

ПРАВОПОРУШЕННЯ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

АНОТАЦІЯ. *Вступ.* 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.

Короткий зміст основних результатів дослідження. 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.

Висновки. Вперше уніфіковано та надано перелік основних правопорушень в децентралізованих мережах таких як блокчейн саме в контексті кримінального права.

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

Як цитувати: Рафальський М. Л. Правопорушення в децентралізованих системах. *Вісник Харківського національного університету імені В.Н. Каразіна, серія «Право».* 2022. Вип. 34. С. 26-36. https://doi.org/10.26565/2075-1834-2022-34-03

In cites: Rafalskyi M. L. (2022). Offenses in decentralized systems. *The Journal of V.N. Karazin Kharkiv National University, Series «Law»*, (34), P. 26-36. https://doi.org/10.26565/2075-1834-2022-34-03(in Ukrainian)

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 злочинів. 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 ефективнихметодів

виявлення, розслідування та попередженняправопорушень 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 (TX1-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]. Що стосується часу підтвердження транзакцій Біткоїну, це близько 10-20 хвилин для транзакцій на невеликі суми і близько години для транзакцій, які переводять суттєві суми монет, але знову ж таки ці значення вибирає не відправник і не система, а сам одержувач для того, щоб переконатися що він дійсно отримав цей платіж, тому що не існує ніякого центру, ніякого суду тощо, хто скаже, що платіж був проведений або не був проведений, завершений або перебуває на якійсь стадії.

Отже, визначимо, які види правопорушень існують в розподілених децентралізованих системах таких як блокчейн, та які передумови склалися для появлення таких правопорушень. В блокчейніБіткоїн 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]. Той факт, що в кінці ланцюжка є певна неоднозначність, має дещо важливе значення для безпеки транзакцій. Наприклад, якщо транзакція користувача опиниться в одній із коротших гілок, вона втратить своє місце в ланцюжку блоків. Як правило, це лише означає, що вона повернеться до пулу непідтверджених транзакцій і буде включена до наступного блоку. На жаль, ця можливість для транзакцій втратити своє місце відкриває двері для атаки подвійних витрат. Дуже малоймовірно, що зловмисник вирішить кілька блоків поспіль швидше, ніж решта в мережі, але це можливо, і ймовірність збільшується, оскільки обчислювальна потужність зловмисника зростає пропорційно решті в мережі. Фактично, це реально для пулу майнерів, куди можуть входити кілька тисяч комп'ютерів, які займаються майнінгом і будують нові блоки 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 ProofofWork (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, можна розглянути технічне вирішення вказаного питання на ще одному різновиді «атаки 51». Наприклад, частина блоків, що генеруються чесними користувачами, відкидаються. Це так звані орфанні блоки (англ. orphan block) - це блоки, які згенеровані паралельно з основним ланцюжком, і велика частина мережі вирішила, що цей ланцюжок не варто продовжувати, тому ці блоки відкидаються. Якщо таких блоків стає багато, коли мережа не встигає синхронізуватися, то може відбутися, що частина обчислювальних потужностей мережі чесних користувачів просто марно втрачається. Це означає, що зловмиснику варто боротися не за 50% обчислювальних потужностей, а, наприклад, за 20%, і контролюючи їх з великою затримкою доставки повідомлень в мережі, зловмисник може успішно реалізовувати дабл-спенд атаки. Саме в цьому випадку знайшли технічне рішення боротьби з таким видом атак, а саме – встановити більше часу між блоками – 10 хвилин, що обмежує пропускну спроможність, для того, щоб мережа встигала чітко синхронізуватись і ймовірність появи таких блоків була дуже низькою [7]. Технічні рішення стосуються попереджень таких правопорушень, проте існують і інші види рішень, в тому числі, юридичні, які будуть розглянуті далі.

Схожими є і інші атаки, де в якості інструменту правопорушення застосовується контрольний пакет хешрейту в мережі блокчейн. Припустимо, що в блокчейні біткоїн загальна майнінгова потужність – 100%, а в блокчейні іншої криптовалюти – 45% від загальної потужності біткоїну. Якщо б у них було однакове майнінгове завдання (однаковий алгоритм), щоб згенерувати блок, то в якийсь момент деякі майнери біткоїну могли б переключитися на мережу іншого блокчейну, і в цей момент створити альтернативний ланцюжок, який перевищував би довжину основного ланцюжка цієї іншої криптовалюти, просто тому, що у майнерівБіткоїну більше основної потужності. Тобто, чим більше потужності спрямоване на створення ланцюжка, тим швидше він створюється. Таким чином, майнериБіткоїну могли б здійснити таку атаку. Тому для Біткоїну та для альтернативних криптовалют створили різні алгоритми майнінгу. Ще один приклад технічного вирішення попередження правопорушень.

Розглянемо інші види атак для розуміння специфіки взаємодії між різними суб’єктами в мережі блокчейн.

Атаки в чек-поінті. Коли правопорушники надсилають хибні ланцюжки блоків із альтернативними версіями стану бази даних, в якій у жертви такої атаки коштів на рахунку немає. Чек-поінт (англ. Check Point) – це відповідність деякої висоти блоку «правильному» хеш-значенню блоку, який має бути на цій висоті. Зазвичай використовується для перевірки того, що блоки, які викачують користувачі, є правильними, при початковому виконанні синхронізації з мережею. Тобто, поки мережа не має даного конкретного вузла, він ще не був запущений, і він "не знає" про певну базу даних з певними транзакціями. Коли він запускається, починається викачування всієї історії транзакцій для того, щоб верифікувати, що вся історія правильна і мати уявлення про не витрачені монети, і далі продовжувати працювати з іншими вузлами мережі. На цьому етапі у блокчейні виникають деякі вразливості, через які можливі атаки. Одна з них – це спам неправильними ланцюжками версій бази даних із боку зловмисника. Тобто, у цьому процесі, коли користувач викачує ланцюжок блоків, йому можуть нав’язати альтернативні версії стану бази даних, за якими цей користувач монет не має, а 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. Інший варіант таких атак, коли в процесі викачування стану бази даних вузол користувача виявляється ізольованим від інших чесних вузлів мережі, і вказаний вузол не може отримати те, що

вважається вже давно підтвердженим правильним станом в мережі Біткоїн. Натомість він отримує фактично альтернативний ланцюжок блоків, тільки від зловмисників.

Атаки посередників (англ. «Maninthemiddle»). Суть полягає в тому, що в блокчейні для того, щоб не завантажувати повний вузол і не зберігати повну копію блокчейна на гаманці, і тим самим спростити роботу гаманця, використовується так званий довірений вузол мережі Біткоїн. Це звичайний вузол мережі Біткоїн, але якому користувачі довіряють перевірку своїх транзакцій. Найчастіше такі довірені вузли використовуються в різних криптогаманцях, і використовуються вони в такому вигляді: компанія, яка надає криптовалютний гаманець, має довірені вузли, і вона гарантує, що перевірка транзакцій в них буде правильна. У такому разі користувачеві потрібно просто довіряти компанії-постачальнику крипто-валютного гаманця. Однак такий підхід зумовлює велику залежність гаманця від довіреного вузла мережі, і у разі використання такого підходу користувачі можуть зіткнутися з атакою, яка називається «Manin the middle». Суть цієї атаки в тому, що зловмисник у цьому випадку може перехоплювати повідомлення користувача та підміняти їх таким чином, щоб видавати вказаним користувачам неправильні 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 (набір команд, який дозволяє користувачам довести володіння монетами), коли зловмисники можуть у цьому наборі команд додати кілька операцій, що нічого не значать, які ніяк не впливають на перевірку підпису, але тим не менш оскільки у них додалися нові дані в транзакцію, хеш у транзакції також змінився. Тобто, через таку змінність транзакцій у зловмисників існує можливість створити таку саму транзакцію, як і оригінальна, але вона буде вже фактично інша, тому що в неї інший хеш, і відповідно вона конкуруватиме з попередньою, і таким чином можна зробити так, щоб попередня транзакція ніколи не потрапила до блокчейну. А якщо зловмисники шляхом зміни хеша транзакції зроблять не валідною хоча б одну транзакцію з цього ланцюжка, весь наступний ланцюжок транзакцій також стане не валідним, і при цьому змінити хеш транзакцій можна, навіть не маючи доступу до особистих ключів, відповідно це досить серйозна проблема [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]. Загроза пов’язана з тим, що нові транзакції можуть не потрапляти в сам журнал транзакцій, тобто, якщо в мережі з’являються занадто великі затримки, або зловмисник може викидати повідомлення, які йому необхідні, в цьому випадку зловмисник не зможе скасувати старі транзакції, але може перешкодити включенню нових транзакцій до самого журналу.

Атаки на DHT. Розподілена хеш-таблиця (англ. Distributedhashtable, 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]. Найефективніша атака на протокол DHT у тому, що зловмисник може майже повністю заблокувати один конкретний контент. Для цього йому необхідно запустити десятки чи навіть сотні спеціально модифікованих вузлів. Тоді виходить, що велика кількість фейкових учасників оточує цільовий контент і за рахунок чого до них звертаються практично всі учасники, які шукають цей контент. Таким

чином, доступ до одного конкретного контенту можна тимчасово заблокувати.

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 продукт, 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 необо-ротними. Виникає питання: в якому порядку ці валідатори формуватимуть блоки та як це питання вирішується. По-перше, для вирішення цього питання висуваються певні вимоги. Перша найголовніша вимога – це те, щоб порядок розраховувався незалежно, а не диктувався якоюсь однією централізованою сутністю, бо в децентралізованій мережі це неприпустимо. Далі вимога така, що кожний вузол сам повинен розрахувати цей порядок, тому що він нікому не довіряє, і у всіх фактично повинен цей порядок бути однаковий при цьому розрахунку. Тобто кожен розраховує сам і отримує те ж саме, що й інші. В цьому місці з'являються певні вразливості, коли валідатори можуть увійти в змову та згенерувати певний ряд блоків поспіль, щоб здійснити певну махінацію. Щодо змови, вона може бути і серед валідаторів в консенсусі Delegated Proof of Stake (DPoS). DPoS — це консенсусний механізм, який є різновидом класичного консенсуса PoS. DPoS розвинувся з PoS і дозволяє користувачам мережі голосувати за делегатів, які потім підтверджують блоки [15]. Даний консенсус, порівняно з іншими консенсусами Proof of Stake (PoS), має перевагу, яка проявляється в тому, що більша частина монет бере участь у консенсусі. Це означає, що існує безліч користувачів, які з певних причин не беруть участь у голосуванні/прийняті рішень, хоча для цього вони мають достатню кількість монет. Відповідно, можуть виникати ситуації, в яких певна підмножина користувачів захоплюють більшу частину голосувальної здатності при формуванні блоків, і ця підмножина може потрапити під певний вплив, змовитися тощо.

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, при якій може бути шахрайство: відкритий канал, клієнт формую транзакцію, наприклад, номер 3, з якої монети розподіляються між одержувачами. Сервіс перевіряє правильність транзакції та підпису та приймає платіж. Якщо сервіс має намір далі надавати обслуговування клієнта та отримувати оплату в рамках каналу, він просто зберігає цю транзакцію номер 3 локально до закриття каналу. Для відправки всіх наступних платежів клієнт змінює вихідні значення транзакції номер 3, відповідно передпідписує її і передає сервісу тільки сам підпис і суму зміни. Сервіс також перевіряє отримані дані та зберігає вже нову версію транзакції номер 3, оскільки в цій версії він отримує більше монет. Також виконується закриття каналу. Сервіс повинен встигнути опублікувати в блокчейні останню версію транзакції номер 3 до завершення роботи каналу, в іншому випадку відправник може спробувати ввести в оману, допідписати і оприлюднити вже іншу транзакцію, наприклад, номер два, де 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 крипто-валюти 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 «Manin 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-відповідей. 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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Popovic A, Milijic A. Crypto-democracy: implications of the blockchain technology on the democratic choice. 2020. [cited for 03, February 2023]. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=pnwJInEAAAAJ&citation_for_view=pnwJInEAAAAJ:d1gkVwhDpl0C
2. Driscoll S. How Bitcoin Works Under the Hood [Інтернет]. [цит. за 21, Лютий 2023]. URL: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
3. Черніков М.Ю. Методи захисту транзакцій в блокчейн системах. 2021 [цит. за 21, Лютий 2023]; URL: https://openarchive.nure.ua/handle/document/19433
4. Double-Spending Problem and Byzantine General's Problem in Relation to Cryptocurrency [Інтернет]. Freeman Law. [цит. за 03, Лютий 2023]. URL: https://freemanlaw.com/double-spending-problem-and-byzantine-generals-problem-in-relation-to-cryptocurrency-2/
5. Kovalchuk D, Ivko T, Kuznetsova T, Nariezhnii O. Огляд протоколів консенсусу, що застосовуються в технологіях блокчейн. CS&CS E-journal. 24, Червень 2019;(1):30–43. [цит. за 03, Лютий 2023]. URL: https://periodicals.karazin.ua/cscs/article/view/13081
6. The Longest Chain—Blockchain Guide [Інтернет]. [цит. за 21, Лютий 2023]. URL: https://learnmeabitcoin.com/technical/longest-chain
7. Обзор актуальных протоколов достижения консенсуса в децентрализованной среде [Інтернет]. Хабр. [цит. за 21, Лютий 2023]. URL: https://habr.com/ru/company/distributedlab/blog/419185/
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. [Інтернет]. [цит. за 21, Лютий 2023]. URL: https://eprint.iacr.org/search?q=BitcoinEnhanced+&title=&authors=&category=&submittedafter=&submittedbefore=&revisedafter=&revisedbefore=
9. Синхронизация кошельков с Биткоин сетью [Інтернет]. Хабр. [цит. за 21, Лютий 2023]. URL: https://habr.com/ru/company/distributedlab/blog/416469/
10. Подробно об обновлении Segregated Witness и последствиях его принятия в Bitcoin [Інтернет]. Хабр. [цит. за 21, Лютий 2023]. URL: https://habr.com/ru/company/distributedlab/blog/418853/
11. Tse D. Bribery and stake grinding attacks. Scaling Blockchains, Stanford University. 2020. EE 374. 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 Topics [Інтернет]. [цит. за 23, Січень 2023]. Доступний у: https://www.sciencedirect.com/topics/engineering/liveness
13. What is a distributed hash table? [Інтернет]. Educative: Interactive Courses for Software Developers. [цит. за 23, Січень 2023]. Доступний у: https://www.educative.io/answers/what-is-a-distributed-hash-table
14. Thellman P. Validators Create New Attack Vectors for Decentralized Systems [Інтернет]. 2019 [цит. за 21, Лютий 2023]. Доступний у: https://www.coindesk.com/markets/2019/02/24/validators-create-new-attack-vectors-for-decentralized-systems/
15. What Is Delegated Proof of Stake? [Інтернет]. [цит. за 21, Лютий 2023]. URL: https://crypto.com/university/what-is-dpos-delegated-proof-of-stake
16. Crypto Off-Chain vs. On-Chain Transactions: What Are They? [Інтернет]. Bybit Learn. 2021 [цит. за 29, Січень 2023]. URL: https://learn.bybit.com/blockchain/off-chain-vs-on-chain-transactions
17. Bitcoin White Paper [Інтернет]. [цит. за 03, Лютий 2023]. URL: https://bitcoinwhitepaper.co
18. What is Simplified Payment Verification (SPV)? Definition & Meaning | Crypto Wiki [Інтернет]. BitDegree.org Crypto Exchanges. [цит. за 20, Січень 2023]. URL: https://www.bitdegree.org/crypto/learn/crypto-terms/what-is-simplified-payment-verification-spv
19. What is ARP Spoofing | ARP Cache Poisoning Attack Explained | Imperva [Інтернет]. Learning Center. [цит. за 23, Січень 2023]. URL: https://www.imperva.com/learn/application-security/arp-spoofing
20. DHCP Starvation Attack [Інтернет]. GeeksforGeeks. 2022 [цит. за 21, Лютий 2023]. URL: https://www.geeksforgeeks.org/dhcp-starvation-attack

Стаття надійшла до редакції 8.10.2022
Стаття рекомендована до друку 19.11.2022

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

OFFENSES IN DECENTRALIZED SYSTEMS

ANNOTATION. *Introduction.* 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.

Summary of the main results of the study. 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.

Conclusions. For the first time, a list of the main offenses in decentralized networks such as blockchain has been unified and provided in the context of criminal law.

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

REFERENCES

1. Popovic A, Milijic A. Crypto-democracy: implications of the blockchain technology on the democratic choice. 2020. [cited for 03, February 2023]. URL: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=pnwJInEAAAAJ&citation_for_view=pnwJInEAAAAJ:d1gkVwhDpl0C

2. Driscoll S. How Bitcoin Works Under the Hood [Internet]. [cited for 21, February 2023]. URL: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

3. Chernikov M.Yu. Methods of protecting transactions in blockchain systems. 2021 [cited for February 21, 2023] URL: https://openarchive.nure.ua/handle/document/1943 (in Ukrainian)

4. Double-Spending Problem and Byzantine General's Problem in Relation to Cryptocurrency [Internet]. Freeman Law. [cited for 03, February 2023]. URL: https://freemanlaw.com/double-spending-problem-and-byzantine-generals-problem-in-relation-to-cryptocurrency-2/

5. Kovalchuk D, Ivko T, Kuznetsova T, Nariezhnii O. Overview of consensus protocols used in blockchain technologies. CS&CS E-journal. 24, June 2019;(1):30–43. [cited for 03, February 2023]. URL: https://periodicals.karazin.ua/cscs/article/view/13081 (in Ukrainian)

6. The Longest Chain—Blockchain Guide [Internet]. [cited for 21, February 2023]. URL: https://learnmeabitcoin.com/technical/longest-chain

7. Overview of actual consensus-building protocols in a decentralized environment [Internet]. Habr [cited for 21, February 2023]. URL: https://habr.com/ru/company/distributedlab/blog/419185/

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. [Internet]. [cited for 21, February 2023]. URL: https://eprint.iacr.org/search?q=BitcoinEnhanced+&title=&authors=&category=&submittedafter=&submittedbefore=&revisedafter=&revisedbefore= (in Russian)

9. Synchronization of wallets with the Bitcoin network [Internet]. Habr [cited for 21, February 2023]. URL: https://habr.com/ru/company/distributedlab/blog/416469/

10. Details on the Segregated Witness update and the consequences of its acceptance in Bitcoin [Internet]. Habr [cited for 21, February 2023]. URL: https://habr.com/ru/company/distributedlab/blog/418853/ (in Russian)

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

12. Liveness – an overview. Science Direct Topics [Internet] [cited for 23, January 2023]. URL: https://www.sciencedirect.com/topics/engineering/liveness

13. What is a distributed hash table? [Internet]. Educational: Interactive Courses for Software Developers. [cited for 23, January 2023]. URL: https://www.educative.io/answers/what-is-a-distributed-hash-table

14. Thellman P. Validators Create New Attack Vectors for Decentralized Systems [Internet]. 2019 [cited for 21, February 2023]. URL: https://www.coindesk.com/markets/2019/02/24/validators-create-new-attack-vectors-for-decentralized-systems/

15. What Is Delegated Proof of Stake? [Internet]. [cited for 21, February 2023]. URL: https://crypto.com/university/what-is-dpos-delegated-proof-of-stake

16. Crypto Off-Chain vs. On-Chain Transactions: What Are They? [Internet]. Bybit Learn. 2021 [cited for 29, January 2023]. URL: https://learn.bybit.com/blockchain/off-chain-vs-on-chain-transactions/

17. Bitcoin White Paper [Internet]. [cited for 03, February 2023]. URL: https://bitcoinwhitepaper.co/

18. What is Simplified Payment Verification (SPV)? Definition & Meaning | Crypto Wiki [Internet]. BitDegree.org Crypto Exchanges. [cited for 20, January 2023]. URL: https://www.bitdegree.org/crypto/learn/crypto-terms/what-is-simplified-payment-verification-spv

19. What is ARP Spoofing | ARP Cache Poisoning Attack Explained | Imperva [Internet]. Learning Center. [cited for 23, January 2023]. URL: https://www.imperva.com/learn/application-security/arp-spoofing/

20. DHCP Starvation Attack [Internet]. GeeksforGeeks. 2022 [cited for 21, February 2023]. URL: https://www.geeksforgeeks.org/dhcp-starvation-attack/

The article was received by the editors 08.10.2022
The article is recommended for printing 19.11.2022