ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВИХ АКТИВІВ У BLOCKCHAIN НА ОСНОВІ РІШЕННЯ GNOSIS SAFE»

Виконав студент 6 курсу,групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Крук Д.М.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. Хоча характеристики проектів та рішень з використанням Blockchain значно різняться, загальною рисою, що приписується використанню технології розподіленого реєстру, є менша залежність від посередників, включаючи можливість полегшення безпечної передачі вартості між сторонами без використання взаємно довіреної третьої сторони. Розподілена модель ведення обліку та обчислень також надає можливість більш прямих однорангових та повністю автоматизованих транзакцій, які разом можуть забезпечити майбутні переваги, пов'язані з: швидшим розрахунком фінансових транзакцій; новими фінансовими продуктами; та прямим доступом до мереж цифрових активів для окремих споживачів, інвесторів та підприємств. Впровадження нових технологій, у свою чергу, приводить до появи додаткових видів ризику.

На сьогоднішній день, окрім типових фінансових ризиків, використання цифрових активів у Blockchain піддає користувачів до нових форм операційних ризиків. Вкрай важливо, щоб регулюючі органи працювали над усуненням цих ризиків, у тому числі за рахунок ширшого застосування існуючих стандартів управління операційними ризиками, та більш активного використання наглядових вказівок, а також сповіщення користувачів про необхідність застосування покращеної тактики обачності.

Разом із цим існує необхідність в опрацюванні регуляторного статусу цифрових активів Blockchain, розробці нових документів та стандартів, які враховують профілі ризиків, різні базові технології та постійну еволюцію самого ландшафту, що є унікальними для технології DLT. Також необхідно визначити, як саме ринок цифрових активів буде взаємодіяти з існуючими фінансовими ринками.

Окрім цього, залишаються невирішеними або недостатньо дослідженими питання, пов’язані з безпекою цифрових активів. У сфері децентралізованих фінансів хакерські атаки залишаються основною причиною збитків порівняно з

шахрайством. Смарт-контракти, які широко використовуються в багатьох публічних блокчейнах, також становлять ризики через поєднання властивостей незмінності та публічного перегляду.

Таким чином, залишається актуальною необхідність у дослідженні проблем захисту цифрових активів та розробці рішень щодо забезпечення їх безпеки.

Об'єкт дослідження – безпека цифрових активів у Blockchain.

Предмет дослідження – технологія забезпечення безпеки цифрових активів у Blockchain.

Мета роботи – розробити рекомендації щодо забезпечення безпеки цифрових активів у Blockchain із використанням рішення Gnosis Safe.

Для реалізації поставленої мети були сформульовані наступні завдання:

- проаналізувати особливості та історичний розвиток технології Blockchain, визначити мету створення та переваги над сучасними технологіями;
- дослідити розвиток цифрових активів у Blockchain, визначити основні характеристики та способи використання;
- проаналізувати ризики та проблеми захисту цифрових активів у Blockchain;
- розробити рекомендації щодо забезпечення безпеки цифрових активів у Blockchain із використанням рішення Gnosis Safe.

Практичне впровадження одержаних результатів полягає в опрацюванні й аналізі технології та функцій захисту рішення Gnosis Safe, а також розробці рекомендацій щодо забезпечення безпеки цифрових активів у Blockchain.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції:

1) Всеукраїнська науково-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 79-80 стр.

ДОСЛІДЖЕННЯ РОЗВИТКУ ТЕХНОЛОГІЇ BLOCKCHAIN ТА ЦИФРОВИХ АКТИВІВ

Аналіз особливостей та історичного розвитку технології Blockchain

Технологія Blockchain це база даних записів транзакцій, яка поширюється, перевіряється та підтримується мережею комп'ютерів по всьому світу. Замість єдиного центрального органу, такого як банк, записи контролюються великою спільнотою, і жодна окрема особа не контролює їх, і ніхто не може повернутися назад і змінити або стерти історію транзакцій. Як база даних Blockchain зберігає інформацію в електронному вигляді в цифровому форматі. Блокчейни найбільш відомі своєю ключовою роллю в системах криптовалют, таких як Bitcoin, для підтримки безпечного та децентралізованого запису транзакцій. Інновація з Blockchain полягає в тому, що він гарантує точність і безпеку запису даних і створює довіру без необхідності довіреної третьої сторони.

Однією з ключових відмінностей між типовою базою даних і Blockchain є те, як структуровані дані. Blockchain збирає інформацію разом у групи, відомі як блоки, які містять набори інформації. Блоки мають певну ємність для зберігання, і після заповнення закриваються та пов'язуються з попередньо заповненим блоком, утворюючи ланцюжок даних, відомий як Blockchain. Уся нова інформація, що слідує за щойно доданим блоком, компілюється у новосформований блок, який після заповнення також буде додано до ланцюжка [1].

База даних зазвичай структурує свої дані в таблиці, тоді як Blockchain, як випливає з назви, структурує свої дані в фрагменти (блоки), які об'єднані разом. Ця структура даних за своєю суттю робить незворотну часову шкалу даних, якщо вона реалізована в децентралізованому характері. Коли блок заповнюється, він встановлюється в камінь і стає частиною цієї шкали часу. Кожен блок у ланцюжку отримує точну позначку часу, коли він додається до ланцюжка.

Технологія Blockchain була вперше описана в 1991 році Стюартом Хабером і В. Скоттом Сторнеттою, двома дослідниками, які хотіли впровадити систему, у якій часові позначки документів не можна було б підробити. Але лише майже через два десятиліття, після запуску біткойна в січні 2009 року, цей блокчейн отримав своє перше реальне застосування [2].

Мета Blockchain — дозволити записувати та розповсюджувати цифрову інформацію, але не редагувати її. Таким чином, Blockchain є основою для виду транзакцій, які не можна змінити, видалити або знищити. Ось чому блокчейни також відомі як технологія розподіленої реєстру або distributed ledger technology (DLT) [3].

Технологія розподіленої книги (DLT) — це протокол, який забезпечує безпечне функціонування децентралізованої цифрової бази даних. Розподілені мережі усувають потребу в центральному органі для контролю за маніпуляціями.

DLT дозволяє зберігати всю інформацію безпечним і точним способом за допомогою криптографії. Те ж саме можна отримати за допомогою «ключів» і криптографічних підписів. Після збереження інформації вона стає незмінною базою даних і регулюється правилами мережі.

Ідея розподіленого реєстру не нова, багато організацій зберігають дані в різних місцях. Однак кожне розташування зазвичай знаходиться в підключеній центральній системі, яка періодично оновлює кожне з них. Це робить центральну базу даних вразливою до кіберзлочинності та схильною до затримок, оскільки центральний орган має оновлювати кожну віддалену базу даних.

Сама природа децентралізованої реєстру робить їх несприйнятливими до кіберзлочинів, оскільки всі копії, що зберігаються в мережі, повинні бути атаковані одночасно, щоб атака була успішною. Крім того, одночасний (одноранговий) обмін і оновлення записів робить весь процес набагато швидшим, ефективнішим і дешевшим.

DLT має великий потенціал для революції в роботі урядів, установ і корпорацій [4]. Він може допомогти урядам зі збором податків, видачею паспортів, реєстрацією земельних реєстрів і ліцензіями, витратами на соціальне страхування,

а також процедурами голосування. Ця технологія стає новим етапом розвитку в таких галузях, як фінанси, музика та розваги, мистецтво, ланцюжки поставок різноманітних товарів тощо.

Наразі десятки тисяч проектів прагнуть запровадити технологію Blockchain різними способами, щоб допомогти суспільству, крім простого запису транзакцій, наприклад, як спосіб безпечного голосування на демократичних виборах. Природа незмінності Blockchain означає, що шахрайське голосування стане набагато складнішим. Наприклад, система голосування може працювати так, що кожному громадянину країни буде видана один цифровий актив, криптовалюта або токен. Тоді кожному кандидату буде надана конкретна адреса гаманця, і виборці надсилатимуть свій токен або криптовалюту на адресу будь-якого кандидата, за якого вони бажають проголосувати. Прозорий і відстежуваний характер Blockchain усуне як потребу в підрахунку голосів людьми, так і можливість зловмисників підробляти фізичні бюлетені.

Також мережі Blockchain поділяються за рівнем доступності. В основному їх поділяють на 2 типи:

- Public Blockchains (загальнодоступні або публічні);
- Permissioned Blockchains (авторизовані, дозволені або Blockchain з обмеженим доступом).

Хоча Blockchain-мережі спочатку були розроблені як відкриті, загальнодоступні та доступні для будь-кого, їх авторизовані аналоги служать дещо іншій меті, але все ще забезпечують цінність для учасників.

Blockchain — це цифрова книга, яка дублюється та прозоро поширюється між усіма учасниками мережі. Щоразу, коли Blockchain оновлюється або змінюється (наприклад, додається новий блок до ланцюжка), це реєструється в книзі всіх учасників у режимі реального часу.

Оскільки вони мають доступ до тієї самої розподіленої книги, користувачі можуть відстежувати та перевіряти транзакції, що дозволяє їм визначати походження та автентичність цифрових активів.

Окремі учасники не можуть змінювати або втручатися в транзакцію, записану в ланцюжку, що робить Blockchain незмінним. Щоб оновити облікову книгу, учасники мають досягти консенсусу за допомогою механізму, наприклад Proof-of-Work (PoW) або Proof-of-Stake (PoS) [5].

На відміну від традиційних комп'ютерних систем, де дані розміщуються на центральному сервері, Blockchain-рішення обслуговуються розгалуженою мережею комп'ютерів (майнерів або валідаторів), які перевіряють транзакції та генерують нові блоки в обмін на компенсацію (наприклад, винагороди за блокування, комісії за транзакції).

Це усуває єдину точку відмови, що робить Blockchain-мережі більш стійкими до кіберзагроз. Ще один рівень безпеки додається завдяки шифруванню всіх транзакцій за допомогою криптографії з відкритим ключем.

Через те, що в мережі немає центрального органу (наприклад, компанії, установи чи державного органу), блокчейни є децентралізованими за своєю природою.

Крім того, важливою особливістю Blockchain-мереж є те, що вони працюють на одноранговій основі (P2P) за допомогою автоматизованих процесів, тобто немає потреби третім особам брати участь у транзакції.

Блокчейни без дозволу — це блокчейни, для приєднання та взаємодії з якими не потрібен дозвіл. Вони також відомі як публічні блокчейни. У більшості випадків блокчейн без дозволу ідеально підходить для запуску та керування цифровими валютами [6].

У блокчейні без дозволу користувач може створити особисту адресу, а потім взаємодіяти з мережею, допомагаючи мережі перевіряти транзакції або просто надсилаючи транзакції іншому користувачеві мережі. Тут будь-хто може отримати доступ і брати участь у мережі без географічних чи інших обмежень. Користувачі можуть надсилати транзакції один одному, перевіряти записи в книзі та ставати валідаторами.

Оскільки їм не вистачає централізованої сторони з підвищеними повноваженнями або контролем над іншими користувачами, публічні блокчейни

мають високий рівень децентралізації. Громада несе відповідальність за участь у прийнятті управлінських рішень і підтримку екосистеми.

Оскільки будь-хто має вільний доступ до загальнодоступного блокчейну без подання документів Know Your Customer (KYC) або підтвердження (розкриття) своєї особи, користувачі підвищили (псевдо)анонімність у цих мережах.

Недоліком є те, що блокчейни без дозволу потребують, щоб усі валідатори досягли консенсусу перед додаванням нових блоків у ланцюг. З цієї причини вони менш швидкі та менш масштабовані, ніж їхні дозволені аналоги.

Крім того, спільнота має працювати разом, щоб мережа залишалася ефективною. Якщо це не так, бурхливі дебати можуть розколоти як Blockchain, так і його спільноту під час хардфорку (серйозне оновлення мережі, несумісне з попередніми версіями).

На відміну від публічних блокчейнів, дозволені мережі DLT мають ліміти, які обмежують, хто може брати участь і як (наприклад, деяким користувачам дозволено взаємодіяти лише з певним типом транзакцій).

Дозволені блокчейни зазвичай обслуговуються та управляються бізнесом, у якому беруть участь лише його зацікавлені сторони, співробітники та партнери. Обмеживши доступ до мережі, підприємства можуть захистити свою конфіденційну інформацію, одночасно використовуючи переваги технології блокчейн.

Оскільки кількість учасників обмежена, консенсусу можна досягти лише за допомогою кількох валідаторів, а це означає, що дозволені блокчейни мають набагато кращу продуктивність і можливості масштабування, ніж їх публічні аналоги.

Крім того, оскільки підприємства можуть встановлювати власні правила в дозволених мережах; вони можуть контролювати інфраструктуру та ефективніше виконувати відповідні закони, політику та правила.

Рівень децентралізації в дозволених Blockchain-мережах різний і може бути від дуже низького до високого. Крім управління та механізму схвалення участі,

дозволені блокчейни можуть керувати всіма іншими процесами на повністю децентралізованій основі.

Однак у системі присутній централізований орган (системний адміністратор), який відповідає за надання або заборону доступу новим користувачам.

З цієї причини дозволеним мережам бракує (псевдо)анонімності загальнодоступних блокчейнів, оскільки користувачі відомі як адміністратори, і їм, можливо, доведеться надати документи та іншу інформацію для підтвердження своєї особи.

Знання особи кожного користувача є життєво важливим для ефективної роботи дозволених блокчейнів. Усвідомлення ролі кожного учасника та організації, з якою вони пов’язані, змушує користувачів поводитися чесно (або стикатися з наслідками в своїх компаніях за недотримання правил мережі).

З тієї ж причини дозволені блокчейни можуть уникнути серйозних дебатів і проблем (наприклад, поділу ланцюга) між зацікавленими сторонами та валідаторами.

Використовуючи переваги DLT, такі як підвищена прозорість, відстежуваність і відсутність посередників, як дозволені, так і публічні блокчейни забезпечують учасникам користь та цінність.

Публічні блокчейни, які підтримуються спільнотою та керуються децентралізовано, служать універсальній меті, надаючи кожному доступ до мережі.

З іншого боку, дозволені мережі — це спеціалізовані рішення, створені відповідно до вподобань підприємств, урядів та установ.

Протоколи однорангової верифікації Blockchain означають, що, незалежно від швидкості транзакцій блокчейну, існують затримки в обробці транзакцій, які можуть складати десятки хвилин між виконанням транзакції та її публікацією в мережі. Ці мережеві затримки в оновленні облікових книг можуть спричинити створення невідповідності записаних даних та призвести до можливих втрат через шахрайство, системні атаки, подвійні витрати та фальшиві транзакції [7].

Рис. 1.1. Порівняння Permissioned та Permissionless Blockchains

Майнінг став спеціалізованою галуззю зі значною концентрацією гравців у майнінгових пулах. Якщо майнінговий пул контролюватиме більше половини загальної швидкості хешування, це може призвести до атаки 51% на мережу. Такі атаки можуть виникати. через неузгоджені стимули майнерів.

Крім того, рішення щодо роботи розподіленого реєстру приймаються «основними розробниками» програмного забезпечення для цього реєстру та

валідаторами транзакцій у реєстрі, які визначають остаточний запис про право власності на цифрові активи у цьому реєстрі.

У середовищі PoS можливість перевірки та об'єднання транзакцій у блоки залежить від частки всіх наявних токенів протоколу, що може створити стимули для змови. Така консолідація влади може дозволити валідатору контролювати, які транзакції можуть бути включені до остаточного реєстру. Оскільки валідатори зазвичай винагороджуються знову випущеними токенами, в деяких блокчейнах PoS спостерігається консолідація влади за рахунок купівлі голосів.

У системах PoW майнери також вибирають, замовляють і пропонують транзакції для додавання запис блокчейна, що означає, що майнери отримують прибуток, наприклад, від продажу слотів більш ранньої обробки. Це може вплинути на прибутковість транзакцій та ініціювати чи затримати передачу права власності, регульовану смарт-контратами.

Крім того, незалежно від того, чи це механізм консенсусу PoS або PoW, майнери можуть спостерігати, вибирати та реорганізовувати транзакції під час процесу перевірки, а також регулярно включати, виключати або змінювати порядок транзакцій у створюваних ними блоках, таким чином віддаючи пріоритет транзакціям, які платять більші збори. Ця дискреційна практика, яка називається «вартістю, що видобувається майнером» (MEV), є одночасно непрозорою та потенційно невигідною для користувачів в екосистемі цифрових активів у Blockchain.

Цифрові активи у Blockchain, їх види та способи застосування

Цифрові активи або криптовалюти — це просто віртуальні активи, що працюють на основі технології Blockchain. DLT або розподілена книга записує та підтверджує транзакції, здійснені з використанням цих цифрових активів, і, по суті, усуває потребу в банках третіх сторін. Ці валюти не мають фізичної форми. Тому їм потрібні складні системи безпеки.

Завдяки впровадженню криптографії в технологію Blockchain стає можливим призначити два набори ключів, які служать формою встановлення права власності на монети, а також шифрування та дешифрування транзакцій або інформації. Ці криптографічні ключі, які називаються приватними та відкритими ключами, являють собою довгі рядки буквено-цифрових символів, які гарантують, що лише уповноважені особи мають доступ до монет, як імена облікових записів і паролі функціонують у банківському світі.

Проходячи цю аналогію, можна сказати, що приватні ключі мають такий же рівень чутливості, як і банківські паролі, оскільки вони використовуються для підписання транзакцій і розшифровки вхідних коштів. З іншого боку, відкритими ключами є Blockchain-ітерації імен і номерів облікових записів, які також шифрують вихідні транзакції. Щоб успішно надіслати цифрові активи, ви повинні включити відкритий ключ одержувача для шифрування транзакції, а одержувач повинен використовувати відповідний закритий ключ, щоб розшифрувати його, щоб отримати кошти.

Однак, на відміну від традиційних банківських систем, це не фактичний обмін активами, а лише передача права власності, який визначається і підписується у Blockchain-транзакції.

Завдяки цій структурі приватні та відкритий ключі є важливими компонентами безпеки Blockchain, оскільки вони допомагають встановити право власності на цифрові активи та авторизувати користувачів для виконання транзакцій. Тому було сенс створити інфраструктуру безпеки, призначену для зберігання цих конфіденційних ключів. У цьому полягає мотивація для впровадження цифрових гаманців.

Всупереч поширеній думці, цифрові гаманці не зберігають цифрові активи. Натомість вони забезпечують відповідне сховище для особистих і відкритих ключів. Також варто зауважити, що адреси гаманців – це просто хешовані відкриті ключі. Простіше кажучи, адреси гаманців – це скорочені версії відкритих ключів. І як було зазначено раніше, цифрові гаманці змінюють баланс лише на основі зміни власника активу. Якщо користувач втратить доступ до свого закритого ключа,

шансів відновити свої активи буде мало або взагалі немає. Крім того, на відміну від звичайних фінансових систем, важко скасувати транзакції, а ще важче повернути вкрадені кошти. Отже, необхідно зробити все можливе, щоб убезпечити свої гаманці.

Цифрові активи можуть бути оригінальними та невід'ємними твореннями основного розподіленого реєстру або блокчейну - їх іноді називають «рідним» для певної мережі. Крім того, вони можуть бути «токенізованими» представленнями активів, випущених традиційними фінансовими установами або юридичними особами, такі як акції чи облігації, без початкової залежності від DLT.

Кожен тип цифрових активів може мати різну конвертованість, взаємозамінність та інші атрибути. Учасники ринку часто розрізняють «взаємозамінні» та «невзаємозамінні» активи або токени, причому кожен тип створюється відповідно до іншого стандарту токенів [8]. Для взаємозамінних токенів кожна одиниця токена має дорівнювати за характером та вартістю іншим одиницям цих токенів. Стейблкоїни є прикладом одного з типів взаємозамінних токенів. Стейблкоїни розробляються з метою підтримки стабільної вартості, зазвичай по відношенню до фіатної валюти або інших активів [9].

Не взаємозамінні токени (NFT) - це цифрові активи, створені з використанням програмного коду, який не взаємозамінний з іншим програмним кодом. NFT призначені для подання вимоги або квитанції на актив чи об'єкт, який має унікальні характеристики або відрізняється від аналогічних активів будь-яким помітним чином.

Хоча NFT можна продавати, вони не взаємозамінні. Прихильники NFT заявляють, що вони мають багато потенційних застосувань, таких як представлення предметів колекціонування (наприклад, творів мистецтва чи музики), цифрових товарів, індивідуальних ідентифікаційних даних, ключів доступу, документів на власність чи титулів, а також квитків на подорожі чи заходи.

Також до потенційних можливостей NFT можна віднести:

- можливість реєстрації та перевірки передачі прав власності на нерухомість;

- сприяння автоматичним виплатам роялті за музику та фільми;
- запобігання дублюванню та підробкам при оформленні прав на інше майно та споживчі товари;
- забезпечення більшої кількості цифрових облікових даних, включаючи ідентифікацію, ліцензування, сертифікацію.

NFT можуть працювати як у цифровому просторі, так і у фізичному світі. В результаті NFT можуть включати функції, які служать членськими картами або квитками, забезпечуючи доступ до заходів, ексклюзивних товарів і спеціальних знижок.

Однак багато з потенційних випадків використання NFT все ще матеріалізуються, частково через розвиток технологічного та правового ландшафту, зокрема щодо ліцензування, контрактів, авторського права та інтелектуальної власності, боротьби з відмиванням грошей і захисту даних. Незважаючи на всі переваги технології, юридичні права, що надаються NFT, неясні і є предметом судових розглядів [10].

1.3 Правовий і нормативний статус цифрових активів у Blockchain

Випуск, торгівля, розрахунки та зберігання цінних паперів та національних валют чітко визначені законодавством і нормативними актами в кожній країні з активним ринком капіталу. Розширення цих законодавчих і нормативних рамок на екосистеми, засновані на мережах DLT, врегульовано в кількох юрисдикціях і ще не врегульовано в багатьох інших. Однак доцільно завжди припускати, що закони про цінні папери застосовуються до цифрових активів у Blockchain. Також розумно очікувати, що існуючі закони та нормативні акти про цінні папери з часом будуть розширені та адаптовані для адаптації до екосистем Blockchain, не в останню чергу тому, що багато регуляторних органів у всьому світі працюють над досягненням цього.

Тим не менш, емітенти та інвестори в цифрові активи зараз працюють в середовищі, в якому правовий і нормативний статус цих нових інструментів все ще

розвивається. За цих обставин методи, розроблені індустрією послуг з цінними паперами для дотримання законів і правил, що регулюють випуск, розрахунки, зберігання та обслуговування цінних паперів, дають цінну інформацію про те, як можна захистити інвесторів у криптоактиви та зберегти цілісність ринків.

Отже, необхідно розглянути проблеми, які залишаються для регуляторів у цьому просторі для того, щоб вони змогли забезпечити стабільне та прозоре регуляторне середовище. Основні серед них:

1. Неможливо узгодити стандартний набір таксономії для різних цифрових активів на глобальній основі. Це пов’язано з тим, що існує багато різних факторів, які необхідно враховувати, будь то профілі ризиків, різні базові технології, постійна еволюція самого ландшафту таких активів та історичні проблеми визначення цінного паперу. Ключовим прикладом цього може бути стейблкойни, які можуть мати значно різні профілі ризику залежно від їх емітента та базових активів, які їх підтримують.

2. Регулятори визнають, що новому ринку цифрових активів необхідно буде взаємодіяти з існуючими фінансовими ринками. Це вимагає розуміння того, де існуючі нормативні периметри можуть бути застосовані до цих активів, а де потрібні нові регулювання. Складність полягає у визначенні ключових прогалин і пропорційному застосуванні нових правил.

3. Незважаючи на те, що багато урядів прагнуть процвітання інновацій у їхніх країнах, Blockchain і пов’язані продукти є особливою сферою уваги, регулятори побоюються дозволити зростання крипторинку до точки, коли це стане ризиком для фінансової стабільності. Критика після кризи 2009 року, зрозуміло, спонукала до консервативного підходу до нового ринку, який потенційно може створити нові ризики.

4. Існує думка, що технологія DLT нерозривно пов’язана з самими цифровими активами та управлінням навколо них. Тобто, використовуючи розподілену архітектуру, немає жодного органу чи органу, який несе відповідальність, коли щось йде не так. У нормативному середовищі, яке зосереджується на притягненні до відповідальності установ та окремих осіб, це

важко узгодити. Існує бажання серед багатьох у регуляторному співтоваристві застосувати ту саму діяльність, той самий ризик, той самий підхід до правил, але це може бути важко застосувати, якщо не ясно, що діяльність і ризики є такими ж, як на існуючих ринках.

5. У зв'язку з точкою управління існує думка, що розподілений характер технології є загрозою операційній стійкості, а не позитивним розвитком, який потенційно може зменшити одиничні точки відмови та зменшити складність постторгових процесів. Регулятори хочуть, щоб галузь пояснила, як саме технологія може протистояти кібератакам, збоям у хмарі тощо.

Протягом останніх двох років можна було визнати, що дебати навколо цифрових активів у Blockchain, які класифікуються як цінні папери, часто перекривалися дискусіями навколо домовленостей про стейблкойн. В останньому звіті ФСБ про прогрес у сфері регулювання, нагляду та контролю за угодами «Global Stablecoin» були зазначені огляд та рекомендації щодо регулювання цього виду цифрового активу [11].

Різні країни застосовують або розглядають різні підходи до впровадження рекомендацій високого рівня. Оскільки ландшафт стейблкойнів швидко розвивається та розробляється регуляторна та наглядова політика, відмінності між регуляторними підходами та класифікаціями можуть зростати. Наприклад, деякі юрисдикції прагнуть реалізувати рекомендації шляхом прийняття нових правил і норм, тоді як інші внесли або планують внести зміни в існуючі правила і норми таким чином, щоб вони були застосовні до стейблкойнів. Інші юрисдикції значною мірою покладаються на існуючі режими регулювання та нагляду для вирішення ризиків, пов'язаних зі стейблкойнами або з організаціями, які є частиною угоди про стейблкойни.

Різні нормативні класифікації та підходи до стейблкойнів на рівні країн можуть призвести до ризику регуляторного арбітражу та шкідливої фрагментації ринку.

Тим не менш, органи влади визначили кілька проблем, пов’язаних із впровадженням рекомендацій, які можуть вимагати подальшого розгляду та де подальша робота на міжнародному рівні може бути корисною. До них належать:

- умови для кваліфікації стейблкойна як «глобального стейблкоіна»;
- пруденційні вимоги, вимоги щодо захисту інвесторів та інші вимоги до емітентів, зберігачів і постачальників інших глобальних функцій стейблкойнів (наприклад, постачальників гаманців);
- права викупу;
- транскордонне та міжгалузеве співробітництво та координація;
- взаємне визнання та прийняття.

На даний момент, попри всю невизначеність і занепокоєння, одне юридичне та нормативне питання є першорядним для зберігачів і центральних депозитаріїв. Чіткість щодо регуляторного статусу криптоактиву є необхідною умовою для прийняття емітентами, інвестування інвесторами та підтримки з боку постачальників послуг, оскільки це має наслідки для юридичної обґрунтованості інвестицій та правового статусу суб’єктів, що обслуговують такі активи, і послуги, які вони надають. Крім того, правовий статус такого активу також впливає на його бухгалтерський облік.

Ключова відмінність, яку необхідно встановити в регулюванні, полягає в тому, чи є цифровий актив у Blockchain цінним папером, чи платежем, чи чимось іншим. Критерії, за якими цифрові активи вважаються цінними паперами, різняться між країнами, що ускладнює будь-яку оцінку ризиків, яких зазнають постачальники послуг цифрових активів у різних країнах – або, принаймні, змушує постачальників послуг приймати рішення на основі кожної з країн. Крім того, поява цифрових активів у Blockchain показала, що активи можуть бути випущені під одну категорію, але протягом життєвого циклу їх існування можуть змінювати свої характеристики та потрапляти в іншу категорію. Яскравим прикладом цього є Bitcoin. Спочатку випущений з наміром служити платіжним засобом, тепер він використовується переважно як засіб інвестування.

Деякі регулятори оцінюють цифрові активи в кожному конкретному випадку, але інші використовують фіксовані критерії. Деякі юрисдикції, наприклад Велика Британія, розробили вказівки щодо класифікації платіжних токенів, корисних токенів і токенів цінних паперів. Інші юрисдикції надали механізми, які допомагають учасникам ринку оцінити, чи застосовується законодавство про цінні папери до конкретних цифрових активів. Наприклад, у Сполучених Штатах Комісія з цінних паперів і бірж (SEC) «Framework for Investment Contract Analysis of Digital Assets» використовує тест Хауї [12]. У Франції Autorité des Marchés Financiers (AMF) використав Закон PACTE (Action Plan for Business Growth and Transformation) для підтримки розвитку певних типів цифрових активів.

Деякі країни створили або знаходяться в процесі створення правової бази для цифрових активів у Blockchain, щоб надати певність для фінансових ринків. Деякі органи влади оновлюють існуючі рамки, а інші створюють нові на основі існуючих. Кілька прикладів:

1. **Європейський Союз.** 24 вересня 2020 року Європейська комісія (EUComm) прийняла пакет цифрових фінансів, включаючи стратегію цифрового фінансування та законодавчі пропозиції щодо цифрових активів і цифрової стійкості, для конкурентоспроможного фінансового сектору ЄС, який надає споживачам доступ до інноваційних фінансових продуктів, забезпечуючи при цьому споживачам захист і фінансову стабільність. Що стосується цифрових активів у Blockchain, ЄС розрізняє ті активи, які вже регулюються законодавством ЄС, та інші цифрові активи. Перше залишатиметься підпорядкованим чинному законодавству, але EUComm пропонує пілотний режим для ринкових інфраструктур, які хочуть спробувати торгувати та здійснювати розрахунки за транзакціями фінансових інструментів у формі цифрових активів у Blockchain. Це повинно дозволити учасникам ринку та регуляторам отримати досвід використання бірж DLT, які торгуватимуть або реєструватимуть акції чи облігації в цифровому реєстрі.

Для раніше нерегульованих цифрових активів, включаючи «стейблкойни», EUComm пропонує спеціальний режим («Markets in Crypto Assets, MiCA») [13].

Запропонований регламент встановлює суворі вимоги до емітентів криптоактивів у Європі та постачальників послуг криптоактивів, які бажають подати заявку на отримання дозволу надавати свої послуги на єдиному ринку. Запобіжні заходи включають вимоги щодо капіталу, зберігання активів, обов'язкову процедуру подання скарги, доступну для інвесторів, і права інвестора проти емітента. До емітентів значних забезпечених активами криптоактивів пред'являтимуться більш жорсткі вимоги до капіталу, управління ліквідністю та вимоги до сумісності.

Станом на жовтень 2022 року різні проекти пропозицій обговорюються та узгоджуються в триалоговому обговоренні між установами ЄС. Очікуване набуття чинності, швидше за все, не раніше 2023 року.

2. **Німеччина.** Законопроект про запровадження електронних цінних паперів (Electronic Securities Act, eWpG) був прийнятий парламентом Німеччини 6 травня 2021 року та набув чинності 10 червня 2021 року. Закон розглядає ключові міркування зі Blockchain Strategy (опублікованої в 2019 році), запроваджуючи нову категорію «електронних цінних паперів», які еквівалентні традиційним цінним паперам, випущеним за допомогою фізичного сертифіката. Вимогу щодо фізичного сертифіката замінено записом в електронному реєстрі цінних паперів. Новий закон класифікує електронні цінні папери як «рухоме майно» за значенням Цивільного кодексу Німеччини.

5 серпня 2021 року Федеральне міністерство фінансів Німеччини опублікувало спільний з Федеральним міністерством юстиції та захисту прав споживачів проект закону про розпорядження про електронні реєстри цінних паперів (eWpRV) [14].

3. **Швейцарія.** У Швейцарії 1 серпня 2021 року набула чинності поправка до Закону про інфраструктуру фінансового ринку (FMIA), яка є частиною законопроекту 19.074 щодо «приведення швейцарського законодавства до розробок у сфері технології розподіленого реєстру», яка запроваджує торгову систему DLT як нову категорію ліцензії на торгівлю токенами безпеки. Хоча цей крок справді усуває регуляторні перешкоди, які досі перешкоджали створенню

ефективних вторинних ринків для маркерів безпеки, не можна ігнорувати, що вимоги до роботи торгової системи DLT будуть подібні до вимог традиційних бірж.

Уже 1 лютого 2021 року набула чинності перша частина рамкового закону DLT, яка запроваджує цінні папери на основі бухгалтерської книги, такі цінні папери створюються шляхом запису в книзі цінних паперів і можуть бути використані та передані лише через цю книгу цінних паперів. Книга цінних паперів повинна відповідати вимогам, згаданим і охарактеризованим у Швейцарському кодексі зобов'язань. Реєстраційний договір створює установчий зв'язок між правом і записом у книзі. Цінні папери, засновані на реєстрі, виконують ті ж функції, що й фізичне замовлення або інструмент на пред'явника (документовані цінні папери), особливо функції прозорості, підтвердження права власності та захисту комерційних операцій [15].

4. **Україна.** 15 березня 2022 року Президент України підписав Закон України «Про віртуальні активи» [16]. Законом легалізується ринок віртуальних активів, запроваджується комплексне регулювання правовідносин, що виникають у зв’язку з обігом віртуальних активів в Україні, визначаються права та обов’язки учасників ринку віртуальних активів, засади державної політики у сфері обігу віртуальних активів.

Закон має на меті встановлення правил для постачальників послуг, пов’язаних з обігом віртуальних активів і відповідальність за порушення встановлених правил, та, як заявлено, базується на актуальних стандартах регулювання операцій із віртуальними активами міжнародної групи з протидії відмиванню грошей (FATF). Закон не регулює питання оподаткування операцій, пов’язаних із віртуальними активами.

Сфера застосування Закону обмежується визначеним колом правовідносин, зокрема, випадками, коли:

- сторони визначили право України як таке, що підлягає застосуванню до правочину, предметом якого є віртуальний актив, в цілому або до окремої його частини;

- обидві сторони правочину, предметом якого є віртуальний актив, є резидентами України;
- особа, яка здійснює операції з віртуальними активами у своїх інтересах (набувач віртуального активу), є резидентом України;
- у разі постачання послуг, пов'язаних з оборотом віртуальних активів, суб'єкти правовідносин мають зареєстроване місцезнаходження або постійне представництво на території України.

Закон визначає віртуальний актив як нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав.

Закон виділяє такі види віртуальних активів:

- незабезпечені – віртуальні активи, що не посвідчують жодних майнових або немайнових прав (наприклад, Bitcoin);
- забезпечені – віртуальні активи, що посвідчують майнові права, зокрема права вимоги на інші об'єкти цивільних прав (наприклад, окремі стейблкойни);
- фінансові – віртуальні активи, забезпечені цінними паперами або гривнею (наприклад, токени безпеки).

Одним із ключових учасників ринку віртуальних активів є постачальники послуг, пов'язаних з оборотом віртуальних активів. Ними визнаються виключно суб'єкти господарювання юридичні особи, які провадять в інтересах третіх осіб один або декілька з таких видів діяльності, що вимагають отримання спеціального дозволу відповідно до Закону.

Закон передбачає можливість набуття права власності на віртуальний актив за фактом його створення, внаслідок вчинення і виконання щодо нього правочину та на підставі норм закону або рішення суду. Право власності на віртуальний актив засвідчується володінням ключа такого віртуального активу, крім окремих випадків, визначених Законом.

Законом встановлено, що розпорядження забезпеченим віртуальним активом вважатиметься розпорядженням майновим правом на об’єкт забезпечення цього віртуального активу. При цьому варто мати на увазі, що під час вчинення правочину щодо розпорядження забезпеченим віртуальним активом Закон вимагає дотримання встановлених вимог щодо форми або істотних умов правочину про розпорядження об’єктом забезпечення віртуального активу.

Одним із ключових обмежень, передбачених Законом, є заборона використовувати віртуальні активи в якості засобу платежу на території України та обмінювати їх на майно (товари), роботи (послуги). Таким чином, якщо правочин щодо майна (товарів), робіт (послуг) підпадатиме під сферу регулювання Закону, проведення розрахунків із використанням криптовалют буде неможливо.

Очевидно, наведене вище обмеження не повинно стосуватись випадків передачі об’єкта забезпечення забезпеченого віртуального активу його власнику під час його погашення (припинення обороту).

Для постачальників послуг, пов’язаних з оборотом віртуальних активів встановлено ряд вимог, зокрема щодо складу менеджменту, власників істотної участі та бенефіціарних власників, розміру статутного капіталу. При цьому, за певних умов постачальником послуг, пов’язаних з оборотом віртуальних активів, може бути іноземна юридична особа.

Варто зазначити, що станом на листопад 2022 року Закон ще не набрав чинності. Закон набере чинності лише з дня набрання чинності Законом України «Про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами».

Також, у листопаді 2022 року Національна комісія з цінних паперів та фондового ринку створила консультаційну раду для отримання якісної експертизи та професійної оцінки у напрямку впровадження віртуальних активів [17].

Основним завданням ради є розробка та узгодження законопроекту про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами та змін до Закону України «Про віртуальні

активи». А також узгодження інших питань щодо нормативного врегулювання діяльності на ринку віртуальних активів.

Тим не менш, на даному етапі залишається значна правова невизначеність щодо регуляторного статусу цифрових активів Blockchain у багатьох країнах, у тому числі, в деяких випадках, у межах однієї юрисдикції. Однак загалом регулятори, як правило, віддають перевагу підходу «сутність над формою», за якого цифровий актив, який має ті самі характеристики, що й регульований цінний папір, регулюється таким же чином.

Висновки до першого розділу

Досліджено особливості та історичний розвиток технології Blockchain. Окреслено та систематизовано основні поняття щодо технології та її застосування.

Зроблено висновок, що основною метою Blockchain є створення децентралізованої технології без посередників, яка дозволить записувати та розповсюджевати інформацію без можливості її редагування, а також створювати цифрові активи з метою збереження цінності або для грошових розрахунків, які захищені криптографією.

Визначено, що основними особливостями та перевагами технології розподіленого реєстру є: захищена криптографією транзакція грошей, прозорість, децентралізація, розумні контракти (smart contracts), підтвердження власності та цифрова ідентифікація.

Здійснено аналіз сучасної законодавчої та нормативно-правової бази щодо статусу цифрових активів Blockchain у різних країнах. Зроблено висновок, що на даному етапі впровадження технології розподіленого реєстру в сучасну фінансову систему все ще залишається значна правова невизначеність щодо регуляторного статусу цифрових активів у Blockchain. На території нашої країни підписаний Закон «Про віртуальні активи», а також створена рада, основним завданням якої є розробка та узгодження законопроекту про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами.

2 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ЗАХИСТУ ЦИФРОВИХ АКТИВІВ У ТЕХНОЛОГІЇ BLOCKCHAIN

2.1 Аналіз ризиків щодо використання та зберігання цифрових активів у Blockchain

Здатність технології Blockchain здійснювати транзакції в «ненадійних» середовищах із зменшеним числом посередників створює низку потенційних можливостей, багато з яких ще необхідно реалізувати. Прихильники вже давно заявляють, що нові фінансові продукти та послуги можуть бути створені для роботи в автоматизованому та розподіленому середовищі з потенційно нижчими експлуатаційними витратами та за рахунок швидшого розрахунку платежів з використанням цифрових активів. Однак використання нових технологій приводить до виникнення додаткових ризиків.

У міру зростання ринку цифрових активів та криптовалют зростала і кількість шахрайства, а об’єм незаконних транзакцій у всьому світі досягнув рекордно високого рівня в 2021 році. Злочинці часто користуються інноваціями та новими технологіями для здійснення шахрайських дій, включаючи обіцянки або гарантії високого прибутку. Більш того, екосистема цифрових активів у Blockchain має унікальні особливості, які роблять її все більш привабливою мішенню для протиправної діяльності, включаючи еволюцію базової технології, що триває, псевдоанонімність, незворотність транзакцій і поточну асиметрію інформації між емітентами цифрових активів і споживачами та інвесторами.

Декілька урядових агентств США відстежують і публікують скарги, пов'язані з цифровими активами, про які повідомляє громадськість, що вказує на різке збільшення втрат, пов'язаних із цими активами. Вони також випустили попередження, пов'язані з їхніми висновками, у тому числі відзначивши суттєве збільшення криптовалют як спосіб оплати для всіх типів шахрайства, включаючи

шахрайство з інвестиціями, шахрайство в романтичних відносинах, а також шахрайство з видачею себе за іншу особу з боку бізнесу та уряду.

У період з 1 січня 2021 року по 31 березня 2022 року Федеральна торгова комісія (FTC) повідомила про понад 46 000 випадків шахрайства, при цьому люди заявляли про збитки цифрових активів на суму понад 1 мільярд доларів США [18]. Цифрові активи та криптовалюта становили 24% усіх збитків, пов’язаних із шахрайством, про які повідомили FTC протягом цього періоду, — це більше, ніж будь-який інший спосіб оплати.

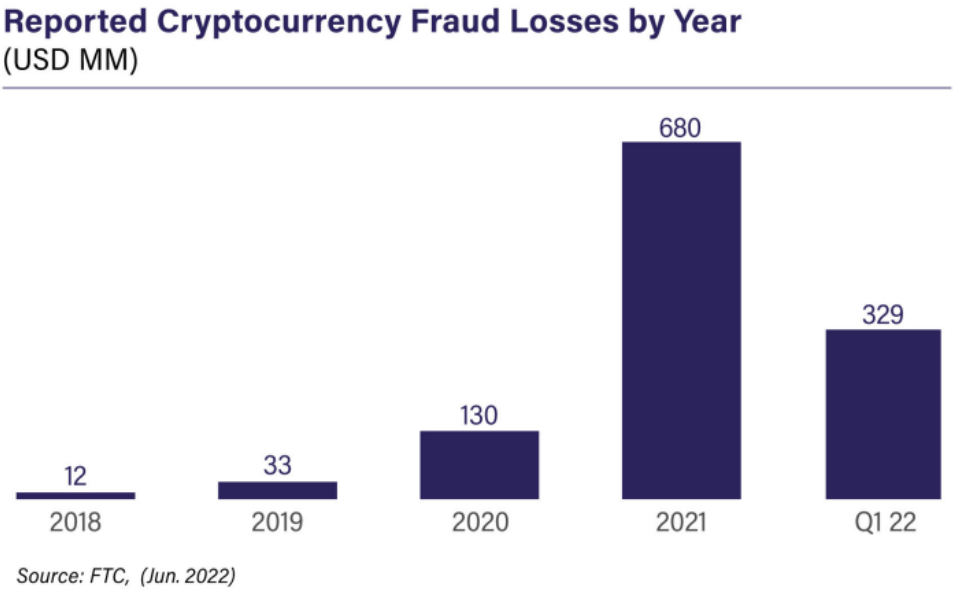

Рис. 2.1. Повідомлені втрати від шахрайства з криптовалютою за роками

При використанні цифрових активів у Blockchain є безліч потенційних можливостей, а також відомих та нових ризиків для споживачів, інвесторів та бізнесу. Характер та інтенсивність цих ризиків та можливостей може відрізнятися залежно від населення та спільноти. Це пов'язано як з основними соціальними та економічними факторами (наприклад, нерівність у рівні добробуту, історичне виключення з фінансової системи та нерівномірний цифровий доступ), так і з поведінкою, характерною для цифрових активів, включаючи маркетингові методи, які можуть бути орієнтовані на певні спільноти.

Не всі групи населення, вразливі до різних впливів однаково, і існують суттєві відмінності як усередині, так і між спільнотами та окремими людьми. Деякі особи можуть вважатися вразливими для різного впливу через порівняння з наявним доходом, наприклад, особи з низьким доходом. В інших може бути підвищена можливість зіткнутися з упередженістю і дискримінацією, наприклад, Співтовариства корінних народів та кольорових людей (BIPOC). Деякі люди похилого віку можуть бути менш знайомі з цифровими пропозиціями і можуть бути більш схильні до шахрайства. Діти можуть бути більш вразливими і, отже, менш схильними піддавати сумніву цільовий маркетинг. Неспівставні наслідки можуть відрізнятися залежно від пропозиції цифрових активів, оскільки різні продукти та послуги потенційно представляють різні можливості та ризики для користувачів.

Деякі учасники галузі просувають цифрові активи у Blockchain тим, хто не має доступу до стандарних фінансових послуг, як засіб розширення доступу до них та накопичення багатства, із заявленою обіцянкою служити альтернативою точкою входу в банківську систему. Зокрема, деякі прихильники стверджують, що цифрові активи можуть полегшити та надати ширший доступ до інвестиційних можливостей та потенційно дешевших і доступніших фінансових продуктів.

Тим не менш, наявні на сьогоднішній день дані свідчать про те, що потенційні переваги цифрових активів у Blockchain у фінансовій доступності значною мірою ще не матеріалізувалися, а продукти таких активів можуть становити підвищений ризик для населення, вразливого до різних впливів.

Певний тип цифрових активів, наприклад, криптовалюти, схильні до значних коливань цін, і групи захисту прав споживачів попереджають про відсутність належного захисту прав споживачів [19]. Багато в чому ризики, пов'язані з володінням цифровими активами, однакові для всіх. Однак особи з меншими ресурсами, у тому числі особи з низьким доходом, можуть наражатися на більший ризик щодо свого наявного доходу, а це означає, що понесені збитки можуть вплинути на їх фінансове благополуччя.

Волатильність ринку та відсутність засобів захисту або достатнього розкриття інформації про ризики також можуть підірвати довіру до цифрових

активів, особливо серед груп населення, деякі з яких можуть особливо насторожено ставитися до фінансових ринків та установ. Несподівані збитки через рухи ринку та нерозуміння потенційного ризику можуть підірвати довіру споживачів та довіру до екосистеми цифрових активів у Blockchain. Таке погіршення довіри може призвести до подальшого негативного впливу на ціну активу. Ця динаміка аналогічна тій, що спостерігалася у банківській системі США до появи сучасного режиму банківського законодавства та регулювання [20].

Операційний ризик використання цифрових активів у Blockchain в цілому визначається як ризик збитків, спричинених недосконалістю або збоєм процесів, політик, систем або подій [21]. У контексті багатосторонніх систем розрахунків і реєстрації фінансових операцій це включає ризик того, що недоліки в інформаційних системах або внутрішніх процесах, людські помилки, збої керівництва та управління або збої через зовнішні події будуть знижувати, погіршувати або викликати збої в послугах, що надаються. Такі недоліки в інформаційних системах або процесах також включають помилки або затримки в обробці, перебої в роботі системи, загрози інформаційній безпеці, такі як кібератаки, недостатня потужність, шахрайство, втрата даних та витік (наприклад, помилки у розрахунках, упущення та неточності) [22].

Коли активи зі значною вартістю знаходяться і торгуються у дозволених блокчейнах або блокчейнах без дозволу, власники активів покладаються на технологію системи Blockchain для доступу до своєї цифрової власності. Крім того, в системах цифрових активів у Blockchain використовуються інші технології, процеси транзакцій та розподілені структури управління з новими функціями, які можуть бути не такими надійними, як стандарти зниження операційного ризику на зареєстрованих ринках [23]. Ці характеристики технологій та продуктів цифрових активів приводять користувачів до унікальних операційних ризиків. Деякі приклади включають відсутність механізмів реверсу або інших засобів захисту від випадкових чи хибних транзакцій, а також проблеми, пов'язані з відсутністю сумісності блокчейнів, у тому числі виникаючі через недоліки мостів між ланцюгами, уразливостей, пов'язаних із закритими ключами, і труднощів інтеграції

блокчейнів із традиційними або застарілими системами. Таким чином, споживачі, інвестори та підприємства повинні знати, що зростання загальнодоступних блокчейнів у тому вигляді, в якому вони існують в даний час, піддає їх цим новим формам ризику.

На додаток до ризиків поведінки та впливів у екосистемі цифрових активів та нових операційних ризиків існують також традиційні фінансові ризики, які можуть виявлятися на ринках цифрових активів з особливими наслідками, враховуючи динаміку таких ринків. Цифрові активи, незалежно від низки фінансових та нефінансових характеристик, які вони можуть мати, часто створюються, продаються, торгуються та зберігаються з використанням одних і тих самих технологічних систем, протоколів безпеки, а також фінансового та операційного контролю. Унікальні ризики між об'єктами цифрових активів та продуктами можуть створити основу для підвищеного занепокоєння. А саме, фірми, що діють як посередники, системні адміністратори та інші сторони на ринках цифрових активів, можуть недостатньо враховувати негативні зовнішні фактори, які можуть вплинути на ці взаємопов'язані активи, фірми або діяльність, в порівнянні з традиційними фінансовими фірмами, чия нефінансова діяльність часто обмежені чи підлягають значному контролю.

Споживачі, інвестори та підприємства, які використовують цифрові активи, схильні до ризиків, оскільки посередники цифрових активів можуть не мати (або не виділили чи розвивати) адекватні ресурси та можливості для виконання своїх зобов'язань щодо захисту, що призводить до втрати цінності для користувачів, збої у роботі бізнесу постраждалих клієнтів та зниження довіри до сектору цифрових активів загалом. Втрата довіри, що виникає в результаті, може також призвести до локального або загального вилучення ресурсів із порушених фірм або видів діяльності, що посилить вплив первісних наслідків.

До потенційних ризиків, які пов'язані з фірмами, що займаються цифровими активами та ринковими методами, відносяться:

1. *Ризики ресурсів і можливостей*. Висока нестабільність цін на цифрові активи, включаючи активи, що використовуються для кредитування та розміщення

ставок, можуть збільшити ризик вимог до маржі щодо фактичних посередників цифрових валют, а також подальшої ліквідації забезпечення, якщо вимоги до маржі не будуть задоволені. Хоча деякі держави регулюють безпеку та стійкість компаній, які займаються активами цифрових валют, ліцензованих небанкінськими діями, державні закони не регулюють національні та міжнародні масштаби діяльності цих компаній. Фінансові потрясіння та дисбаланси можуть бути недостатніми для усунення зростаючого ризику банкрутства та невдач у роботі компаній, які можуть негативно вплинути на споживачів, інвесторів та бізнесу, особливо для багатьох компаній та проектів, які займаються цифровими активами у Blockchain на етапі розвитку.

2. *Ризики щодо зберігання.* Незважаючи на те, що зберігання цифрових активів сторонніми компаніями є динамічним полем, яке швидко розвивається, наразі не існує рішення, яке захищає споживачів, інвесторів та підприємств у разі неплатоспроможності та невдачі цих компаній. Крім усього іншого, хоча багато моделей платформи передбачають зберігання, концепція «захисту» для цифрових валют відрізняється, ніж для традиційних фінансових активів, з якими клієнт може бути знайомий. Криптовалютні фірми, які, як здається, мають загальні характеристики з традиційними фінансовими фірмами, але чиї операційні компанії займають позицію, що вони не регулюються, або діють так, ніби вони не регулюються, не підпадають під положення Кодексу про банкрутство. Такі ризики особливо виражені, коли майно неплатоспроможної фірми зосереджена на цифрових активах з нестабільними цінами, що може ускладнити справу про банкрутство.

Проблеми забезпечення безпеки цифрових активів від злому та шахрайства

Загальнодоступні блокчейни без дозволу є формами комп'ютерного програмного забезпечення і схильні до уразливостей програмного забезпечення [24]. Вони можуть мати програмні помилки та потребувати постійного оновлення для усунення проблем і додавання нових функцій.

Програмне забезпечення також уразливе для атак хакерами. Хоча деякі функції безпеки найбільших загальнодоступних блокчейнів, таких як Bitcoin та Ethereum, вважаються надійними, у міру того, як технологія стає більш використовуваною, стимули для атак можуть збільшуватися.

Публічні блокчейни без дозволу зазвичай базуються на програмному забезпеченні з відкритим вихідним кодом, тобто програмному забезпеченні, яке дозволяє перевіряти та модифікувати вихідний код, вільно розповсюджується, є технологічно нейтральним і надає безкоштовні допоміжні ліцензійні права. Хоча ця домовленість збільшує кількість сторін, хто може сприяти подальшому розвитку вихідного коду блокчейну, це може зменшити заохочення щодо своєчасного виправлення помилок та вдосконалення програмного забезпечення. Рішення для посилення стимулів для вдосконаленої розробки програмного забезпечення, такі як основні групи розробників, які керують розробкою, або винагорода для розробників, які приділяють більше часу спільному проекту, також можуть створити нові проблеми, такі як конфлікт інтересів між користувачами мережі та основною групою розробників або джерелами фінансування.

Крім того, альтернативні структури управління, розроблені для кращого узгодження інтересів різних груп, можуть мати інші вразливі місця, що кореняться в їх конструкції.

Смарт-контракти, які широко використовуються в багатьох публічних блокчейнах, також несуть ризики, оскільки вони поєднують у собі властивості незмінності та публічного перегляду. У сукупності ці атрибути створюють кілька вразливостей, які можуть бути використані зловмисниками для крадіжки коштів клієнтів: як тільки зловмисник знаходить помилку в смарт-контракті і використовує її, незмінні протоколи обмежують можливості розробників виправляти використану вразливість, даючи хакерам більше часу для використання вразливості та викрадення активів.

У міру того, як цифрові активи у Blockchain стають все більш популярними, неминуче зростають і кількість зломів, зараження програмами-вимагачами та інші ризики для кібербезпеки. За оцінками Immunefi, злочинність, пов’язана з

Blockchain, може бути найвищою за весь час. Лише за 3 квартал 2022 року шахраї викрали рекордні 428,7 мільйони доларів США [25]. Хакерські атаки залишаються основною причиною збитків порівняно з шахрайством. Аналіз збитків показує, що на шахрайство припадає лише 7% (9 інцидентів на суму приблизно 29,8 млн. доларів США) загальних збитків у третьому кварталі 2022 року, а на зломи – 93% (близько 398,9 млн. доларів США за 30 інцидентів).

Частіше всього зламують смарт-контракти на таких блокчейнах:

- BNB Chain - 28,6%;
- Ethereum — 23,2%;
- Solana — 7,1%.

Це пов'язано з їх популярністю та слабким захистом частини проектів, оскільки створювати свій продукт на цих блокчейнах нескладно.

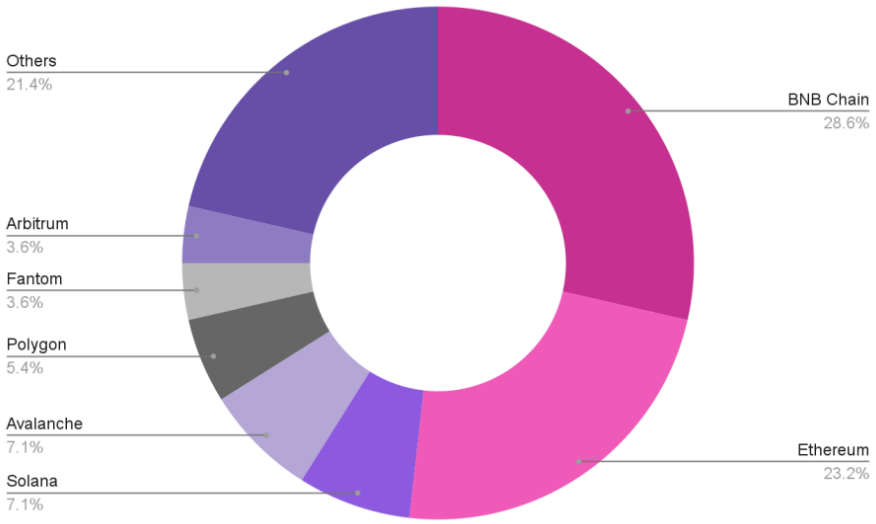

Рис. 2.2. Частка злому різних блокчейнів протягом третього кварталу 2022 року за даними Immunefi

BNB Chain, як і раніше, приваблює спільноту розробників, які створюють безліч копій протоколів Ethereum, а також приваблює безліч користувачів, які бажають швидко заробити. Розгалужений код може містити вразливості, і вже були випадки, коли розробники BNB Chain модифікували розгалужений код без особливих знань про базову структуру програми, що вводить нові вразливості, які потім використовуються.

Крім того, багато традицій і культур безпеки, що існують у спільноті розробників Ethereum, ще не існують у спільноті BNB Chain. Вразливості, які все рідше зустрічаються в протоколах Ethereum, як і раніше, виникають у ланцюжку BNB. З часом, якщо BNB Chain вдасться залучити більш серйозних талановитих розробників, ці традиції безпеки зрештою зростатимуть.

Рідко можна знайти один метод атаки на основі смарт-контрактів, який однаково впливає на всі різні ланцюжки проекту, але ці випадки не є винятком. З Impermax Finance вектором атаки була компрометація закритого ключа, яка торкнулася гаманців команди у різних ланцюжках. Це не був експлойт смарт-контракту, який дозволяв хакеру виводити кошти з контрактів у різних ланцюжках. У Celer Network експлойт був DNS-атакою, яка дозволяла зловмиснику перенаправляти користувачів на зовнішній інтерфейс Celer, контрольований цим хакером. Як тільки користувачі взаємодіяли з цим створеним інтерфейсом хакерами, незалежно від ланцюжка, їх засоби зникали.

Загалом, за перші три квартали 2022 року хакерами було викрадено близько 2,32 млрд. доларів США.

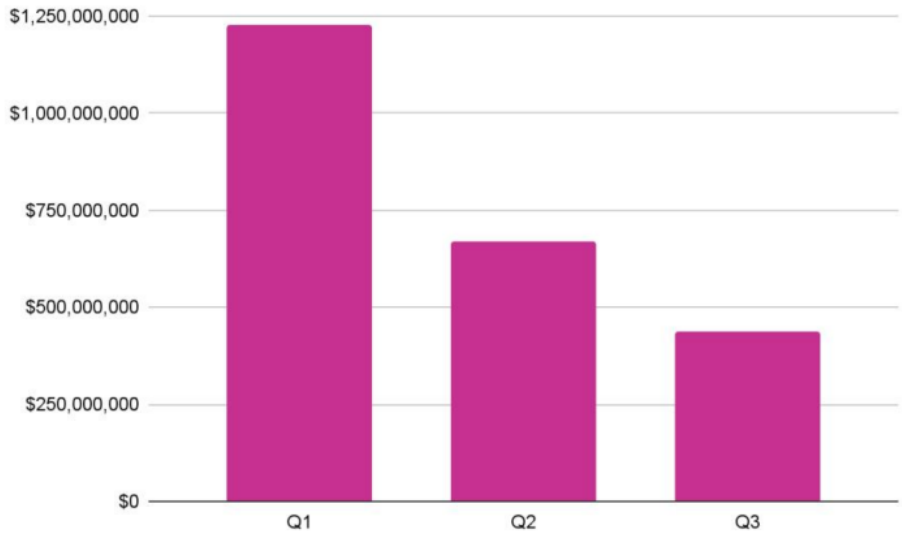

Рис. 2.3. Розміри збитків у Blockchain за перші три квартали 2022 року

Варто зазначити, що за 2022 рік DeFi продовжує залишатися ключовою ціллю для експлойтів в порівнянні з CeFi. DeFi складає 98,8% від загальних збитків, а CeFi - 1,2% від загальних збитків.

Зламати централізовану біржу, таку як Binance та Coinbase, складніше, оскільки вони вклали багато ресурсів у безпеку. Враховуючи їх базові налаштування інфраструктури, для виведення грошей із централізованої біржі хакерам часто потрібно долати набагато більше перешкод, ніж для виведення грошей з протоколу DeFi. Іншими словами, вразливі проекти DeFi є набагато легшим видобуванням для зловмисних хакерів, і влада з меншою ймовірністю буде залучена до процесу злому безіменного протоколу. Також існує набагато більше протоколів DeFi, ніж централізованих бірж або проектів CeFi, що призводить до значно більшої поверхні для атак. Тому користуватись своїми активами краще на централізованих біржах.

Аналіз особливостей зберігання та захисту цифрових активів у Blockchain

1 Захист приватних ключів інвесторів від втрати

У мережі Blockchain приватні ключі є єдиним способом ідентифікації власника цифрового активу. Будь-хто, хто володіє закритим ключем до Blockchain адреси, матиме повні права власності на цей цифровий актив, тобто втрата закритого ключа публічної адреси блокчейнах без дозволу дорівнює втраті всіх активів на цій адресі.

Щоб вирішити цю проблему для користувачів у мережі DLT без дозволу або платформи токенізації, розробляються додаткові технології. Такі методи, як токен ERC-721, дозволяють записувати та перевипускати токени цифрових активів у разі втрати або крадіжки приватних ключів. Власники токенів у дозволених мережах мають гарантію доступу до «головних ключів» (іноді відомих як «seed-фрази»), які використовуються для створення всіх приватних і відкритих ключів у мережі.

Однак ризик втрати приватних ключів, що призводить до втрати активів у дозволених мережах DLT або платформах токенізації, зменшується головним чином завдяки заходам управління та контролю. Фактично, найбільш очевидним засобом зменшення ризику є той факт, що дозволена мережа є закритою. Це

означає, що можливість «записувати» інформацію в реєстр і досягати консенсусу щодо дійсності транзакцій обмежена групою попередньо схвалених учасників.

Ще одна послуга, яку можна запропонувати, — це зберігання «криптографічного насіння». У двох словах, блокчейни — це в основному список пов'язаних списків транзакцій, кожен з яких прив'язаний до попереднього за допомогою криптографії. Ці рішення дозволяють учасникам розміщувати інформацію в цифрових гаманцях, доступ до яких контролюється асиметричною криптографією, яка складається з відкритого ключа, який зазвичай використовується як адреса або гаманець, і закритого ключа, еквівалентного паролю, що дозволяє авторизувати транзакції. У разі втрати закритого ключа його можна відновити шляхом застосування хеш-функції до послідовності впорядкованих слів, які знає лише учасник, якому належить адреса. Ця послідовність відома як «криптографічне насіння» або «seed-фраза».

Оскільки seed-фраза діє як резервна копія, вона повинна зберігатися безпечно. Її можна охороняти як зашифровано у цифровому вигляді, так і фізично. В обох випадках довірена третя сторона повинна зберігати це «насіння».

2.3.2 Зберігання самого цифрового активу

Якщо інвестор просить зберігача або центральний депозитарій(ЦД) зберігати лише приватні ключі, зберігач або центральний депозитарій не має права доступу до самих цифрових активів. Інвестори можуть контролювати доступ до валют у Blockchain так само, як клієнти банку можуть контролювати доступ до елементів у своєму банківському сховищі. Зберігач або його центральний депозитарій, який володіє лише особистими ключами, не може гарантувати безпеку фактичних активів або підтвердити, що інструкції щодо передачі надійшли від інвестора. В принципі, будь-хто, хто знає ваш закритий ключ, може передати ваші цифрові активи.

Зберігання фізичних активів у зберігача або центрального депозитарію є більш безпечною альтернативою, яка краще відображає реальність послуг, які

пропонуються на ринку. У цьому випадку інвестори передають цифрові активи на адресу цифрового гаманця зберігача разом із можливістю прямого доступу та передачі активів. Приватні ключі зберігаються лише у адміністратора або його центральному депозитарії цінних паперів (CSD). Цифровий гаманець, наданий зберігачем або його центральним депозитарієм, може бути адресою окремого гаманця (якщо цифрові активи зберігаються від імені інвестора) або адресою загального гаманця (якщо цифрові активи кількох інвесторів змішані).

Клієнти можуть купувати та продавати цифрові активи, використовуючи існуючі механізми автентифікації, і отримувати доступ до зберігача або її системи ЦД для видачі інструкцій щодо переказу. Автентифікація може підтримуватися різноманітними усталеними технологіями, адаптованими до епохи цифрових технологій. До них належать порогові підписи (як працює двофакторна автентифікація, коли можливість створювати підписи розподілено між кількома пристроями) або використання кількох підписів (вимагають кількох приватних ключів для авторизації транзакції).

Щоб досягти успіху, зберігачі та центральні депозитарії повинні будуть співпрацювати з правоохоронними органами, де торгують цифровими активами, і працювати разом, щоб полегшити рух активів до та з правоохоронних органів. Це дозволяє їм підтримувати клієнтів, які хочуть торгувати та розраховуватися на кількох торгових майданчиках.

Ризик бути зламаним, звичайно, не є специфічним для активів, які випущені та зберігаються в мережах DLT. Цінні папери, що зберігаються в цифровій формі в центральних депозитаріях і банках-зберігачах, однаково вразливі до крадіжки хакерами. Тим не менш, цифрові активи у Blockchain створюють нові ризики. Смарт-контракти, у яких договірні зобов’язання виконуються автоматично, помилки яких важко виправити, є одним із прикладів, що посилюється юридичною невизначеністю смарт-контрактів.

Зберігачі та центральні депозитарії між ними виконують два життєво важливі обов’язки на ринках цінних паперів. По-перше, захистити інвесторів від ризику втрати їхніх активів і прав, які належать до цих активів. По-друге, забезпечити

безперешкодний доступ до них, коли вони хочуть продати або передати заставу. Вони добре підходять для виконання тих самих обов’язків на ринках активів у Blockchain.

Зрештою, забезпечення належного правового титулу та забезпечення дійсності та повної автентифікації переказів — це методи, які зберігачі та центральні депозитарії об’єднали для надання інвесторам цінних паперів протягом тривалого часу. Що ще важливіше, їх виконання також може допомогти інвесторам у цифрові активи у Blockchain дотримуватися існуючих законів і правил, які так само безумовно застосовуються як і до цих активів, так і до цінних паперів.

2.3.3 Різновиди цифрових гаманців

Іншою важливою концепцією екосистеми цифрових активів є їх зберігання у цифровому гаманці. Цифровий гаманець — це програмний додаток, апаратне забезпечення або інший пристрій та служба, в яких зберігаються відкриті та закриті криптографічні ключі користувача, які дозволяють користувачам взаємодіяти з одним або декількома ланцюжками блоків, а також відправляти та отримувати цифрові активи.

Відкритий ключ — це криптографічна адреса, якою користувач ділиться з іншими користувачами в блокчейні для транзакцій з криптоактивами, і він має бути пов'язаний із закритим ключем користувача для підтвердження права власності на криптоактиви та авторизації транзакцій.

Закритий ключ – це криптографічний пароль, необхідний для доступу до криптоактивів, пов'язаних з адресою гаманця, і тому його слід зберігати у безпеці [26].

Цифрові активи користувача у Blockchain не зберігаються в гаманці, а натомість записуються у блокчейні та можуть контролюватись лише за допомогою закритого ключа користувача. Гаманець може бути сумісний з одним конкретним ланцюжком блоків (одноланцюжковий гаманець) або може підтримувати інформацію з кількох різних ланцюжків блоків (багатоланцюжковий гаманець).

Цифрові гаманці бувають трьох різновидів, кожен з яких забезпечує різний баланс між безпекою та ліквідністю.

Деякі цифрові гаманці зазвичай вимагають використання підключеного до Інтернету обладнання для отримання та передачі базової інформації. Хоча доступність гаманців, безпосередньо підключених до Інтернету («гарячі гаманці»), робить їх більш зручними для користувача, вони також можуть бути більш вразливими для крадіжки та шахрайства, і тому становлять більше ризиків для користувачів. Проте, цифрові активи, які на них зберігаються, доступні онлайн для негайної передачі.

Навпаки, «холодні гаманці» дозволяють користувачам зберігати свої закриті ключі на фізичному пристрої або іншому обладнанні, яке підтримується в автономному режимі, що робить його недоступним для спроб злому онлайн, але яке можна підключити до мережі для транзакцій. Залежно від зберігання, холодний гаманець також може бути вразливим для втрати, крадіжки, пошкодження чи знищення. Так само, як фізичні гаманці можуть бути втрачені або вкрадені, гаманці з цифровими активами можуть бути зламані, закриті ключі можуть бути втрачені або скомпрометовані, що призведе до втрати коштів або облікових даних.

Апаратний модуль безпеки (HSM) або апаратний гаманець – це спосіб зберігання закритих ключів, який ніколи не залишає фізичний пристрій. Будь-яка функція, яка вимагає доступу до цих ключів, працює безпосередньо на цих пристроях і підтримується додатковими функціями безпеки, такими як двофакторна автентифікація або персональні ідентифікаційні номери (PIN-код). Транзакції завжди підписуються на іншому пристрої, тож закритий ключ ніколи не піддається хакерам. Однак передача цифрових активів із таких «холодних» гаманців є більш громіздкою та трудомісткою, а також перешкоджає миттєвій передачі ліквідності.

На додаток до «гарячих» і «холодних» цифрових гаманців існують гібриди, відомі як «теплі» гаманці. Найпопулярніші з них можуть отримувати цифрові активи з будь-якої відкритої адреси, але можуть передавати цифрові активи лише на обмежений список (зазвичай «холодних») адрес гаманців. Їхня робота схожа на

роздрібний депозитний ощадний рахунок, вміст якого можна перенести лише на роздрібний чековий рахунок того самого інвестора. Це забезпечує певний рівень ліквідності, одночасно знижуючи ризик шахрайського переказу невизначеним сторонам.

Через регулярні хакерські атаки, пов’язані з «гарячими» гаманцями, доцільно вибрати «холодні» гаманці. Таким чином користувач усуває контрагентів, які потенційно можуть втратити його кошти. Це також зменшує ймовірність втрати активів користувача через збій комп’ютера, спричинений вірусами чи іншим шкідливим програмним забезпеченням.

Тим не менш, ці аргументи не пом’якшують їхній очевидний недолік. По-перше, він не підходить для частого використання. Іншими словами, це не ідеальне рішення гаманця для людей, які, ймовірно, часто будуть виконувати транзакції. Для таких людей найкраще використовувати обидва типи гаманців. Рекомендується зберігати основну частину своїх коштів у холодному гаманці, а невеликий відсоток відправити у гарячий гаманець для торгівлі на біржах або виконання миттєвих транзакцій.

Оскільки, описані попередньо методи також є не повністю надійними, на даний момент існує необхідність у більш захищених рішеннях для збереження цифрових активів у Blockchain.

Висновки до другого розділу

Досліджено ризики щодо використання та зберігання цифрових активів у Blockchain. Виокремлено основні види ризиків, а саме: ризики поведінки та шахрайство; ризики впливу на уразливі групи населення; операційні ризики; традиційні фінансові ризики, такі як ризики ресурсів і можливостей та ризики щодо зберігання.

Досліджено проблеми захисту і безпеки цифрових активів від злому та шахрайства. Зроблено висновок, що Blockchain та суміжні технології є формами комп'ютерного програмного забезпечення і схильні до уразливостей програмного

забезпечення. Проаналізовано дані щодо злочинності, пов'язаної з Blockchain, протягом перших трьох кварталів 2022 року, показано суми зломів та частки злому різних блокчейнів за цей період. Визначено, що сектор децентралізованих фінансів DeFi є основною ціллю для хакерів на даний момент.

Проаналізовано різні методи та засоби для зберігання цифрових активів у Blockchain. Зроблено висновок, що найбільш популярні способи для безпечного збереження цифрових активів є не повністю надійними та потребують нових комплексних рішень для забезпечення безпеки.

3 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВИХ АКТИВІВ У BLOCKCHAIN НА ОСНОВІ РІШЕННЯ GNOSIS SAFE

3.1 Дослідження рішення Gnosis Safe, основні переваги та можливості

Більшість користувачів цифрових активів у Blockchain, наприклад ті, хто володіє ETH або BNB, звикли до гаманця з одним ключем, який часто називають зовнішнім обліковим записом (EOA) або цифровим гаманцем. Це наприклад: MetaMask, Trustwallet, Exodus тощо. Ці облікові записи захищені «початковою фразою» з 12 слів, яку можна перетворити на приватний ключ для користувача. Якщо цей закритий ключ будь-яким чином скомпрометовано, кошти можуть бути викрадені.

Якщо у проекті працює більше ніж 1 особа, цифровий гаманець не є безпечним способом для керування коштами бізнесу. Якщо працівник зловживає чи недбало поводиться із закритим ключем, кошти зникають назавжди. Навіть якщо бізнес складається лише з однієї особи, зберігання активів на одному гаманці це поганий спосіб управління коштами. Таким чином виникає необхідність у використані нових технологій та способів збереження цифрових активів.

Технологія мультипідпису або Multi-Signature допоможе підвищити рівень безпеки цифрових активів. Gnosis Safe — це розумний контрактний гаманець, який працює на кількох блокчейнах і вимагає мінімальної кількості людей для схвалення транзакції перед її здійсненням (M-of-N) [27]. Наприклад, якщо у бізнесі є 3 основні зацікавлені сторони, можна налаштувати гаманець таким чином, щоб він вимагав схвалення від 2 із 3 (2/3) або від усіх 3 людей перед відправленням транзакції. Це гарантує, що жодна особа не може скомпрометувати кошти.

Порівняння основних можливостей та переваг Gnosis Safe з іншими рішеннями для зберігання цифрових активів:

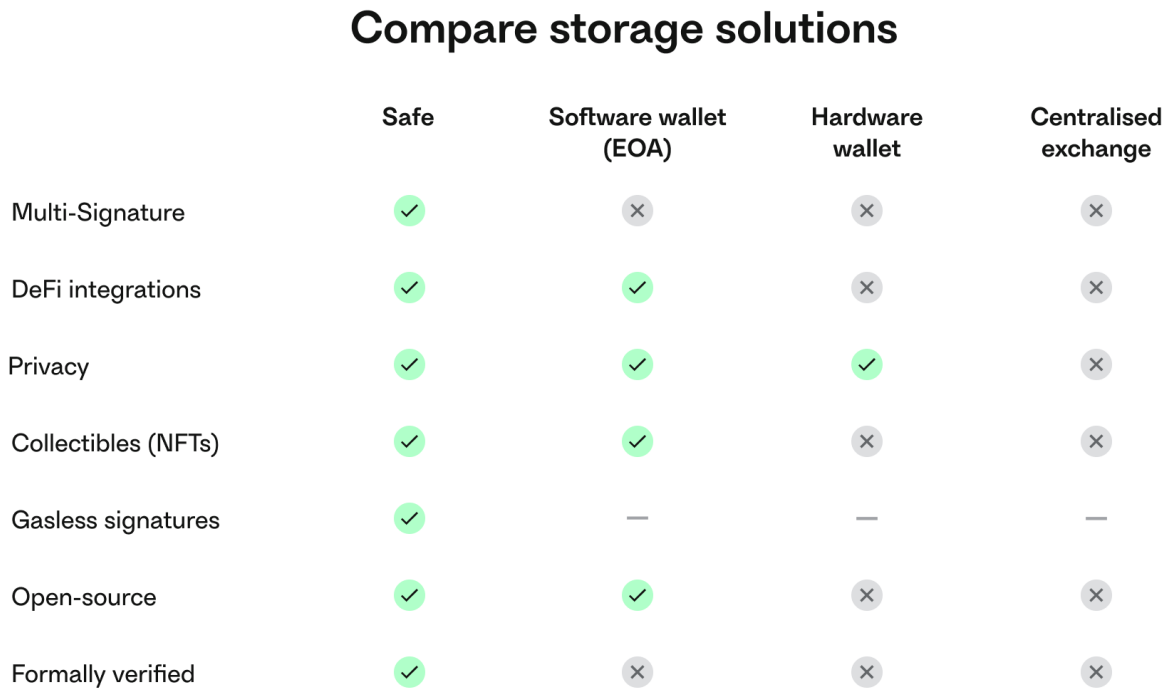

Рис. 3.1. Порівняння Gnosis Safe з іншими рішеннями для зберігання цифрових активів

Основна мета Gnosis Safe – це забезпечення надійного захисту активів користувачів. Функціональність Safe з використанням технології мультипідпису дозволяє визначити список облікових записів власників і порогову кількість підписів, які необхідні для підтвердження транзакцій.

Існує два види облікових записів: зовнішні облікові записи (externally owned accounts, або EOAs) та контрактні облікові записи.

На сьогодні більшість облікових записів, створених у мережі Ethereum, підпадають під категорію зовнішніх облікових записів. Іншими словами, EOA — це облікові записи Ethereum, які використовують традиційні пари ключів. Тобто вони складаються з одного закритого ключа, який можна використовувати для здійснення транзакцій і підпису повідомлень. Якщо зловмисник або стороння особа отримає доступ до цього закритого ключа, то він отримає повний контроль над обліковим записом. Найбільш популярні гаманці, такі як Metamask або imToken, є простими EOA, і навіть апаратні гаманці, такі як Ledger Nano або Trezor, засновані

на EOA. Це означає, що між користувачем та втратою його коштів стоїть лише закритий ключ — єдина точка відмови.

Іншим типом облікових записів Ethereum є облікові записи смарт-контрактів. Як і EOA, облікові записи смарт-контрактів мають унікальну загальнодоступну адресу Ethereum, і їх неможливо відрізнити від EOA, дивлячись на адресу Ethereum. Рахунки смарт-контрактів також можуть отримувати кошти та здійснювати транзакції, як EOA. Загалом ключовою відмінністю є те, що для перевірки транзакцій не використовується окремий закритий ключ. Натомість логіка того, як обліковий запис виконує транзакції, визначається в коді смарт-контракту. Розумні контракти — це програми, які працюють на Blockchain і виконуються, коли виконуються певні умови. Їхня функціональність у рамках контрактних рахунків означає, що такі облікові записи, на відміну від EOA, можуть, наприклад, реалізувати права доступу, які визначають, ким, як і за яких умов можуть виконуватися транзакції, а також більш складну логіку.

Гаманці з кількома підписами — це контрактні облікові записи, які вимагають від кількох сторін підтвердити транзакцію, перш ніж її можна буде виконати. Ці сторони, кожна з яких представлена унікальною адресою облікового запису Ethereum, визначені в розумному контракті як власники гаманця з кількома підписами. Лише коли попередньо визначена кількість цих власників підтвердить транзакцію, транзакцію буде виконано. Таким чином, єдина точка відмови, пов’язана з обліковими записами, керованими приватними ключами, видалена; втрата або компрометація закритого ключа більше не призводить до автоматичної втрати всіх коштів, які контролюються обліковим записом [28].

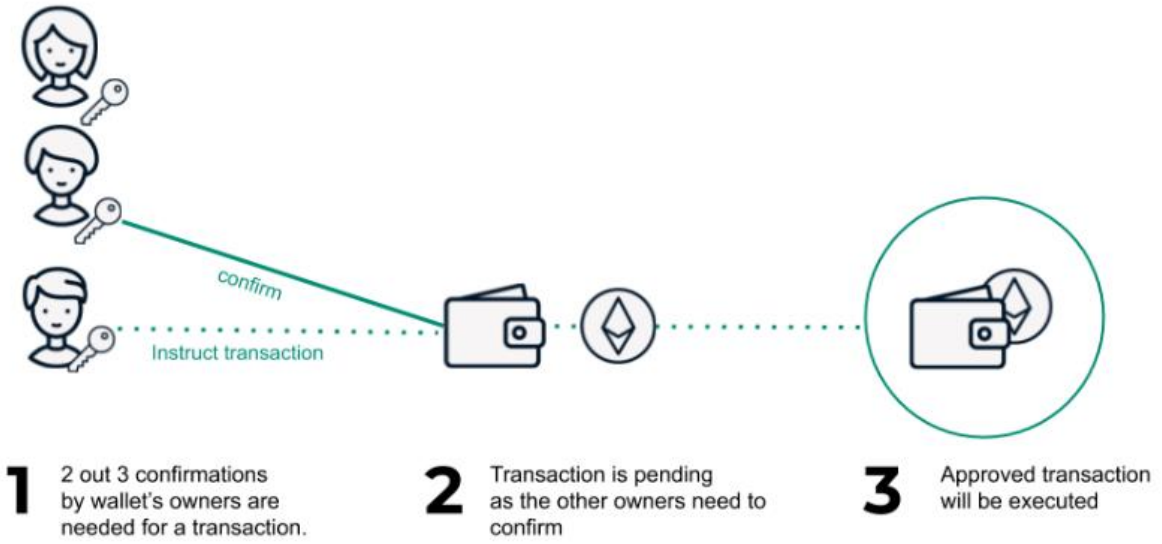

Рис. 3.2. Опис роботи гаманців з функцією мультипідпису

Ще однією з можливостей Gnosis Safe є розширена логіка виконання транзакцій, оскільки рішення дає змогу використовувати різні смарт-контракти та бібліотеки для виконання складних транзакцій. Приклад таких транзакцій може бути поєднання декількох невеликих транзакцій у блокчейні Ethereum в одну. Це дає змогу підписати лише одну пакетну транзакцію замість поступового підпису багатьох, що спрощує переказ активів та економить кошти на оплаті комісії мережі. Більш детально за функція буде розглянута у наступних розділах роботи.

Наступною функцією є можливість розширеного управління доступом. Дана функція дає можливість добавляти модулі до своїх сейфів, які називаються Gnosis Safe Modules. Вони забезпечують додаткову логіку контролю доступу для облікового запису Gnosis Safe. Завдяки цьому можна реалізувати більше тонке управління доступом.

По суті, кожен обліковий запис Gnosis Safe контролюється двома способами. Перший, це коли власники облікових записів використовують свої ключі підписувача, та додаткові модулі, які мають власну спеціальну логіку доступу.

Наприклад, може бути обліковий запис Gnosis Safe, яким керують 3 із 5 власників, і додатковий модуль, який дозволяє ключу адміністратора контролювати обліковий запис Gnosis Safe лише одним підписом.

Це вже підкреслює, що безпечні модулі Gnosis дуже важливі для безпеки, і їх мають додавати лише досвідчені користувачі, які повністю розуміють наслідки безпеки.

Ще один модуль безпеки дозволяє використовувати функцію зворотнього виклику токену. Деякі стандарти токенів вимагають від приймача реалізації функцій зворотного виклику. У Gnosis Safe це робиться через так званий резервний менеджер, який за замовчуванням підтримує зворотні виклики ERC721 і ERC1155. За потреби можна додати більше вручну.

Одною з найважливіших функцій Gnosis Safe є розрахунки без Ethereum, а саме оплата токенами. Як правило, транзакції в Ethereum потребують самого ж активу для оплати за газ, тобто для оплати комісії. За допомогою Gnosis Safe користовачі можуть оплачувати комісію за транзакції декількома іншими токенами стандарту ERC20. Ця функція реалізовується через службу ретрансляції транзакцій, яка приймає ці токени і відправляє транзакцію у блокчейн.

Станом на 8 лютого 2022 року на сейфах проекту зберігались цифрові активи на суму 107 млрд. дол. США.

На порталі Dune зберігаються статистичні дані балансів сховищ Gnosis Safe, які автоматично оновлюються кожної години [29].

Станом на 14 листопада 2022 року лише на блокчейні Ethereum створено понад 109 тис. сховищ, найбільші 25 з яких містять понад 1,3 мільйони ETH на балансі. Загальний баланс активів на усіх сховищах складає понад 1,7 мільйонів ETH, які дорівнють в сумі понад 2 млрд. дол. США в еквіваленті.

Рис. 3.3. Об’єднаний баланс ETH усіх контрактів Gnosis Safe

Gnosis Safe також позиціонує себе як рішення, яке відповідає найвищим стандартам безпеки.

Компанія виконує всі кроки для забезпечення максимальної надійності захисту цифрових активів користувачів. Для цього проект проводить регулярні аудити, одним з яких був ретельний аналіз смарт-контракту компанією Runtime Verification Inc [30].

Вся документація Gnosis Safe знаходиться на Github у відкритому доступі для того, щоб кожен користувач зміг перевірити актуальність та правдивість всієї інформації.

Хоча офіційний смарт-контракт був офіційно перевірений, компанія вирішила проводити ретельні перевірки та аудити кожного оновлення зовнішніми експертами безпеки. На сайті проекту можна знайти всі звіти щодо аудитів, та перевірити які були виявлені помилки [31].

Окрім цього на Gnosis Safe є функція, яка називається «Insurance by Nexus Mutual». Якщо користувачі сумніваються у безпеці смарт-контрактів, то вони можуть застрахувати свої активи, які зберігаються у Gnosis Safe від можливих атак на смарт-контракти через сервіс Nexus Mutual. Для того, щоб це зробити, потрібно

перейти по посиланню щодо цієї функції, яка знаходиться на сайті проекту в розділі «Security».

Також у проекта є програма «Bug Bounty», яка нагороджує програмістів на суму до 1 млн. дол. США за знайдені уразливості та помилки у коді. Дана програма працює з липня 2018 року.

Наразі Gnosis Safe підримує такі мережі:

- Ethereum Mainnet;
- Ethereum Testnets: Rinkeby, Kovan, Ropsten, Görli;
- Gnosis Chain (раніше xDai);
- Arbitrum;
- Aurora;
- Avalanche;
- Binance Smart Chain;
- Energy Web Chain;
- Energy Web Chain Testnet: Volta;
- Optimism;
- Polygon.

Команда Gnosis Safe не має можливостей для розгортання та повної зовнішньої та внутрішньої підтримки для всіх мереж на основі EVM. Весь вихідний код, пов’язаний із проектом, є відкритим. Розробники заохочують всіх розгортати канонічні версії контрактів Safe у відповідних мережах і самостійно запускати необхідні серверні та зовнішні частини.

Платформа Gnosis Safe у першу чергу направлена для збереження цифрових активів для компаній. Технологія Multi-Signature дає можливість надійнішого зберігання активів, оскільки потребує підпису наперед визначеної кількості облікових записів. Крім цього, рішення підходить і для використання звичайними користувачами, які переймаються за безпеку збереження своїх коштів або мають активи на значну суму коштів.

3.2 Створення облікового запису Gnosis Safe та його налаштування

Для того, щоб створити своє сховище Safe, яким користувач зможе керувати та у якому зберігати свої цифрові активи, потрібно зайти на офіційний сайт проекту, де на головній сторінці будуть запропоновані три види інтерфейсу: Web, Desktop та Mobile.

Після встановлення програми, або відкриття веб-інтерфейсу, насамперед потрібно підключити свій зовнішній обліковий запис (EOA) або цифровий гаманець. Для цього необхідно натиснути на кнопку Connect Wallet, яка знаходиться у верхньому правому куті програми, далі натиснути кнопку Connect.

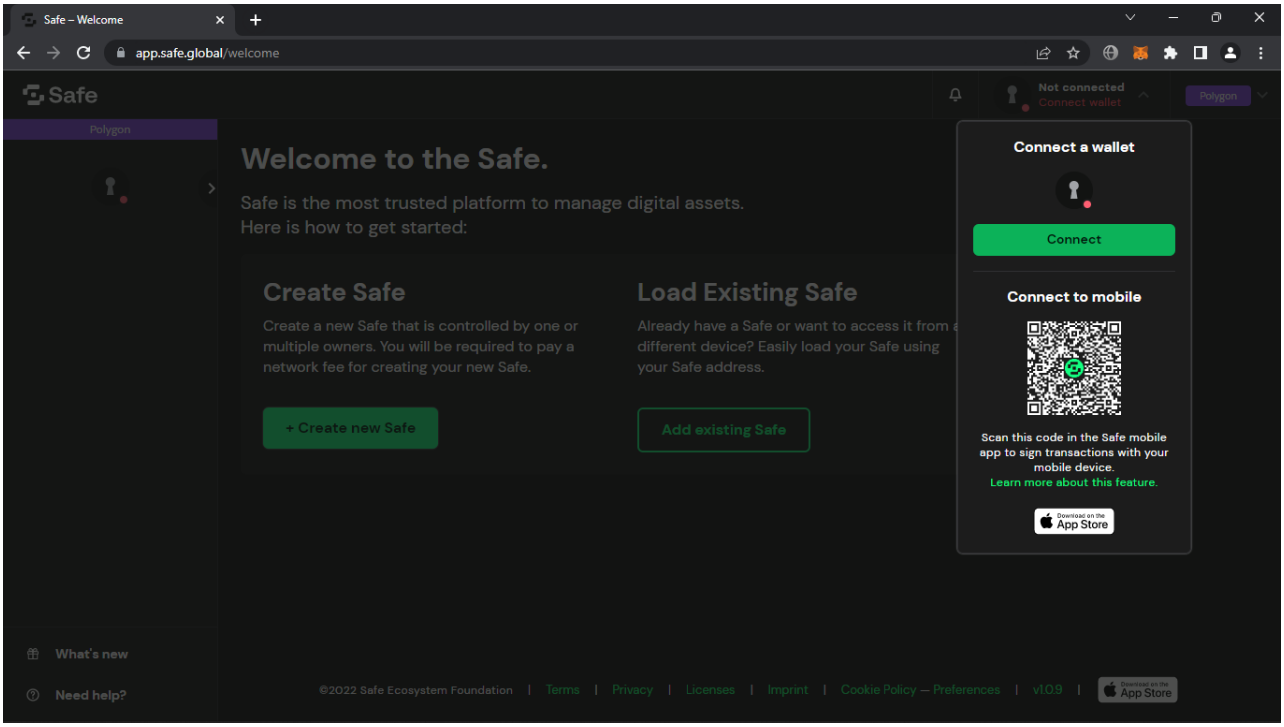

Рис. 3.4. Підключення зовнішнього облікового запису

Далі потрібно вибрати спосіб підключення цифрового гаманця. Серед доступних у програмі є підключення через сканування QR-коду, або підключення через сам Desktop. На даний момент момент програма підтримує підключення понад 20-и видів апаратних або цифрових гаманців, серед яких, наприклад, є одне з найпопулярніших рішень апаратних сховищ Ledger.

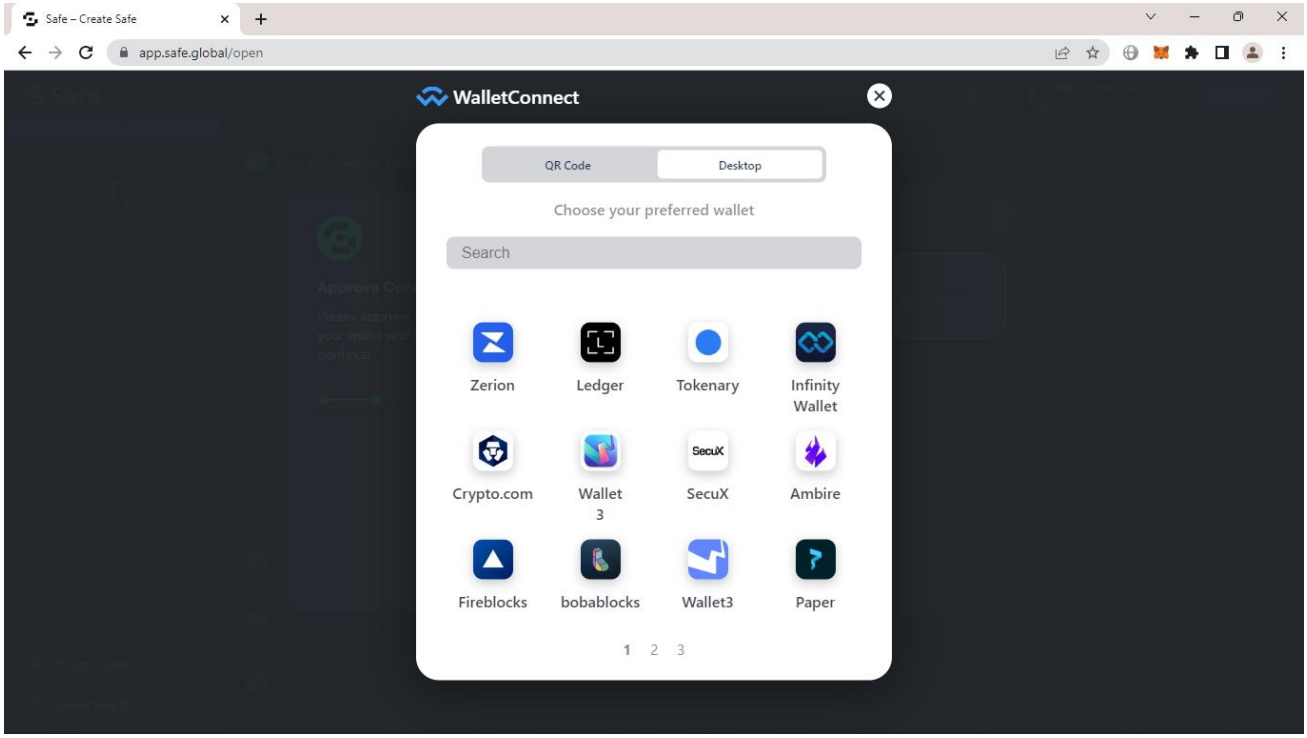

Рис. 3.5. Вибір способу та видів підключення цифрового гаманця

Після підключення потрібно потрібно натиснути кнопку Create new Safe. Першим кроком для створення сейфу є вибір правильної мережі. Це важливо, тому що сховище створюється лише для цифрових активів, які знаходяться на одному блокчейні. Для того, щоб зберігати цифрові активи, наприклад, у мережі Ethereum, а не на Polygon, необхідно буде створити інший сейф. Залежно від мережі ще потрібно переконатись, що на цифровому гаманці власника є власні активи цієї мережі, наприклад ETH, оскільки безпечне розгортання коштуватиме певної комісії за транзакції.

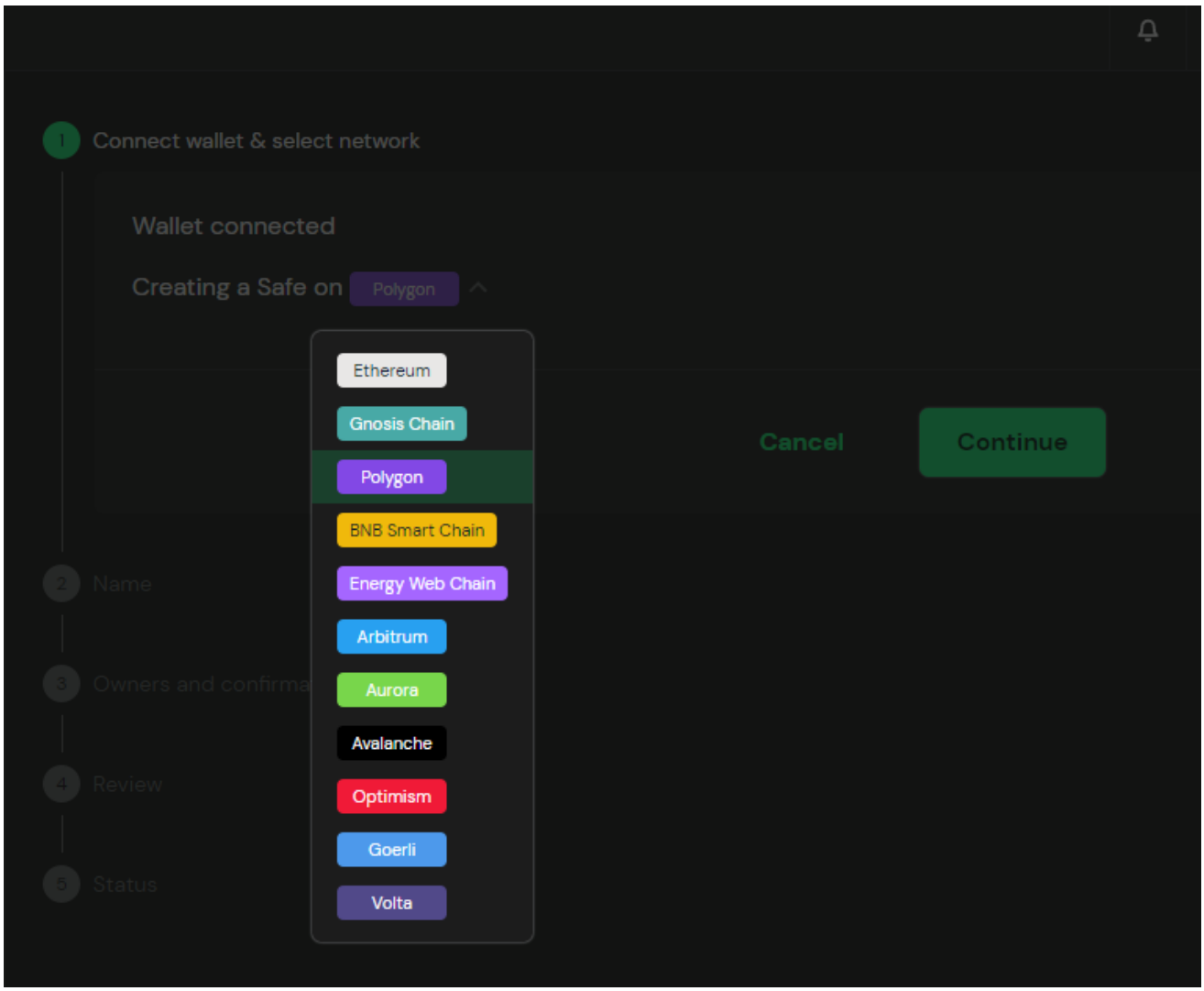

Рис. 3.6. Вибір правильної мережі для збереження активів

Наступним кроком, який необхідно зробити, це дати назву для свого сховища. Під час створення користувача ще раз попереджають, що новий сейф буде доступний лише для однієї мережі (для тестування була вибрана мережа Polygon). Після заповнення назви сховища у відповідному полі потрібно нажати кнопку Continue.

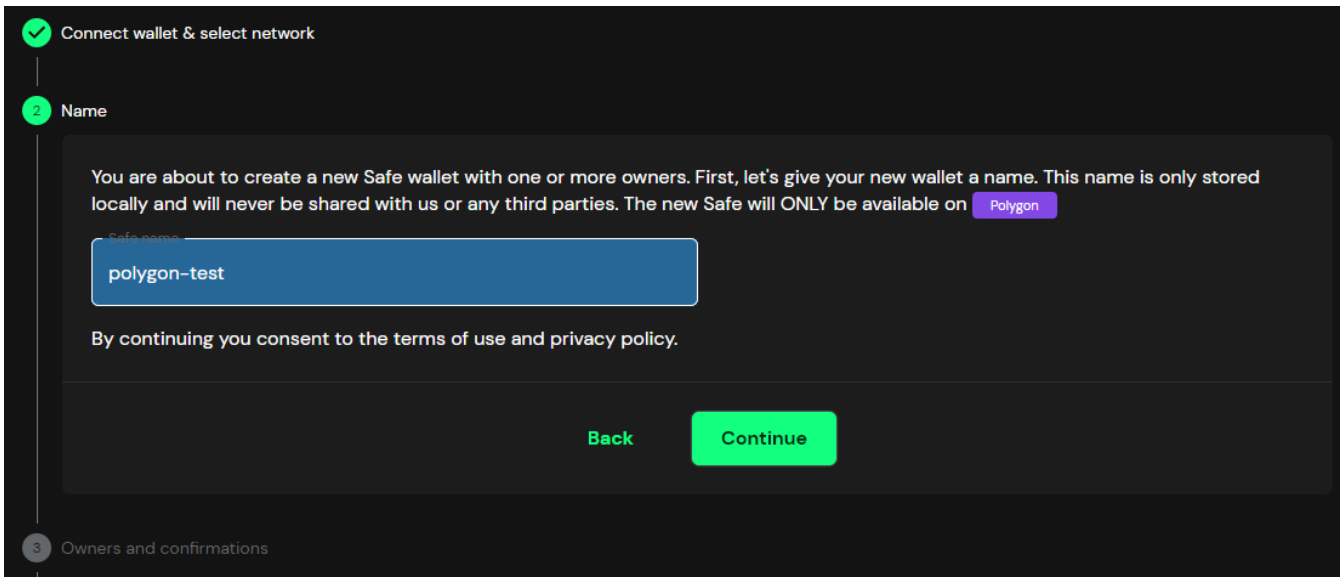

Рис. 3.7. Створення назви для сховища Gnosis Safe

Наступним, найбільш важливим кроком є вибір підписувачів, тобто адреси, які матимуть дозвіл на надсилання та затвердження транзакцій. Варто звернути увагу, що пізніше ці адреси можна видалити або змінити за необхідністю. Перший підключений гаманець підписувача автоматично буде добавлений як пропозицію для першого підписувача, але його також можна змінити. Gnosis Safe дає можливість добавляти скільки завгодно підписантів. Для мережі Ethereum є можливість додавати підписувачів за допомогою ENS. Це означає, що дана платформа підтримує ENS-адреси і цим можна скористатись, щоб не вставляти адресу цифрового гаманця вручну.

Ethereum Name Service (ENS) – це служба імен для адрес гаманців, хешів та інших ідентифікаторів у мережі Ethereum. Вона перетворює складні для читання рядки даних в легкі для читання адреси. Сервіс працює аналогічно системі доменних імен DNS, яка використовується для веб-сайтів.

Для більшої безпеки сховища рекомендується додавати більше підписувачів. Рекомендацією є додавати як мінімум три адреси, які зможуть підписати транзакцію, наприклад, два «гарячих» гаманці та один «холодний».

Наступним кроком, який необхідно зробити це визначити поріг підтвердження. Тобто, вибір кількості підтверджень підписувачів для транзакцій, або будь-яких змін налаштувань облікового запису в Gnosis Safe до того, як вони

будуть підтверджені. Це означає, що необхідно ретельно обдумати налаштування облікового запису. Тобто, якщо у користувачів буде недостатня кількість адрес з доступом для підпису, щоб досягнути порогового значення, вони не зможуть відновити свої активи.

Наприклад, при налаштуванні були вибрані 3 адреси для підпису, а в полі «будь-яка транзакція потребує підтвердження: » було вибрано три учасника із трьох. Це означає, що тільки після того, як три власника підтвердять транзакцію, наприклад, на переказ коштів за межі сховища, вона буде підтверджена. Якщо один із власників втратить доступ до свого апаратного гаманця, який був зареєстрований як підписант, це приведе до того, що цифрові активи усіх користувачів у сховищі будуть заморожені до тих пір, поки власник не знайде свій гаманець, або не відновить його по seed-фразі та знову отримає до нього доступ.

Це означає, що хорошим рішенням задля безпеки буде поставити порогову кількість підписів меншою, аніж загальна кількість підписантів. Наприклад, якщо було зареєстровано 3 адреси підписувачів, а необхідна кількасть підписів дорівнюватиме 2, то транзакція виконається тоді, коли її підтвердять двоє із трьох власників, незалежно від того, хто саме це зробить. Головне, щоб кількість підписів співпадала з налаштуваннями.

Дану функцію можна використовувати і для одного користувача задля безпеки власних активів. Наприклад, заради безпеки користувач створив сховище, а для підтвердження транзакцій додав два своїх цифрових гаманців. Якщо один із гаманців буде скомпроментовано, зловмисник дізнається seed-фразу, він отримає повний доступ до цього гаманця. Але провести будь-яку операцію у Gnosis Safe та заволодіти цифровими активами, які знаходяться у сховищі зловмисник ніяк не зможе, оскільки йому потрібен підпис другого цифрового гаманця, seed-фрази якого у нього немає. Це є дуже хорошим рішенням для безпеки власних цифрових активів.

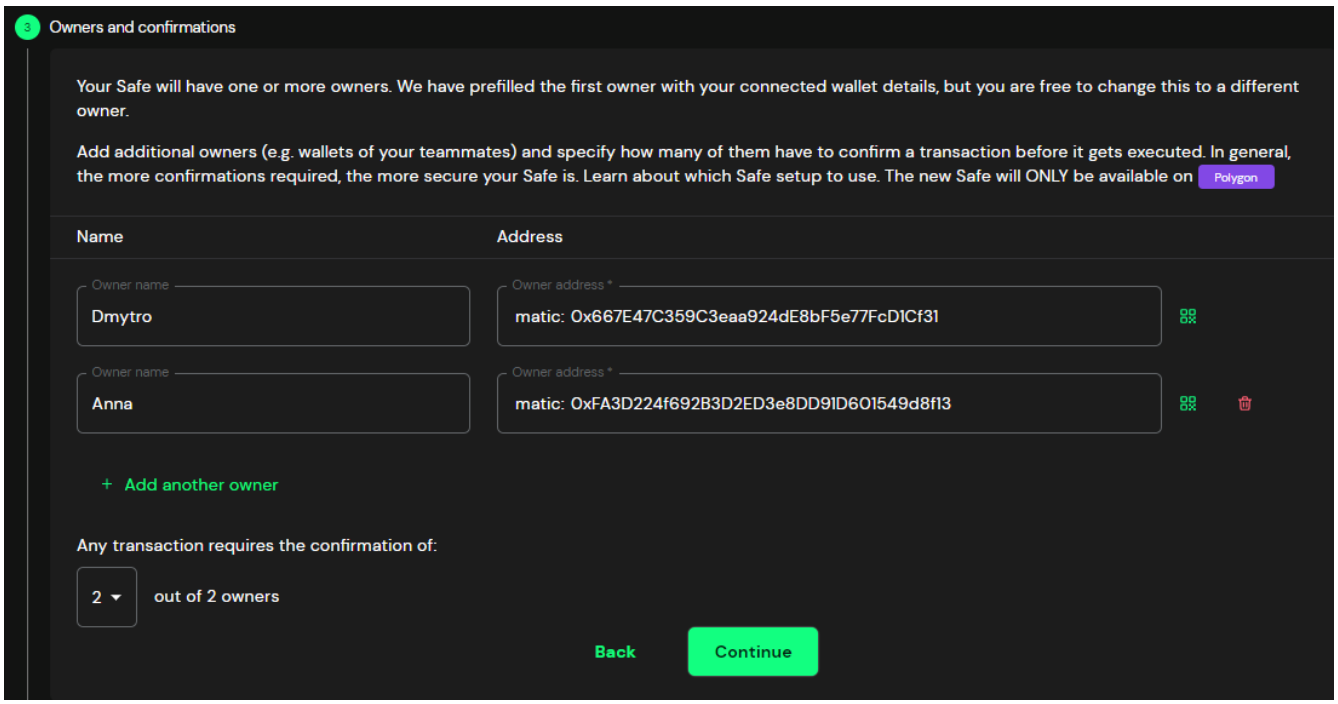

Рис. 3.8. Додавання імен та адреси підписантів під час створення сховища Gnosis Safe

Після заповнення необхідних даних потрібно натиснути кнопку Continue.

Далі користувачу дають змогу переглянути всі деталі майже створеного Gnosis Safe. Тут можна побачити назву нового сховища, інформацію про те, скільки підписувачів потрібно для того, щоб провести транзацію, а також інформація про наявних власників сейфу.

Нижче знаходиться інформація, яка повідомляє про те, що користувач хоче створити новий сейф у мережі Polygon, та попередження про те, що на початковому гаманці повинно бути трохи цифрового активу MATIC, щоб оплатити комісію. Оскільки будь-які операції у Blockchain записуються, а для запису необхідно заплатити основним активом мережі.

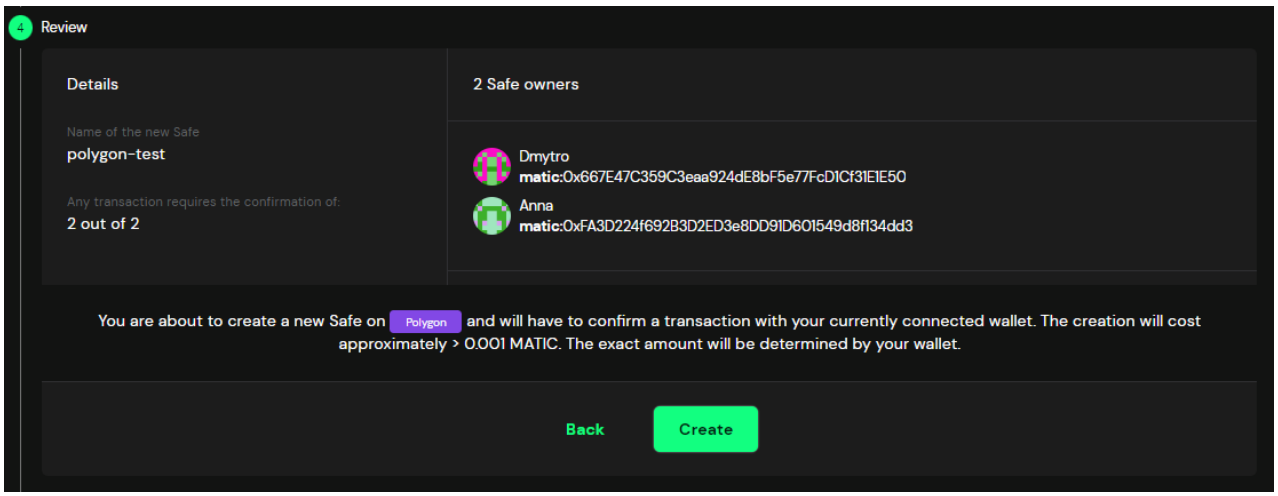

Рис. 3.9. Перевірка детальної інформації про Safe перед створенням

Після перевірки необхідно натиснути кнопку Create, після чого користувача відправить на сторінку підтвердження створення сховища. Як описувалось раніше, для цієї операції на основному гаманці повинно бути трохи MATIC для оплати комісію. Підтвердження операції та підпис транзакції відбувається через основний гаманець, який був зареєстрований на попередніх етапах, у даному випадку Metamask.

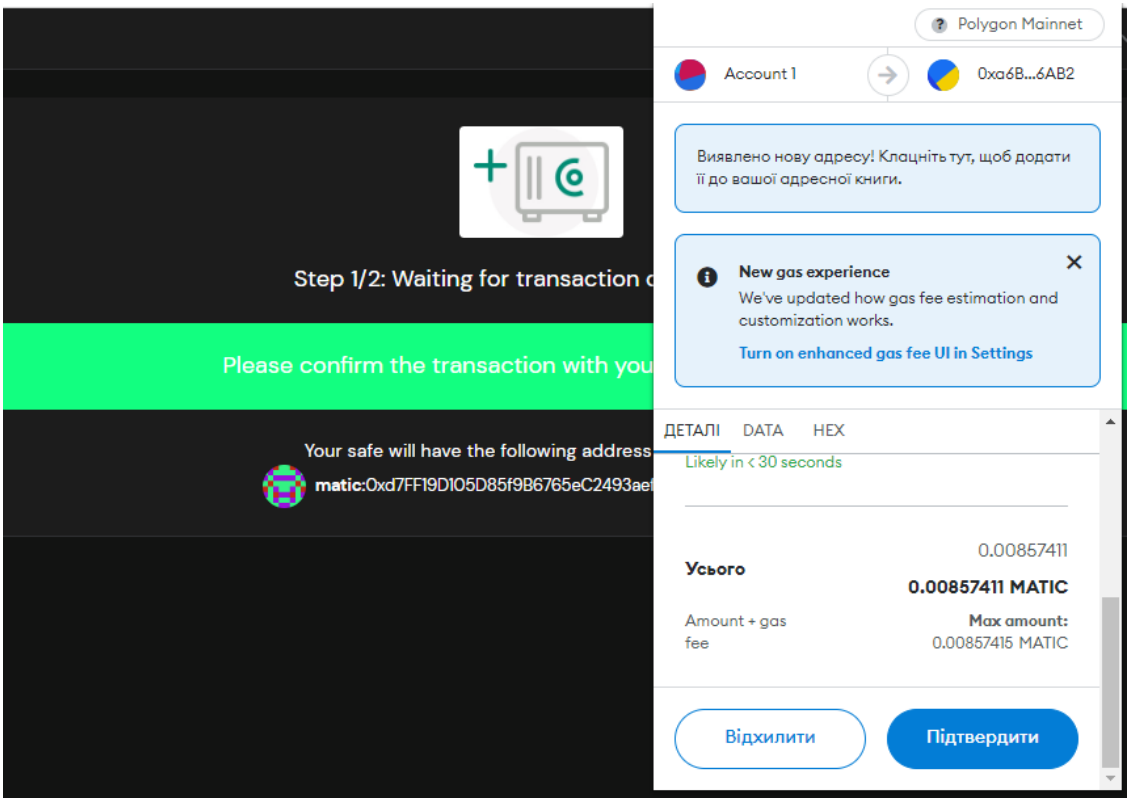

Рис. 3.10. Підтвердження створення Gnosis Safe через Metamask

Через декілька секунд операція буде записана у Blockchain, а нове сховище Gnosis Safe буде створено.

Отже, після проведеної роботи можна виділити декілька висновків.

По-перше, для підтвердження операцій рекомендується використовувати меншу порогову кількість підписів, аніж загальна кількість власників сейфу. Таким чином, навіть якщо один із власників втратить доступ до свого облікового запису, користувачі не будуть автоматично заблоковані для всіх своїх цифрових активів у сейфі. Незважаючи на це, інші власники все ще зможуть виконувати транзакції, та, наприклад, замінити цей втрачений обліковий запис власника на інший.

Для фізичних осіб розробники проекту Gnosis Safe рекомендують створювати сховища з трьома власниками, один з яких є «гарячим» цифровим гаманцем, наприклад Metamask, а два інші «холодні» апаратні гаманці, наприклад, Trezor або Ledger, та з пороговим значенням два із трьох. Тобто, Metamask разом із одним з апаратних гаманців використовується кожного дня для підписання та виконання транзакцій, у той час, як другий апаратний гаманець, зберігається у безпечному місці на випадок, якщо один із двох інших власників раптом втратить доступ до свого облікового запису.

3.3 Демонстрація роботи Gnosis Safe та опис функціоналу

Для того, щоб внести перші цифрові активи на своє сховище Gnosis Safe, користувачам потрібно відправити їх зі свого попереднього гаманця, використовуючи адресу сейфу. Адресу сховища можна знайти над основною панелю навінації у лівому верхньому куті інтерфейсу.

На даний момент доступні два види поповнення: просто через адресу сейфу, скопіювавши її, або за допомогою QR-коду. Більшість «гарячих» цифрових гаманців можна використовувати на своєму смартфонові, тому другий спосіб є більш зручним, швидшим та надійнішим для таких користувачів, оскільки при введені адреси вручну можна помилитись та неправильно її ввести, що приведе до втрати цифрових активів, які відправлятимуться.

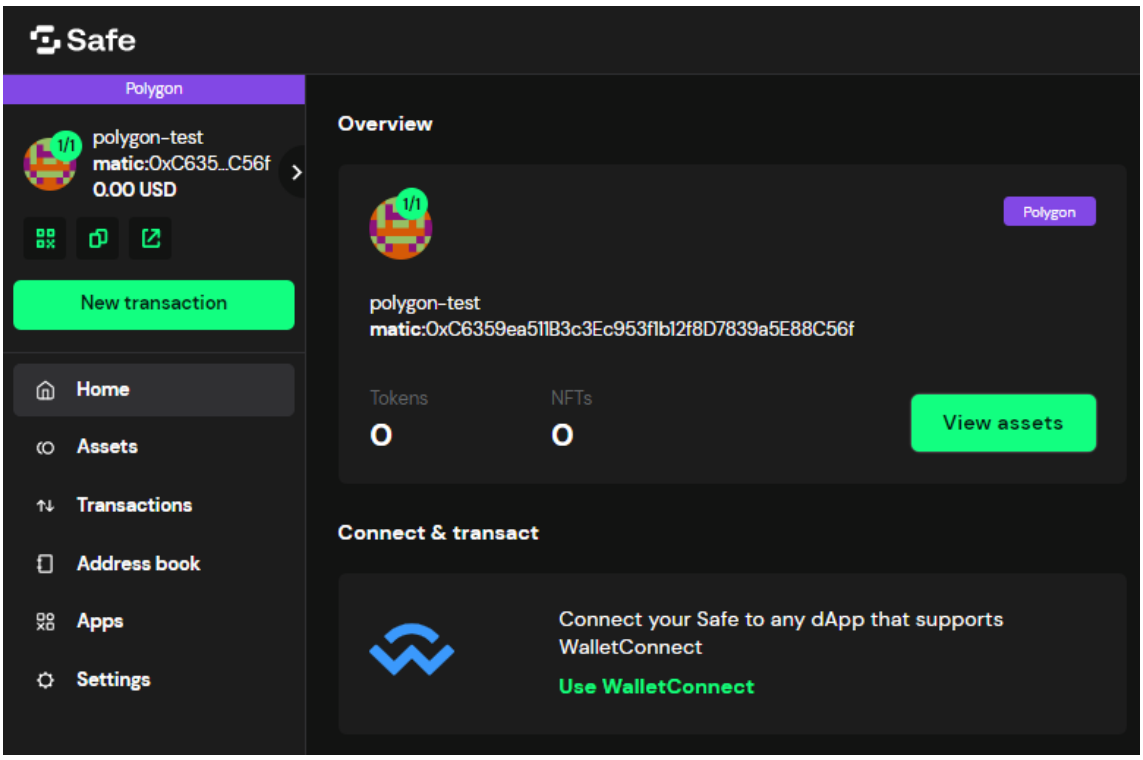

Рис. 3.11. Основна вкладка сховища Gnosis Safe

Окрім цього, на вкладці з QR-кодом користувачу буде написано попередження та нагадування про те, що на дану адресу, оскільки вона була створена на мережі Polygon, потрібно відправляти цифрові активи тільки даної мережі, а також токени, наприклад, ERC20 та ERC721.

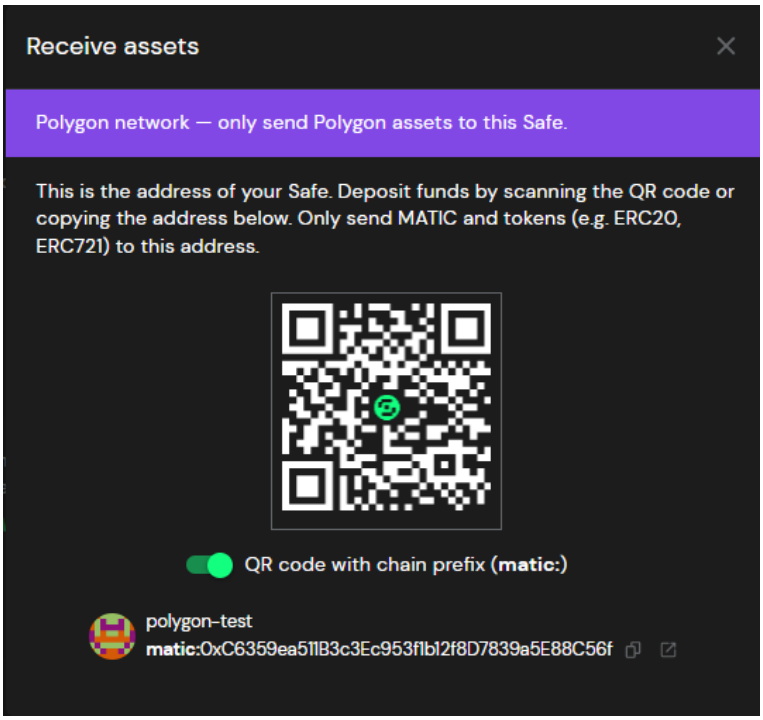

Рис. 3.12 Інтерфейс поповнення Gnosis Safe через QR-код

Якщо користувач відправить на дану адресу цифрові активи, наприклад, із мережі Bitcoin або Avalanche, то вони будуть назавжди втрачені.

Для поповнення раніше створеного сейфу буде використаний цифровий гаманець Metamask. Для цього потрібно відкрити інтерфейс Metamask, та натиснути кнопку Send.

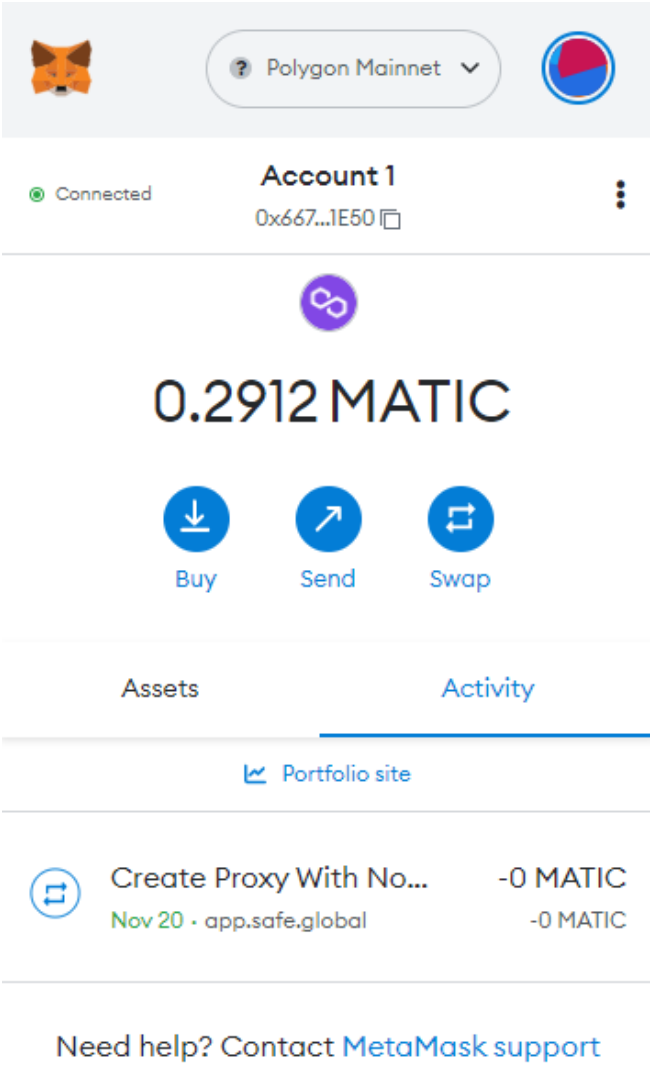

Рис. 3.13 Інтерфейс «гарячого» гаманця Metamask

Наступним кроком потрібно ввести адресу сховища Gnosis Safe, яка була раніше скопійована. Після цього необхідно вибрати цифровий актив, який потрібно буде надіслати (у даному випадку MATIC), а також кількість цього активу. Далі потрібно натиснути кнопку Next.

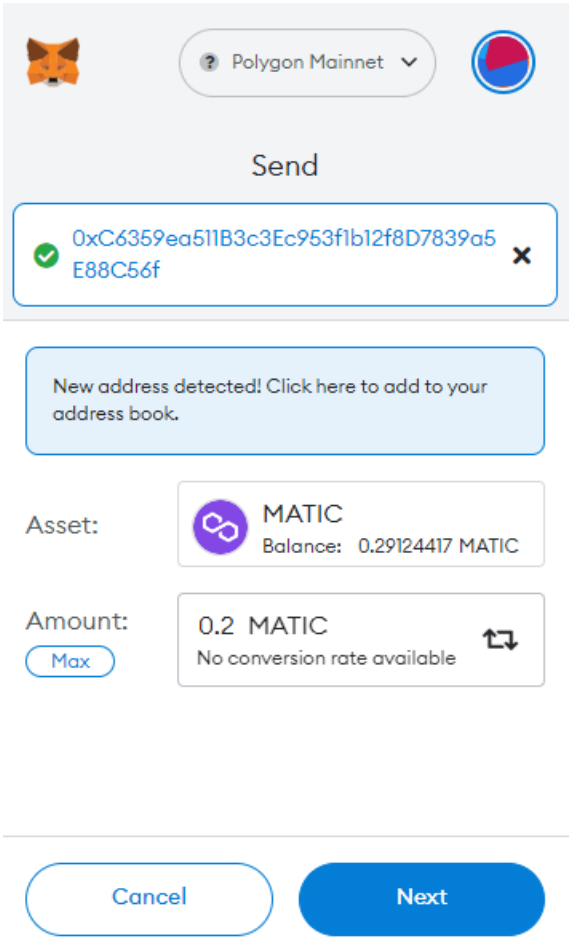

Рис. 3.14. Вибір цифрового активу для відправлення через Metamask

Далі користувача відправлять на вкладку підтвердження транзакції. Там ще раз буде описана кількість та вид цифрового активу, який відправляється, ціна за газ (оплата комісії) та кінцева сума, яку потрібно буде заплатити. Після перевірки правильності інформації потрібно натиснути кнопку Confirm.

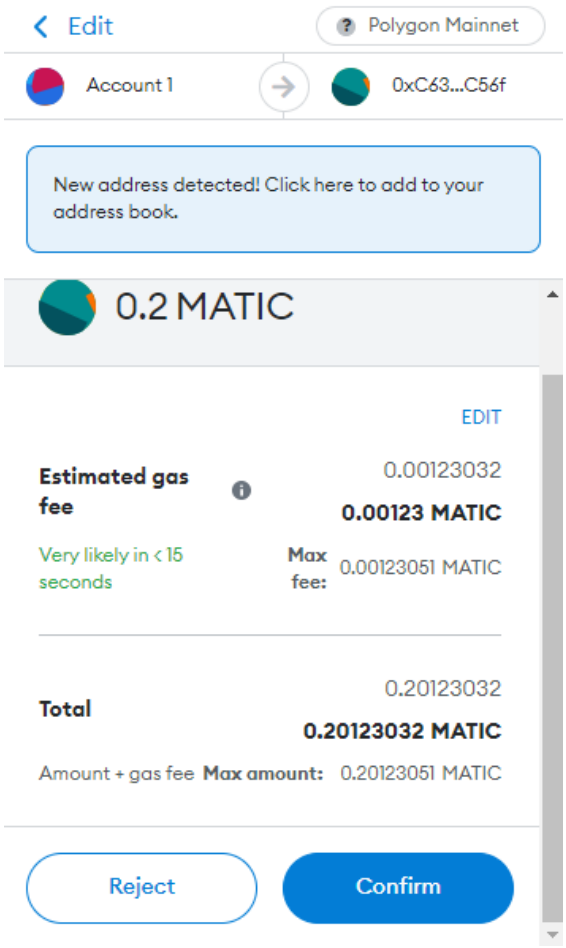

Рис. 3.15 Оплата та підтвердження транзакції через Metamask

Після обробки транзакції у Blockchain та її запису там, через декілька секунд цифрові активи надійдуть на сховище Gnosis Safe.

Перевірити всі деталі транзакції блокчейну Polygon, знаючи хеш даної транзакції, можна через сайт polygonscan. Хеш попередньо проведеної транзакції: 0x5b54dae037436cc5b62c610b05aace26fbf64b8367a31df97f19a50adec84297.

Серед інформації, там буде описаний номер блоку транзакції, її статус, час виконання, адреси гаманців відправника та отримувача, а також кількість надісланого активу, комісії та їх вартість.

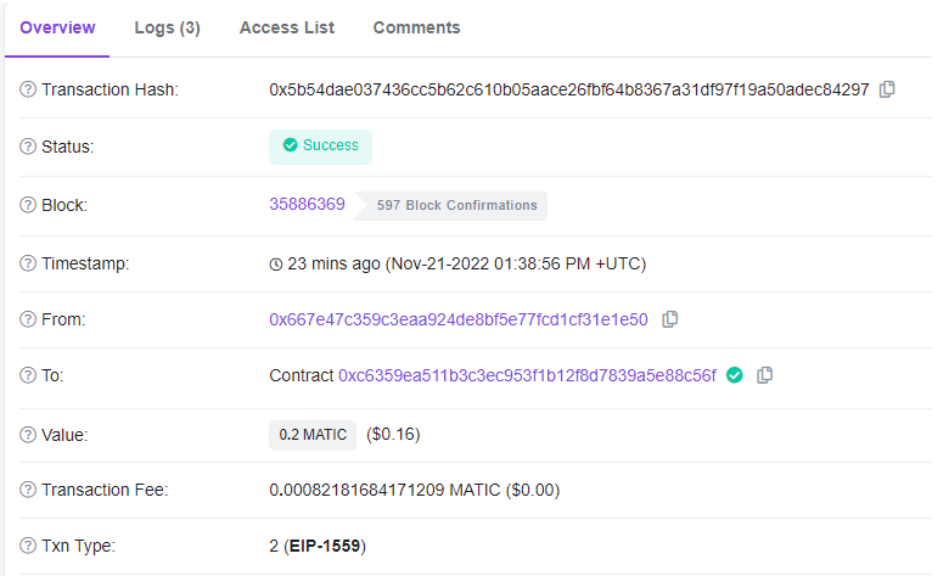

Рис. 3.16. Деталі транзакції через сканер polygonscan

Перевірити кількість на наявність будь-якого цифрового активу у сейфі можна через другий розділ навігації, а саме через кнопку Assets. Окрім опису активу та його кількість, у даній вкладці є можливість перевірити вартість цих активів по відношенню до національних валют, наприклад, долару США, або української гривні.

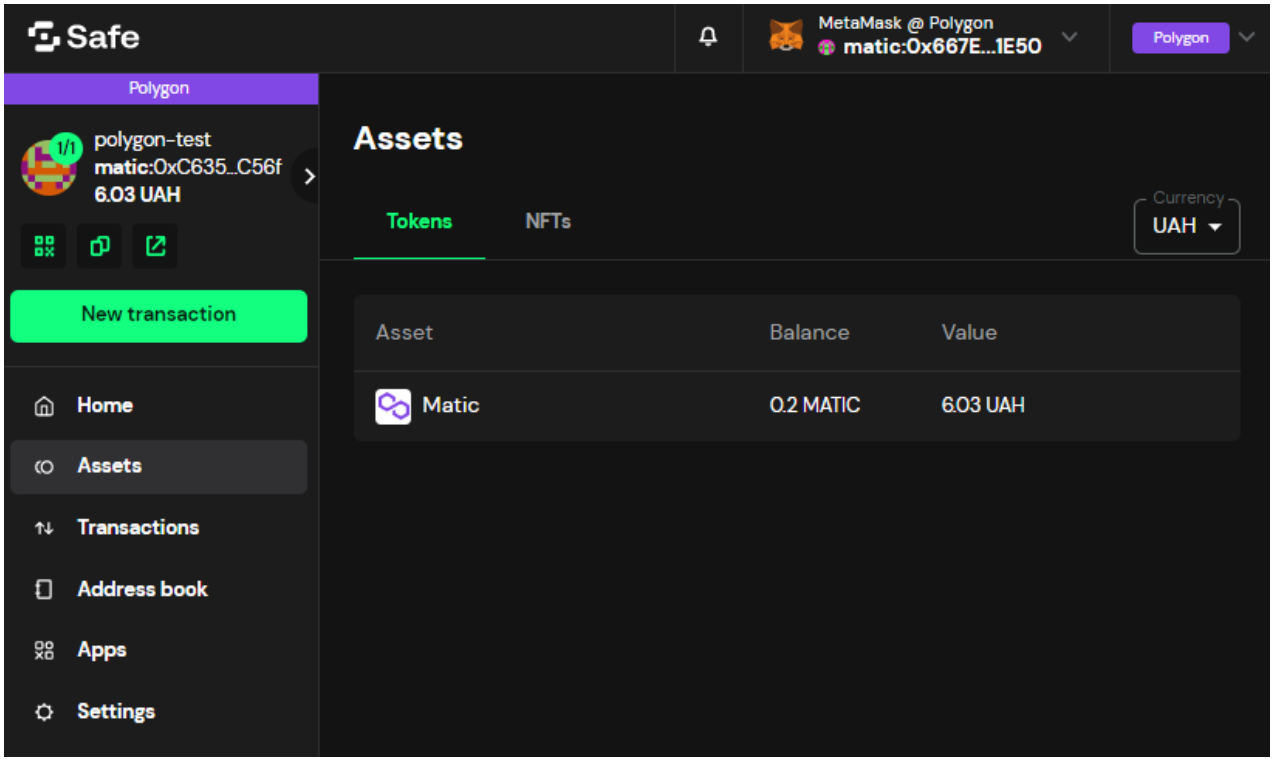

Рис. 3.17. Розділ Assets сховища Gnosis Safe

У наступній вкладці Transactions можна знайти всі транзакції, які вже були виконані раніше, або які очікуються підтвердження. Наприклад, якщо хтось із власників сховища почне транзакцію, яку потрібно буде підписати іншим власникам, то ця транзакція з’явиться саме у цій вкладці.

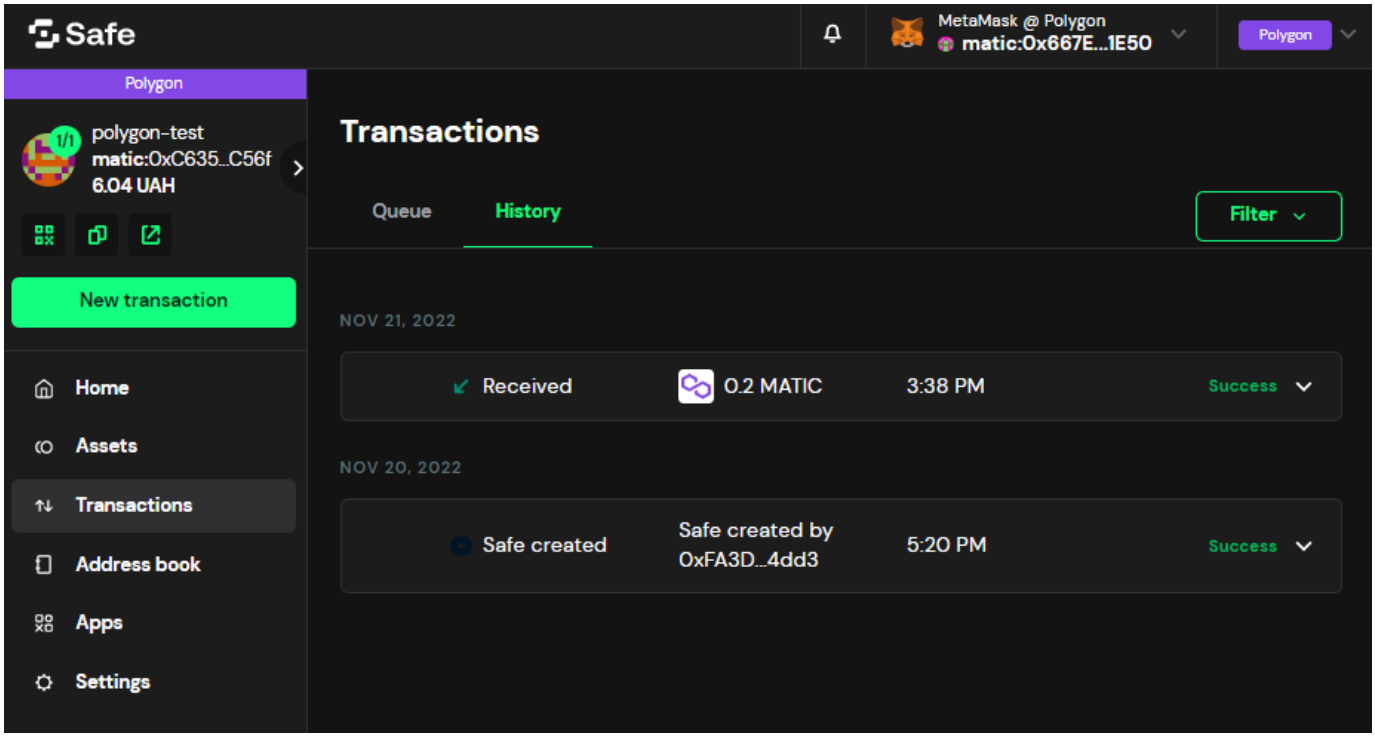

Рис. 3.18. Розділ Transactions сховища Gnosis Safe

Для того, щоб надіслати цифрові активи із Gnosis Safe, потрібно натиснути кнопку New transaction у боковому меню та вибрати пункт Send tokens. Далі потрібно буде вибрати вказати адресу отримувача. Можна вибрати одну з адрес із адресної книги, які були збережені раніше, або вставити нову адресу у поле для введення.

Далі потрібно вибрати який саме цифровий актив користувач бажає відправити, а також його кількість.

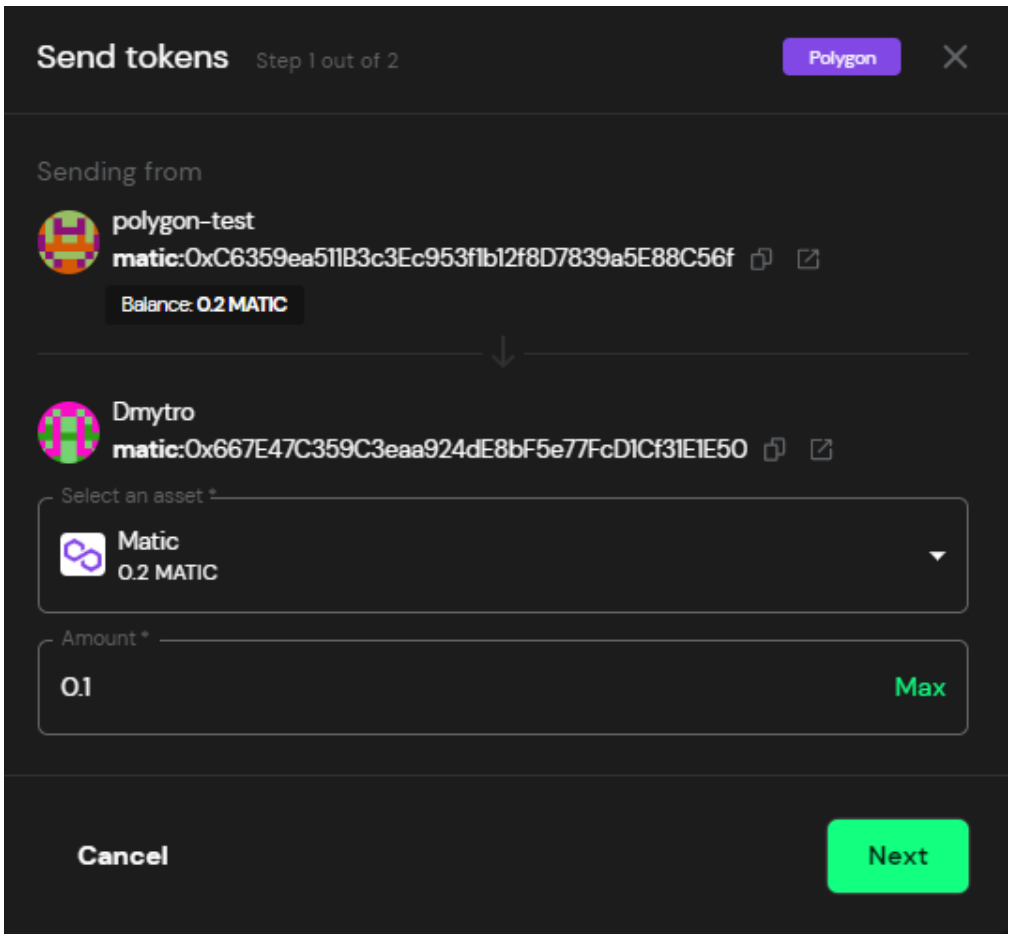

Рис. 3.19. Введення даних для відправлення цифрових актиів із Gnosis Safe

Після цього користувач може подивитись деталі переказу або змінити додаткові параметри транзакції. Цей крок має відношення до ліміту газу, користувач може його змінити для того, щоб транзакція пройшла швидше, шляхом збільшення оплати комісії. Або навпаки, зменшити ліміт газу, щоб транзакція обробилась пізніше, але при цьому економлячи на комісії за переказ.

Такий крок має сенс для переказів у «дорогих» блокчейнах, таких як Ethereum або Bitcoin, у яких оплата за газ по відношенню до національних валют, може коштувати декілька десятків або сотень доларів США.

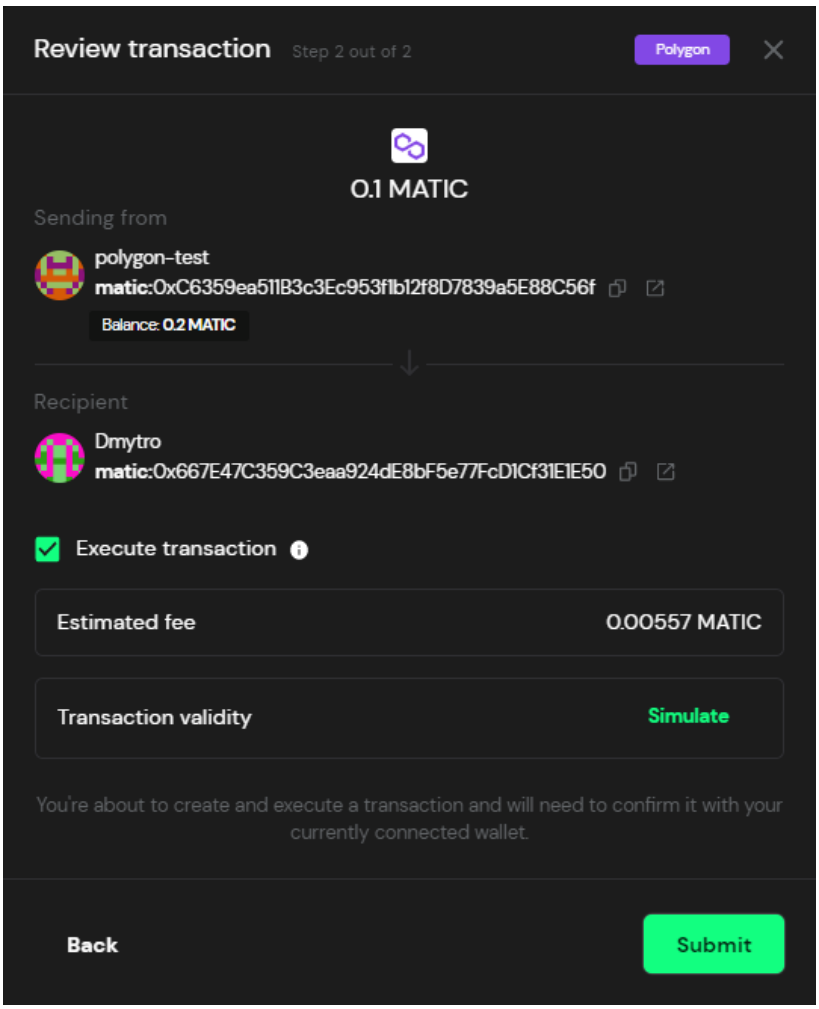

Рис. 3.20 Перевірка та підтвердження транзакції

Після підтведження транзакції її потрібно буде підписати за допомогою цифрового гаманця підписувача, а також, залежно від порогової політики, транзакція буде виконана одразу, якщо для підтвердження був вказаний лише один користувач, або її потрібно буде підписати всіма іншими власниками сховища. Транзакція, яка очікує на підпис інших власників сховища знаходиться у вкладці Transactions – Queue.

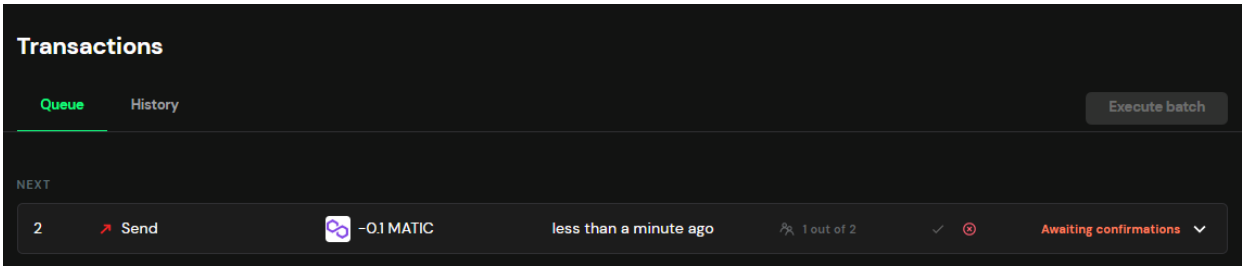

Рис. 3.22. Вигляд транзакції Gnosis Safe, яка очікує на підпис інших власників сховища

Після підпису всіма власниками сейфу, транзакція буде виконана та відобразиться у історії транзакцій.

Вкладка Address book – це адресна книга, яка дозволяє пов’язувати імена разом із зашифрованими адресами Ethereum. Це спрощує розпізнавання контрагентів Gnosis Safe. Користувачі можуть керувати своєю адресною книгою через відповідну вкладку. Для того, щоб створити новий обліковий запис, потрібно нажати на кнопку Create entry. Після цього користувачу потрібно буде записати адресу, яку він хоче додати, та вибрати їй ім’я.

Для того, щоб змінити запис у адресній книзі, користувачу потрібно нажати на значок олівця, який підписаний як Edit entry, та внести потрібні зміни. Також є можливість видалити обліковий запис з адресної книги, якщо він вже не потрібен.

Також користувач може використовувати обліковий запис із адресної книги, вказавши його як отримувача для транзакції, натиснувши кнопку Send напроти цього запису.

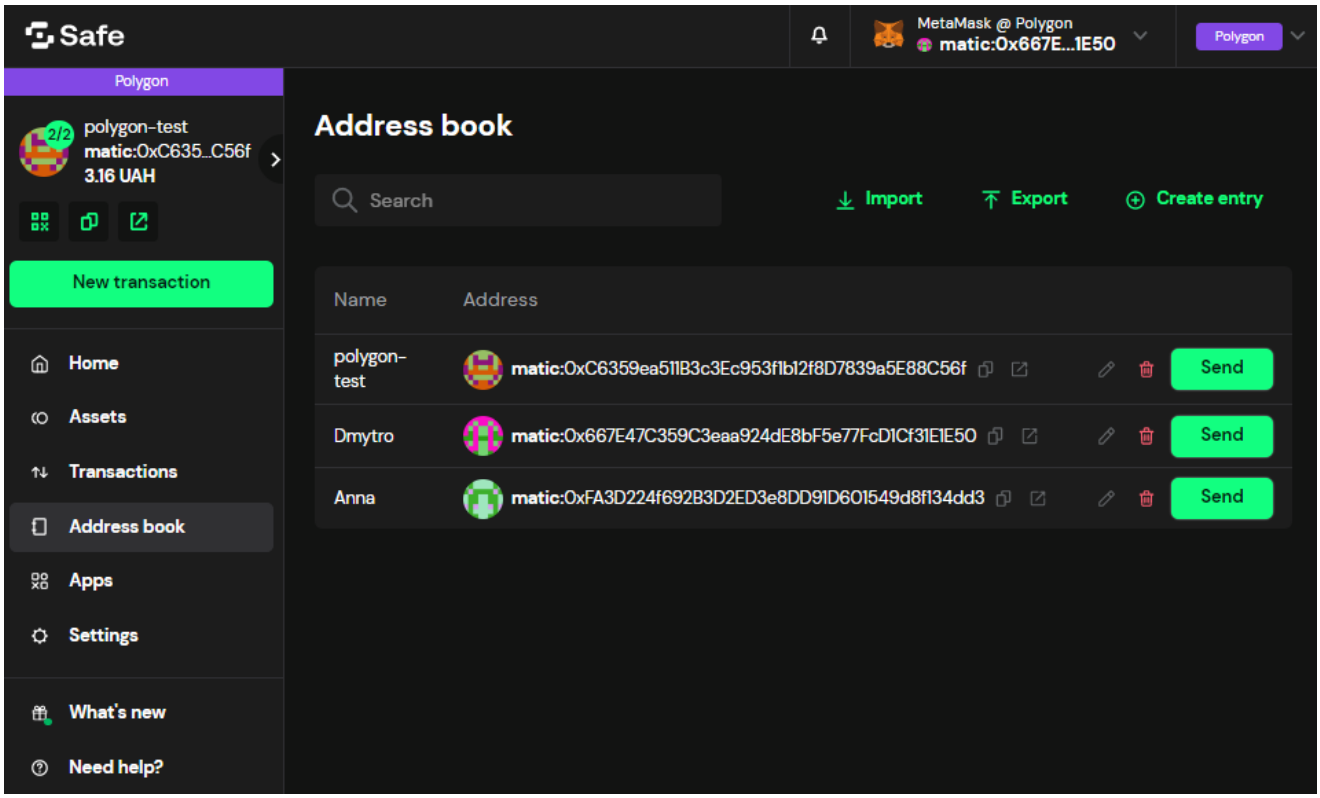

Рис. 3.23. Вкладка Address book сховища Gnosis Safe

Вкладка Apps відповідає за безпечні додатки, які дозволяють користувачам взаємодіяти з додатками на Ethereum прямо з інтерфейсу Gnosis Safe. Це можна зробити шляхом вибору відповідного додатку із доступного списку, або використовуючи додаток Wallet Connect. Для цього у іншій вкладці браузера потрібно відкрити децентралізований додаток, який підтримує Wallet Connect, наприклад Uniswap.

Потім всередині цього децентралізованого додатку необхідно вибрати метод підключення Wallet Connect та натиснути кнопку «копіювати у буфер обміну» під QR-кодом, та вставити скопійовані дані в поле для введення у додатку Gnosis Safe. Після підключення децентралізованого додатку, ним можна буде користуватись прямо з інтерфейсу Gnosis Safe.

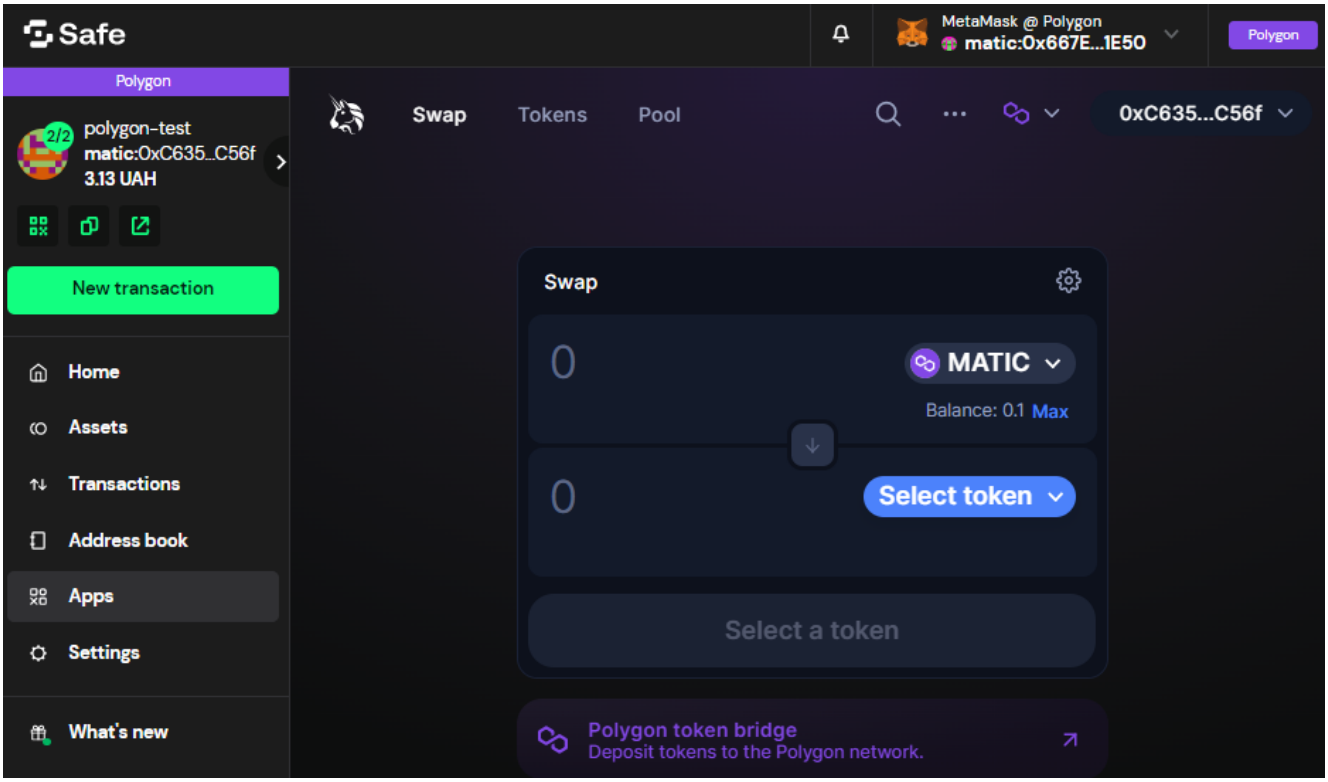

Рис. 3.24. Взаємодія з децентралізованим додатком Uniswap через інтерфейс Gnosis Safe

Після запуску транзакції через сторонні додатки, вона повинна з’явитись у інтерфейсі Gnosis Safe для підписання. Транзакції можуть бути підписані та виконані таким самим способом, як і всі інші транзакції у Gnosis Safe. У списку транзакцій користувач може легко знайти транзакції, які проводились з

використанням Wallet Connect. Таким чином користувач може підключати будь-які децентралізовані додатки та використовувати їх всередині даної платформи, для цього не потрібно буде користуватись іншими сторонніми гаманцями.

Якщо власники сховища захочуть розширити команду та додати ще декількох людей, вони можуть це зробити через вкладку Settings. Для того, щоб додати нового власника, потрібно перейти до вкладки налаштувань та натиснути кнопку Add new owner. Після цього відкриється нове вікно, у якому потрібно буде вказати ім’я нового власника сейфу та адресу його цифрового гаманця для підпису. Далі Gnosis Safe попросить підписувачів підтвердити зміну списку власників шляхом підпису транзакції в Blockchain. Для виконання цієї опції необхідно, щоб всі власники підтвердили цю операцію.

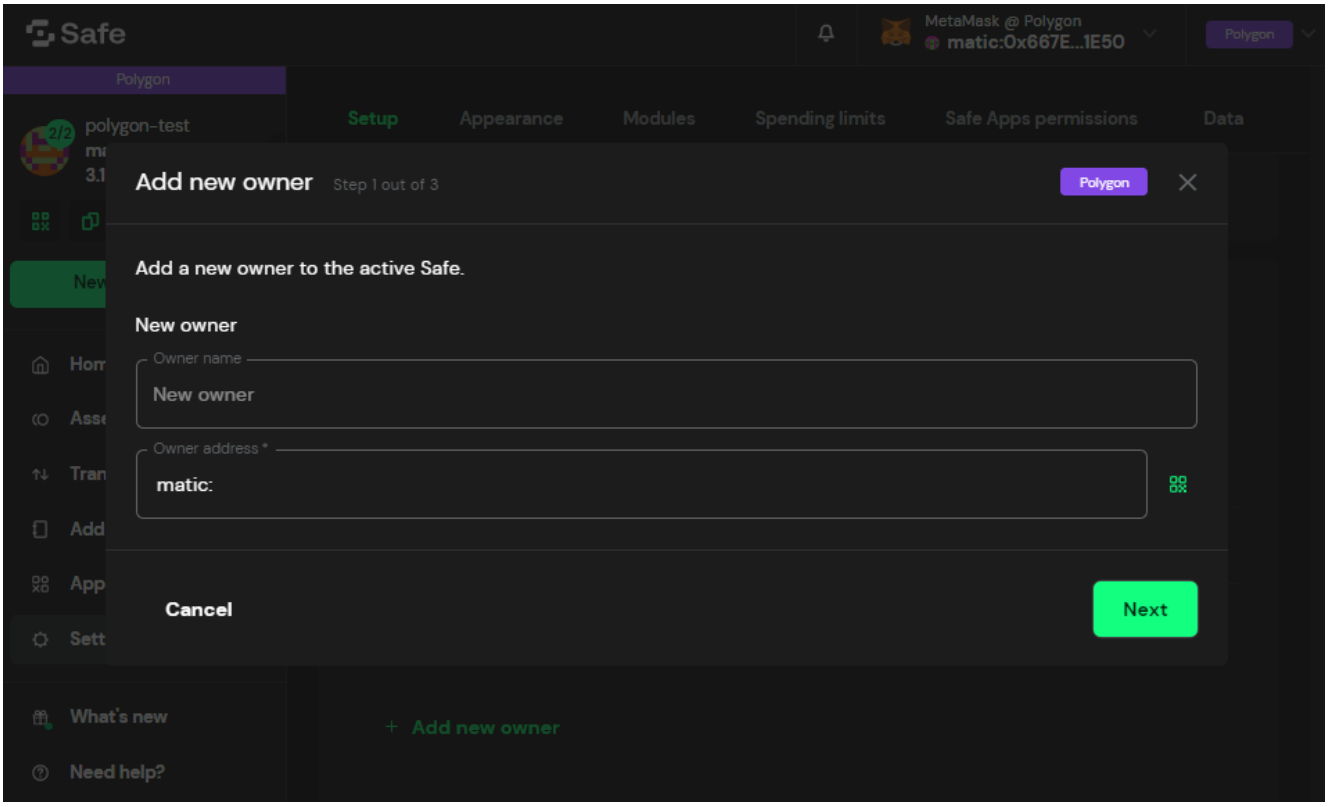

Рис. 3.25. Вкладка для додавання нового власника сховища Gnosis Safe

Ще однією з найбільш важливих функцій, яка є наступною перевагою використання цифрових гаманців зі смарт-контрактами Gnosis Safe, це вміння виконувати пакетні транзакції. Це означає, що замість того, щоб підтверджувати набір транзакцій одна за одною, їх можна бути об’єднати разом та підтвердити

всього один раз. Для цього Gnosis Safe використовує бібліотеку MultiSend, а функція називається Transaction Builder.

Таким чином, сховище Gnosis Safe є прекрасним рішенням для збереження цифрових активів користувачів, оскільки володіє надійними смарт-контрактами, які були перевірені експертами безпеки Blockchain, а також безліччю функцій корисних функцій з додатковим рівнем захищеності.

3.4 Розробка рекомендацій щодо забезпечення безпеки цифрових активів у Blockchain із використанням рішення Gnosis Safe

У цій роботі обговорювались ризики, пов'язані з основними варіантами використання, способами збереження та перспективними можливостями цифрових активів у Blockchain, а також проблеми щодо забезпечення їх захисту. Споживачі, інвестори та підприємства вразливі до багатьох ризиків в екосистемі Blockchain.

Відповідно до поставлених задач, а також відповідального розвитку інновацій платіжних та цифрових активів, рекомендовано комплексний підхід щодо захисту цифрових активів, який описаний нижче. Цей підхід ґрунтується на, та доповнює інші рекомендовані дії, які описано в у звіті President’s Working Group on Financial Markets (PWG) Report on Stablecoins щодо цифрових активів та стейблкоїнів [32], а також інші звіти про ризики фінансової стабільності та регуляторні прогалини, які описані у Розділі 1.

1. Регулюючі та правоохоронні органи повинні, у відповідних випадках, проводити пильний моніторинг сектору цифрових активів у Blockchain щодо незаконної діяльності, активно проводити розслідування та ініціювати цивільні та кримінальні вимоги щодо забезпечення спостережуваних законів, приділяючи особливу увагу споживачам, інвесторам та захисту ринку.

Обман, крадіжки та шахрайство стали особливо серйозною проблемою в цій галузі. Ці незаконні дії завдають значної фінансової шкоди споживачам, інвесторам та підприємствам по всьому світу, і лише у 2021 році ФБР повідомило про загальну втрату понад 1,6 мільярда доларів. Цифрові активи постійно розвиваються, так

само, як і незаконні дії за допомогою цифрових активів. Для забезпечення широкого та послідовного виконання та доповнення інструментів аналітики приватного сектору, регулятори та правоохоронні органи повинні, за необхідності, ділитися інформацією щодо типу та масштабів шахрайських, оманливих або маніпулятивних ринкових практик, які вони спостерігають та розслідують. Наприклад, обмін даними може допомогти визначити відповідні кластери незаконної діяльності та точкові тенденції в аферах та типах шахрайства.

2. Регулюючим органам слід використовувати свої існуючі повноваження для випуску керівних вказівок і правил для усунення поточних і ризиків, що виникають у продуктах і послугах цифрових активів для споживачів, інвесторів і підприємств. Установи повинні працювати спільно, щоб сприяти послідовному та всебічному нагляду.

Користувачі платформ цифрових активів на Blockchain схильні до значних ризиків, включаючи ризики дефолту та прямої крадіжки. Крім того, користувачі часто можуть бути не повною мірою обізнані про ці ризики, враховуючи те, що учасники ринку цифрових активів часто наголошують на торговому прибутку з мінімальним посиланням на збитки, а також загальну відсутність всебічного розкриття інформації. З цих причин доцільно впровадження Міністерства з фінансової грамотності та освіти, яке повинно, при необхідності, координувати та просувати зусилля щодо навчання споживачів цифрових активів. Ці зусилля повинні забезпечити, щоб зручні для споживача, які заслуговують на довіру та послідовні освітні матеріали були доступні, інклюзивні та зрозумілі в максимально можливій мірі. Такі матеріали мають:

- виділити ризики, пов'язані з використанням цифрових активів інвесторами чи споживачами, у тому числі підвищений ризик шахрайства, крадіжок та шахрайства;
- виявлення та попередження про загальноприйняту практику, що використовується особами, які вчинили шахрайство, злодійство та шахрайство;
- надати інформацію про те, як повідомляти про незаконні дії та подавати споживачам скарги;

- надавати інформацію про операційні ризики, які є унікальними для екосистеми Blockchain, та про те, як вони можуть вплинути на інвестиційну вартість цифрових активів.

Нарешті, влада повинна, при необхідності, взаємодіяти з лідерами галузі, розробниками та іншими відповідними сторонами для просування та координації державних та приватних стратегій охоплення споживачів фінансовою освітою.

3. Діючі та нові учасники, які використовують технологію Blockchain, повинні розробляти та впроваджувати сучасні й надійні технічні рішення для забезпечення безпеки своїх проектів.

Ландшафт технології розподіленого реєстру, яка є основою Blockchain, продовжує розвиватися. Таким чином росте і число висококласних проектів, як діючих, так і на стадії тестування, які підтвердили переваги з точки зору ефективності та прозорості. Проте залишається актуальним питання надійного захисту продукту.

Gnosis Safe може стати провідним рішенням для технічного забезпечення безпеки цифрових активів у Blockchain. Використання технології мультипідпису, функції зворотнього виклику та додаткових модулів безпеки дозволить користувачам цифрових активів отримати високий рівень захисту від злому та ризиків, а також стати прикладом або частиною для інтеграції у свої продукти інших розробників.

Висновки до третього розділу

Досліджено рішення для забезпечення безпеки цифрових активів у Blockchain, а саме сховище Gnosis Safe. Проаналізовано технологію мультипідпису для збереження цифрових активів, виокремлено переваги цієї технології над стандартними рішення, такими як програмні та апаратні гаманці.

Простежено, що окрім технології Multi-signature, рішення для забезпечення безпеки цифрових активів Gnosis Safe володіє безліччю функцій захисту, а саме: можливість розширеного управління доступом за допомогою Gnosis Safe Modules;

функція зворотного виклику токену; розрахунки без Ethereum, або оплата токенами; розширена логіка транзакцій, наприклад поєднання декількох невеликих транзакцій у блокчейні Ethereum в одну; функція страхування «Insurance by Nexus Mutual».

Проведено тестування всіх можливостей рішення, показано створення власного сховища Gnosis Safe, надсилання та отримання транзакцій, а також інтеграція з децентралізованими додатками шляхом використання технології Wallet Connect.

Встановлено, що рішення Gnosis Safe володіє всіма необхідними та актуальними технологіями для забезпечення безпеки цифрових активів у Blockchain.

Розроблено рекомендації щодо забезпечення безпеки цифрових активів у Blockchain із використанням рішення Gnosis Safe.

ВИСНОВКИ

В магістерській роботі отримано наступні наукові та науково-практичні результати:

1. Досліджено особливості та історичний розвиток технології Blockchain. Зроблено висновок, що основною метою Blockchain є створення децентралізованої технології без посередників, яка дозволить записувати та розповсюджевати інформацію без можливості її редагування, а також створювати цифрові активи з метою збереження цінності або для грошових розрахунків, які захищені криптографією.

2. Визначено, що основними особливостями та перевагами технології розподіленого реєстру є: захищена криптографією транзакція грошей, прозорість, децентралізація, розумні контракти (smart contracts), підтвердження власності та цифрова ідентифікація.

3. Досліджено розвиток цифрових активів у Blockchain. Виокремлено різні види цифрових активів, основні характеристики та зазначено способи їх використання.

4. Досліджено ризики щодо використання та зберігання цифрових активів у Blockchain. Виокремлено основні види ризиків, а саме: ризики поведінки та шахрайство; ризики впливу на уразливі групи населення; операційні ризики; традиційні фінансові ризики, такі як ризики ресурсів і можливостей та ризики щодо зберігання.

5. Досліджено проблеми захисту і безпеки цифрових активів від злому та шахрайства. Зроблено висновок, що Blockchain та суміжні технології є формами комп'ютерного програмного забезпечення і схильні до уразливостей програмного забезпечення.

6. Проаналізовано різні методи та засоби зберігання цифрових активів у Blockchain. Зроблено висновок, що найбільш популярні способи для безпечного

збереження цифрових активів є не повністю надійними та потребують нових комплексних рішень для забезпечення безпеки.

7. Досліджено рішення для забезпечення безпеки цифрових активів у Blockchain, а саме сховище Gnosis Safe. Проаналізовано технологію мультипідпису для збереження цифрових активів, виокремлено переваги цієї технології над стандартними рішення, такими як програмні та апаратні гаманці.

8. Виявлено, що окрім технології Multi-signature, рішення для забезпечення безпеки цифрових активів Gnosis Safe володіє безліччю функцій захисту, а саме: можливість розширеного управління доступом за допомогою Gnosis Safe Modules; функція зворотного виклику токену; розрахунки без Ethereum, або оплата токенами; розширена логіка транзакцій, наприклад поєднання декількох невеликих транзакцій у блокчейні Ethereum в одну; функція страхування «Insurance by Nexus Mutual».

9. Встановлено, що рішення Gnosis Safe володіє всіма необхідними та актуальними технологіями для забезпечення безпеки цифрових активів у Blockchain.

10. Розроблено рекомендації щодо забезпечення безпеки цифрових активів у Blockchain із використанням рішення Gnosis Safe.