НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри
_____ **Дмитро ЛАНДЕ**
(підпис)
« ___ » _____ 2023 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності: 125 «Кібербезпека»

на тему: Алгоритм форензіки для виявлення незаконної діяльності в публічних блокчейнах

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-93
(шифр групи)

Абдуллаєва Есміра Вагіфівна _____
(прізвище, ім'я, по батькові) (підпис)

Керівник к.т.н, доцент, Гальчинський Леонід Юрійович _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент к.т.н, доцент, Лавренюк Алла Миколаївна _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2023 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність: 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
« ___ » _____ 2023 р.

ЗАВДАННЯ

на дипломну роботу на здобуття вищої освіти

Абдуллаєвій Есмірі Вагіфівні

1. Тема дипломної роботи: Алгоритм форензіки для виявлення незаконної діяльності в публічних блокчейнах,
   керівник роботи: Гальчинський Леонід Юрійович, к.т.н., доцент,
   затверджені наказом по університету від «26» травня 2023 р. № 2028-С
2. Термін подання здобувачем вищої освіти роботи «13» червня 2023 р.
3. Вихідні дані до роботи: алгоритм форензіки блокчейн мережі на основі протоколу Ethereum.
4. Зміст роботи: аналіз публічних блокчейн протоколів, а також їх базрвих вразливостей, визначення метрик ідентифікації незаконної діяльності, побудова та програмна реалізація алгоритму форензіки мережі Ethereum.
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) презентація.
6. Дата видачі завдання: 1 листопада 2022 р

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	01.11.2022	виконано
2	Ознайомлення з джерелами інформації по темі	01.11.2022 – 01.12.2022	
3	Огляд та аналіз предметної області. Ознайомлення з основами блокчейн технологій	02.12.2022 – 01.01.2023	виконано
4	Аналіз основних вразливостей публічних блокчейн протоколів	02.01.2023 – 12.01.2023	виконано
5	Оцінка ефективності методів блокчейн форензіки	13.01.2023 – 01.02.2023	виконано
6	Розробка алгоритму форензіки мережі Ethereum	02.02.2023 – 01.03.2023	виконано
7	Виявлення проблем у відстеженні незаконної діяльності	02.03.2023 – 16.03.2023	виконано
8	Програмна реалізація алгоритму форензіки	17.03.2023 – 01.05.2023	виконано
9	Візуалізація графу транзакцій	02.05.2023 – 17.05.2023	виконано
10	Тестування та аналіз результатів запропонованого алгоритму	18.05.2023 – 01.06.2023	виконано

Здобувач вищої освіти _____ Есміра АБДУЛЛАЄВА
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

Науковий керівник _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Дипломна роботи складається з 3 розділів, включає 21 ілюстрацію, 2 таблиці, 1 додаток та 20 літературних посилання, загальний обсяг роботи – 69 сторінок.

Мета роботи – створення реалізації алгоритму форензіки блокчейн мережі на основі протоколу Ethereum задля виявлення незаконної діяльності.

Об’єкт дослідження – виявлення незаконної діяльності в блокчейн протоколі Ethereum.

Предмет дослідження дипломної роботи – алгоритм блокчейн форензіки спрямований на виявлення незаконної діяльності в публічних блокчейнах.

Методи дослідження - аналіз блокчейн технологій та базових вразливостей публічних блокчейн протоколів, таких як Ethereum, побудова алгоритму форензіки та програмна реалізація аналізу мережі.

Результати досліджень було апробовано на XXI Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського, 11-12 травня 2023 та Всеукраїнській науково-практичній конференції «Theoretical and Applied Cybersecurity» (TACS-2023), 26 травня 2023.

Ключові слова: блокчейн, форензіка, аналіз мережі, Ethereum, вразливості.

ABSTRACT

The thesis consists of 3 chapters, includes 21 illustrations, 2 tables, 1 appendix and 20 literary references, the total volume of work - 69 pages.

The purpose of the work is to create an implementation of the blockchain network forensics algorithm based on the Ethereum protocol to detect illegal activity.

The object of the research is the detection of illegal activity in the Ethereum blockchain protocol.

The subject of the thesis research is the blockchain forensics algorithm aimed at detecting illegal activity in public blockchains.

Research methods - analysis of blockchain technologies and basic vulnerabilities of public blockchain protocols, such as Ethereum, construction of a forensics algorithm and software implementation of network analysis.

The results of the research were tested at the XXI All-Ukrainian scientific and practical conference of students, postgraduates and young scientists "Theoretical and applied problems of physics, mathematics and informatics" of KPI named after Igor Sikorsky, May 11-12, 2023 and the All-Ukrainian Scientific and Practical Conference "Theoretical and Applied Cybersecurity" (TACS-2023), May 26, 2023.

Keywords: blockchain, forensics, network analysis, Ethereum, vulnerabilities.

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів 7
Вступ 8
1 Теоретисні відомості про блокчейн технології 10
1.1 Огляд блокчейн технології 10
1.2 Архітектура публічних блокчейн протоколів 11
1.3 Децентралізація та незмінність у публічних блокчейнах 17
1.4 Популярні публічні блокчейн протоколи 19
1.5 Основні вразливості публічних блокчейн протоколів 23
Висновки до розділу 1 30
2 Оцінка ефективності блокчейн форензіки 32
2.1 Принцип роботи блокчейн форензіки 32
2.2 Огляд методів проведення аналізу даних блокчейну 34
2.3 Основні метрики блокчейн форензіки 39
2.4 Побудова алгоритму аналізу блокчейн мережі на основі протоколу Ethereum 41
2.5 Проблеми у відстеженні діяльності кіберзлочинців 45
Висновки до розділу 2 46
3 Розробка рішення для відстеження діяльності кіберзлочинців у публічному блокчейні 47
3.1 Програмне забезпечення 47
3.2 Аналіз блокчейн мережі на основі протоколу Ethereum 47
3.3 Візуалізація графу транзакцій 52
3.4 Визначення зловмисних адрес 54
Висновки до розділу 3 59
Висновки 60
Перелік джерел посилань 62
Додаток А Лістинг програми 64

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

P2P – Peer-to-Peer – рівний до рівного

PoW – Proof of Work – консенсус на основі доказу виконання роботи

PoS – Proof of Stake – консенсус на основі підтвердження частки

DApps – Decentralized Application – децентралізовані додатки

SHA – Secure Hash Algorithm

TPS – transactions per second – транзакції в секунду

AML – Anti-money laundering – протидія відмиванню грошей

ETH – скорочення від Ethereum

BTC – скорочення від Bitcoin

API – Application Programming Interface

EVM – Ethereum Virtual Machine - віртуальна машина Ethereum

DeFi – Decentralized Finance – децентралізовані фінансові сервіси

NFT – non-fungible token - невзаємозамінний токен

IoT – Internet of Things – інтернет речей

DDoS – (distributed) denial-of-service attack – розподілена атака на відмову в обслуговуванні

ВСТУП

Стрімкий розвиток блокчейн технологій призвів до змін в усіх сферах життя, забезпечуючи безпечне та прозоре зберігання даних і транзакцій. Завдяки децентралізованій природі та незмінності публічні блокчейн протоколи привернули значну увагу, але їх широке впровадження призвело до появи незаконної діяльності, включаючи відмивання грошей, шахрайство та незаконні транзакції.

Розглянувши сучасні блокчейн протоколи, зрозуміло, що одним з найпоширеніших є Ethereum, проте, навіть при постійному вдосконаленні протокол має низку вразливостей. Один з варіантів запобігання – аналіз мережі, на наявність різних протиправних дій, що вирішальне значення для підтримки довіри та цілісності системи.

Мета роботи полягає у створення алгоритму форензіки блокчейн мережі на основі протоколу Ethereum, а також його програмна реалізація, яка допоможе провести аналіз та виявити незаконну діяльність.

Об’єкт дослідження: виявлення незаконної діяльності в блокчейн протоколі Ethereum.

Предмет дослідження: алгоритм блокчейн форензіки спрямований на виявлення незаконної діяльності в публічних блокчейнах.

Завдання на дипломну роботу:

1. Розглянути принцип роботи та основні вразливості блокчейн мережі на основі протоколу Ethereum.
2. Відібрати показники, які можуть свідчити про наявність незаконної діяльності в публічному блокчейні.
3. Побудувати алгоритм для аналізу блокчейн мережі, який може ефективно ідентифікувати незаконну діяльність.
4. Програмно реалізувати запропонований алгоритм форензіки для аналізу блокчейн мережі на основі протоколу Ethereum та провести розбір отриманих результатів.

5. Виконати та проаналізувати візуалізацію графу транзакцій з використанням отриманих даних.

Метод дослідження – аналіз блокчейн технологій та базових вразливостей публічних блокчейн протоколів, таких як Ethereum, побудова алгоритму форензіки та програмна реалізація аналізу мережі. Також були використанні комплексі дослідницькі методи, а саме:

- загальнонауковий: обґрунтування основних теоретичних відомостей, аналіз та узагальнення отриманих результатів;
- логічний: визначення основних напрямів дослідження;
- системний: програмна реалізація алгоритму.

Наукова новизна дослідження полягає у створенні та реалізації алгоритму форензіки протоколу Ethereum.

Практичне значення одержаних результатів є те, що програмна реалізації алгоритму форензіки може використовуватись для виявлення незаконної діяльності та її запобіганню в майбутньому.

Апробація результатів роботи. XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики» та Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023).

Публікація за результатами досліджень.

Абдуллаєва Е. В., Гальчинський Л. Ю. Алгоритм форензіки блокчейн мережі Ethereum для виявлення незаконної діяльності. Матеріали XIX Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики» КПІ ім. Ігоря Сікорського, 2023. С. 225-227.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО БЛОКЧЕЙН ТЕХНОЛОГІЇ

1.1 Огляд блокчейн технології

Блокчейн технологія – це покращенный механізм бази даних, який дає можливість організувати обмін інформацією в середині бізнес-мережі. Блокчейн зберігає дані в блоках, які з’єднані між собою в ланцюг. Кожен блок містить позначку часу, геш попереднього блока та дані транзакцій, що подані як геш-дерево[3]. Всі дані узгоджені в часі, адже потоки не можна видаляти або змінювати без згоди з боку мережі.

Таким чином, технологія блокчейн може бути використана для створення незмінного або постійного реєстру для відстеження платежів, рахунків, тощо[1].

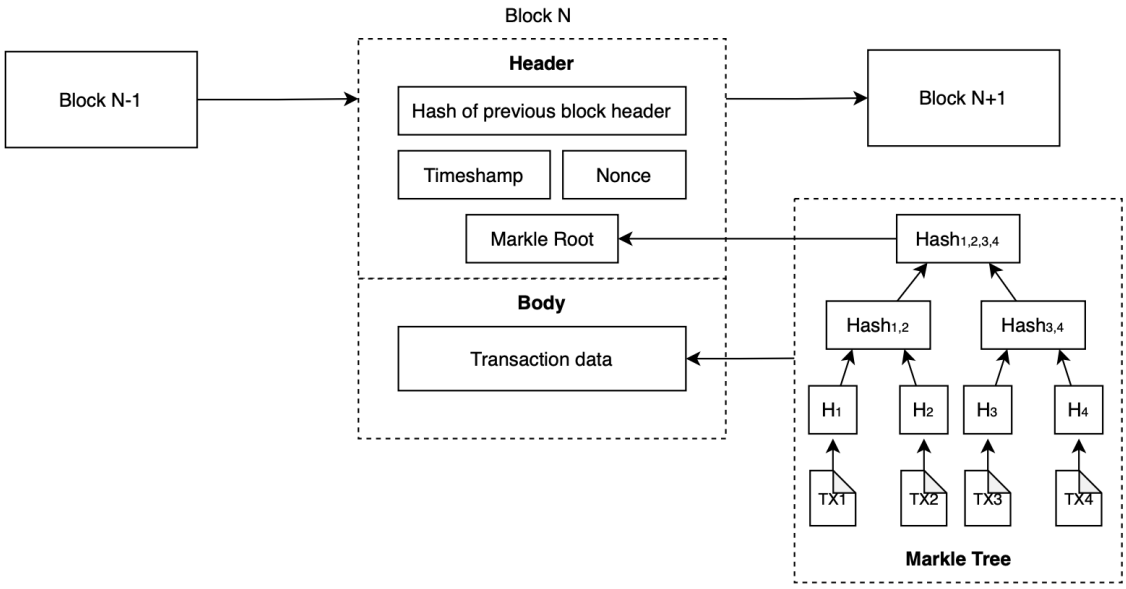

Рисунок 1.1 – Схематичне зображення структури блокчейну

Важливість блокчейну базується на швидкості й точності передачі інфомації. Він надає миттєву та повністю прозору інформацію, що зберігається в незмінній книзі, доступ до якої мають лише авторизовані учасники мережі. Блокчейн-мережа може відстежувати замовлення, платежі, рахунки-фактури, виробництво тощо. Отже, варто також визначити ключові елементи блокчейну [3]:

- Розподілена книга – кожен з учасникім мережі має доступ до розподіленої книги та незмінногозапису транзакцій. З їх допомогою транзакції записуються лише один раз, що виключає дублювання.
- Незмінні записи – жоден не може змінити або підробити спільний реєст транзакцій.
- Смарт-контракти – використовуються для прискорення транзакцій. Вони також можуть визначати умови переказу або оплати.

1.2 Архітектура публічних блокчейн протоколів

Блокчейн протоколи – це набір протоколів, які використовуються для керування мережею блокчейн. Ці правила визначають інтерфейс мережі, взаємодію між комп'ютерами, стимули, тип даних тощо. Протоколи спрямовані на вирішення чотирьох принципів [5]:

- безпеки – забезпечення безпеки всієї мережі;
- децентралізації – відсутність центральної влади, тобто, протоколи авторизують всю мережу;
- узгодженості – оновлення бази даних після кожної транзакції;
- масштабованості – збільшення кількості транзакцій.

Публічна архітектура блокчейну функціонує на основі консенсусних алгоритмів proof-of-work (PoW) або proof-of-stake (PoS) і використовує відповідні протоколи. Публічний блокчейн не потребує жодних дозволів, оскільки він має відкритий код. Він дає можливість визначити нові блоки з їхнім наявним станом, оскільки це відкритий код. Також можна завантажити код блокчейну та перевірити транзакції в мережі[4].

Це робить транзакції можливими по всій мережі. Публічна архітектура блокчейну дозволяє здійснювати прозорі, але анонімні або псевдонімні транзакції.

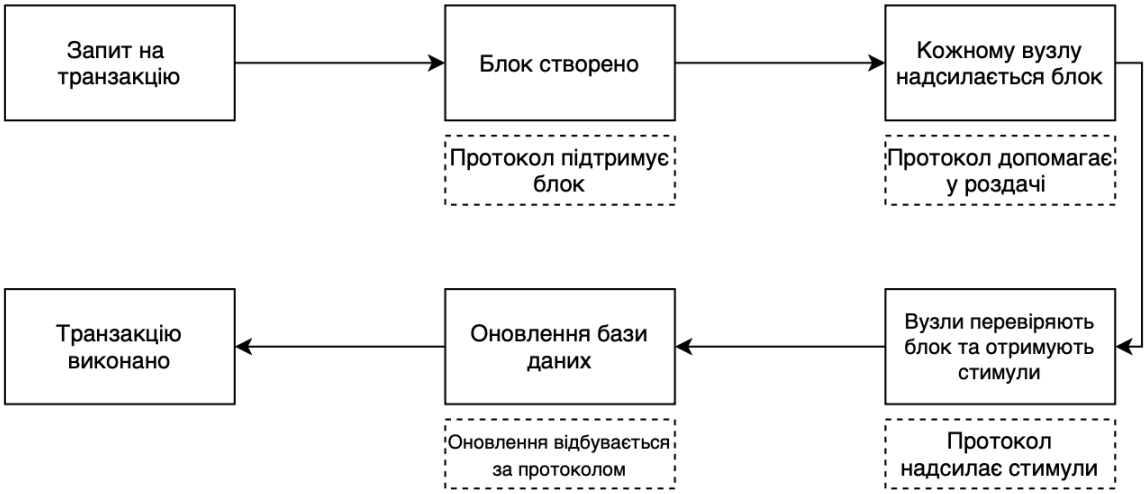

Рисунок 1.2 – Схематичне зображення роботи блокчейн протоколу

Розробка публічних блокчейн протоколів базується на забезпеченні прозорості та високого рівня безпеки за допомогою криптографічних алгоритмів. Додатки, які вимагають високого рівня прозорості та довіри побудовані саме на приватних блокчейнах.

Сама по собі технологія блокчейн доволі обмежена, тож для побудови архітектури публічних блокчейнів використовують такі п’ять рівнів[1]:

- Апаратний рівень (віртуальні машини).
- Рівень даних (електронний підпис, геш).
- Мережевий рівень (P2P).
- Рівень консенсусу (PoW, PoS).
- Прикладний рівень (смарт-контракти, користувацький інтерфейс).

1.2.1 Апаратний рівень

Апаратний рівень безпечно зберігає дані блокчейна на серверах. Доступ до даних отримається через архітектуру клієнт-сервер. Під час використання blockchain програми, клієнтська машина надсилає запит на доступ до сервера даних. Оскільки блокчейни є одноранговими (P2P) мережами, вони з’єднують клієнтів із «одноранговими» клієнтами для обміну даними. Таким чином, цей

рівень є не що інше, як величезна мережа пристроїв, які спілкуються один з одним і обмінюються даними. По суті, так народилися розподілені книги.

1.2.2 Рівень даних

Цей рівень відповідає за керування та захист даних, що зберігаються в блокчейні. Структура даних блокчейну складається з таблиць блокчейну, в яких упорядковані транзакції. Після перевірки певної кількість транзакцій вузлами, дані об'єднуються в «блок», завантажуються в блокчейн і поєднуються з даними попереднього блоку. Це створює блокчейн, який масштабується з часом. Кореневий хеш дерева Merkle включається в кожен блок разом із хешем попереднього блоку, датою тощо. Це забезпечує безпеку, цілісність і неспростовність системи блокчейн.

Кожна транзакція в блоці підписується цифровим закритим ключем з гаманця відправника. Так як, цей ключ доступний лише відправнику, то ніхто не може змінити дані. Даних крок називаються «фінішна обробка». Цифрові підписи також захищають і особу власника, яка зашифрована з міркувань безпеки.

1.2.3 Мережевий рівень

Мережевий рівень відповідяє за за забезпечення зв'язку між вузлами в мережі блокчейн. Також відомий як рівень поширення або рівень P2P. Мережевий рівень також керує виявленням вузлів, ідентифікацією вузлів, транзакціями, створенням блоків і розповсюдженням блоків. Архітектура блокчейну однорангова і дозволяє вузлам досягти згоди щодо законності транзакції, прицьому сама транзакція в блокчейні здійснюється вузлами[10].

Даний рівень гарантує, що вузли можуть виявляти один одного, поширювати інформацію, а також синхронізуватись один з одним, щоб надати автентичності блокчейну. Приклад схеми роботи мережевого (однорангового) рівня, тобто заснованого на рівноправ'ї учасників зображено на Рисунку 1.3:

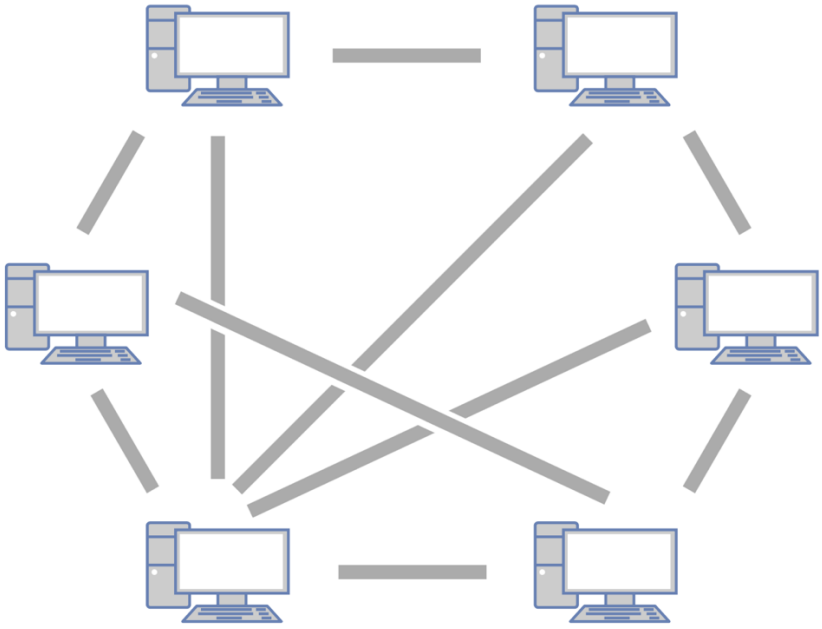

Рисунок 1.3 – Схематичне зображення роботи мережевого рівня (P2P)

1.2.4 Рівень консенсусу

Основним з усіх рівнів вважають консенсусний рівень. Це рівень, що забезпечує ключові функції блокчейну, а саму механізм консенсусу між вузлами. Крім того, він забезпечує консенсус у децентралізований спосіб, отже, усуває потребу в центральному органі влади. Цей підхід є основою децентралізації, яку забезпечує блокчейн. Тому кожна транзакція обробляється великою кількістю вузлів, кожен з яких повиннен бути узгоджений один з одним і перевіряти автентичність транзакції. Жоден окремий вузол не може контролювати будь-які транзакційні дані. І в разі виходу цього рівня з ладу, вся система блокчейну перестає працювати.

Наразі, існує безлічь різноманітних видів консенсусних механізмів, однак найбільш розповсюдженими є Proof of Work та Proof of Stake. Варто розглянути кожен з механізмів консенсусу трохи глибше, аби скласти точніше уявлення про принцип роботи та захищеність блокчейну[4].

Proof of Work:

- це механізм консенсусу, який вимагає від вузлів у мережі розв’язувати складні математичні проблеми для підтвердження транзакцій і додавання нових блоків до ланцюга. Цей процес вимагає обчислень і значного споживання енергії, а це в свою чергу робить його менш ефективним, ніж інші механізми консенсусу. Проте PoW вважається дуже безпечним, оскільки зловмисникам важко маніпулювати блокчейном.

Proof of Stake:

- це консенсусний механізм, який вимагає від вузлів у мережі зберігати певну кількість криптовалюти для підтвердження транзакцій і додавання нових блоків до ланцюжка. Чим більше криптовалюти містить вузол, тим більша ймовірність, що він буде обраний для перевірки наступного блоку.
- PoS вважається більш енергоефективним, ніж PoW, оскільки він не вимагає виконання складних обчислень, проте вважається менш безпечним, оскільки зловмисникам може бути легше маніпулювати блокчейном, якщо вони контролюють значну частину пропозиції криптовалюти.

Обидва ці механізми консенсусу мають як і переваги, так і недоліки. А який з них кращий, залежить саме від конкретного випадку використання та заданих вимог. Проте слід зазанчити, що PoW є безпечним і надійним механізмом консенсусу, але його споживання енергії викликає занепокоєння. PoS є більш енергоефективним, але він вимагає від вузлів зберігати значну кількість криптовалюти, що може призвести до централізації мережі.

1.2.5 Прикладний рівень

Прикладний рівень публічної архітектури блокчейну відноситься до рівня, який включає децентралізовані програми (dApps), побудовані на основі блокчейну.

Цей рівень містить в собі програми, які користувачі використовують для зв’язку з мережею блокчейн. Додаток відіграє роль передньої частини, спрямованої на користувача, тоді як стек блокчейну виконує роль задньої частини[1].

Зокрема, основний компонент прикладного рівня - це смарт-контракти. Самовиконувані контракти, які закодовані в блокчейні та автоматично виконуються, при виконанні певних умови. Їх можна використовувати для автоматизації бізнес-процесів, забезпечення виконання правил і створення децентралізованих програм.

Смарт-контракти використовують прості оператори «якщо/коли...тоді...», написані в коді на блокчейні. Мережа комп’ютерів виконує дію лише після виконання та перевірки заданих умов. Дії можуть включати переказ коштів відповідним сторонам, реєстрацію транспортних засобів, надсилання повідомлень або видачу квитків. Вже після завершення поточної транзакції блокчейн оновлюється – це означає, що транзакції не можуть бути змінені, а результати можуть переглядати всі сторони, залучені до контракту[19].

Ключова особливістю смарт-контракту в публічному блокчейні – це його здатність працювати в ненадійному середовищі. Оскільки виконання смарт-контракту децентралізоване та автоматизоване, немає потреби в посередниках, таких як юристи чи банки, щоб забезпечити виконання умов угоди. Це робить процес швидким, прозорим і рентабельним[3].

Також, на прикладному рівні можна виокремити наступні компоненти:

- Гаманці: це програмні додатки, які дозволяють користувачам зберігати, надсилати та отримувати криптовалюту. Вони також забезпечують зручний інтерфейс для взаємодії користувачів із блокчейном.
- Децентралізовані програми (dApps): це програми, створені на основі блокчейну, які пропонують різні функції, такі як фінансові послуги, соціальні мережі та ігри.

Загалом прикладний рівень публічної архітектури блокчейну відіграє вирішальну роль у тому, щоб зробити блокчейн доступним і придатним для використання кінцевими користувачами. Це дозволяє розробляти децентралізовані

програми та сервіси, які можуть запропонувати нові форми довіри, прозорості та підзвітності.

1.3 Децентралізація та незмінність у публічних блокчейнах

Децентралізація та незмінність є двома фундаментальними принципами публічних блокчейнів, які роблять їх унікальними та цінними. ЦІ дві характеристики забезпечуючи безпеку, надійність і стійкість публічних блокчейнів.

Децентралізація у блокчейні означає, що контроль та рішення передані до розподіленої мережі, тобто централізовані об’єкти не мають жодного впливу на мережу. Відсутність єдиної точки контролю робить систему більш стійкою до атак[5].

У децентралізованому блокчейні транзакції перевіряються та обробляються мережевими вузлами за допомогою консенсусного механізму, такого як PoW або ProS. Це гарантує, що мережа є безпечною та надійною, оскільки жодна особа не має повноважень маніпулювати обліковою книгою чи транзакціями.

Децентралізування керування та доступу до ресурсів у програмі, дає можливість досягти кращого обслуговування. Децентралізація зазвичай має деякі компроміси, такі як менша пропускна здатність транзакцій, проте в ідеалі ці компроміси варті покращеної стабільності та рівня обслуговування, які вони створюють.

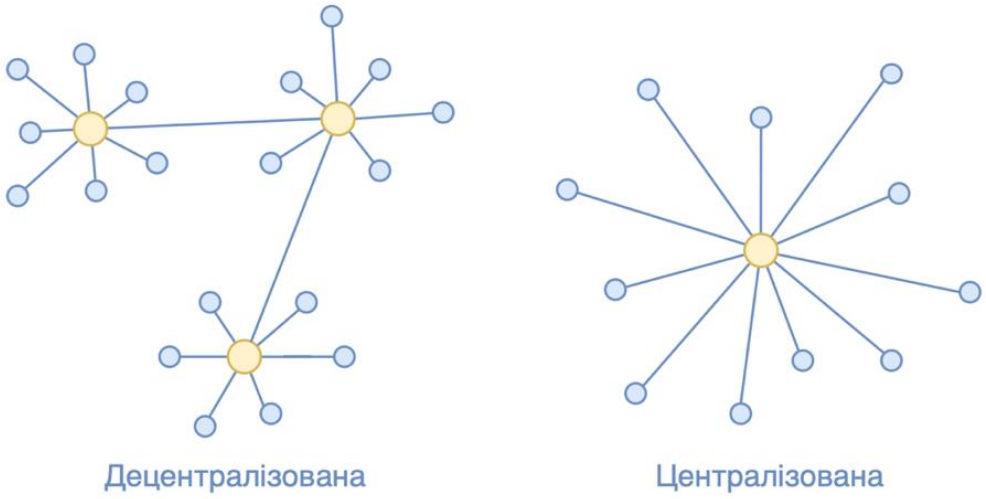

Рисунок 1.4 – Схематичне зображення децентралізованої та централізованої мереж

З іншого боку незмінність унеможливлює змінювання або видалення даних з блокчейну після додавання. Кожен блок криптографічно пов’язаний з попереднім, що дає змогу створити захищений від несанкціонованого доступу запис усіх транзакцій, які відбулися в мережі.

Оскільки, кожен вузол у мережі містить копію однієї книги, будь-яка спроба змінити дані в блокчейні буде відхилена іншими вузлами, що виявить невідповідність. Це робить блокчейн прозорим і доступним для перевірки, оскільки кожен може перевірити цілісність даних у мережі.

До основних переваг поєднання децентралізованості та незмінності мережі публічного блокчейну можна віднести[6]:

- Підвищений рівень безпеки: мережа менш вразлива до злому, оскільки немає однієї точки збою і контролю, тож зловмисник має отримати контроль над більшою частиною вузлів, щоб успішно маніпулювати даними.
- Забезпечення відмовостійкості: у разі виходу з ладу деяких вузлів мережі, вона продовжує функціонувати. Це підвищує стійкість до збоїв.
- Підвищений рівень прозорості: розподілена книга з записом всіх даних та транзакцій дає змогу будь-кому переглядати та перевіряти дані.

Загалом, децентралізація та незмінність є важливими характеристиками публічних блокчейнів, які забезпечують безпечні, прозорі та децентралізовані транзакції без потреби в посередниках.

1.4 Популярні публічні блокчейн протоколи

З роками кількість протоколів блокчейну, створених приватними особами та організаціями, надзвичайно зросла, кожен з яких призначений для унікальної мети. Проте є чотири основних протоколів блокчейну, які виділяються та широко застосовуються компаніями для конкретних випадків використання. Ці протоколи включають Bitcoin та Ethereum[6].

1.4.1 Bitcoin

Bitcoin — це цифрова децентралізована криптовалюта, створена в 2008 році невідомою особою або групою людей під псевдонімом Сатоші Накамото. Він заснований на технології блокчейн, яка є системою розподіленої книги, котра забезпечує безпечні та прозорі транзакції без необхідності центрального органу чи посередника[10].

За своєю суттю біткойн працює за допомогою криптографії для захисту транзакцій і запобігання шахрайству. Транзакції перевіряються за допомогою процесу, який називається майнінг, у якому потужні комп’ютери вирішують складні математичні задачі, щоб підтвердити транзакції та додати їх до блокчейну, децентралізованої загальнодоступної книги, яка записує всі транзакції біткойнів.

Після додавання транзакції до блокчейну вона стає загальнодоступною та не може бути змінена. Це забезпечує цілісність мережі Bitcoin і робить її стійкою до шахрайства та маніпуляцій[19].

Транзакції з біткойнами здійснюються за допомогою адрес біткойна, які є унікальними ідентифікаторами, що дозволяє користувачам надсилати та

отримувати біткойни. Ці адреси не пов’язані з реальними особами, забезпечуючи користувачам високий рівень конфіденційності та анонімності.

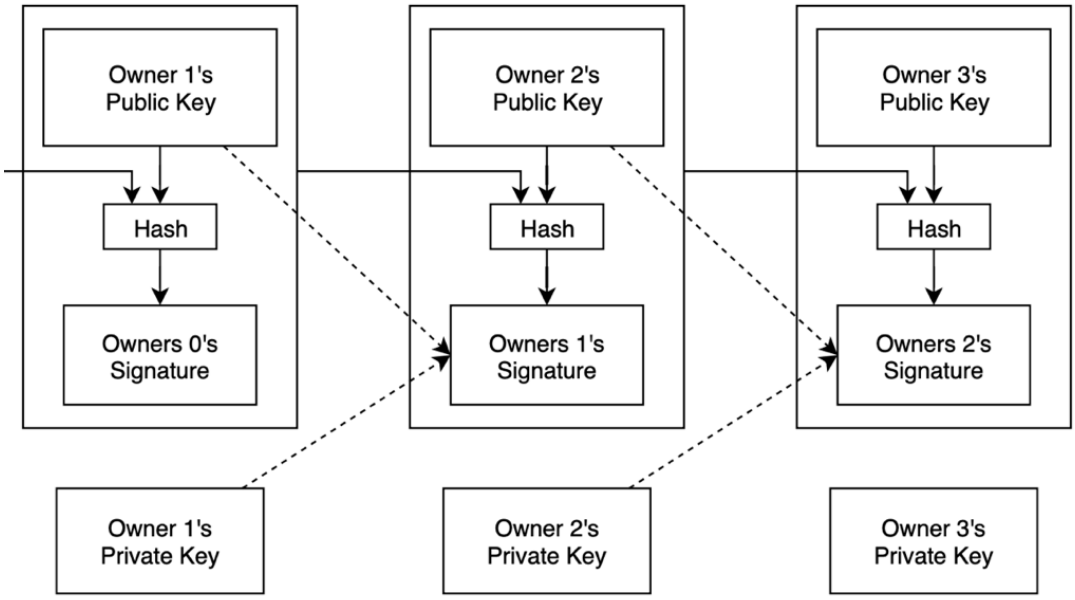

Рисунок 1.5 – Схема Bitcoin блокчейн протоколу

Ключовою особливістю біткойна можна вважати обмеженість пропозиції, з максимальною кількістю в 21 мільйон біткойнів. Це допомагає забезпечити довгострокову вартість і дефіцит валюти.

Сам біткойн набув широкого поширення за останні роки і став основним класом активів, багато компаній і приватних осіб використовують його як засіб платежу та інвестицій. Хоча біткойн був схильний до волатильності цін, він також продемонстрував значну стійкість і виявився популярним засобом збереження вартості та захистом від інфляції.

Однак біткойн не позбавлений проблем, включаючи проблеми з масштабованістю, проблеми з управлінням і регуляторні ризики. Таким чином, розвиток біткойна та ширшої екосистеми криптовалюти триває.

1.4.2 Ethereum

Ethereum — це децентралізована блокчейн-платформа, котра створює однорангову мережу та безпечно виконує й перевіряє код додатків, які називаються смарт-контрактами. Смарт-контракти дозволяють учасникам здійснювати операції один з одним без довіреного центрального органу. Записи транзакцій є незмінними, підлягають перевірці та безпечно поширюються в мережі, що дає учасникам повну власність і видимість даних транзакцій. Транзакції надсилаються та отримуються обліковими записами Ethereum, створеними користувачами. Відправник повинен підписувати транзакції та витрачати Ether, рідну криптовалюту Ethereum, як вартість обробки транзакцій у мережі.

Так само, як і Bitcoin, мережа Ethereum існує на тисячах комп'ютерів по всьому світу завдяки користувачам, які беруть участь як «вузли», а не як централізований сервер. Це робить мережу дуже захищеною від атак, і, по суті, ця мережа не може вийти з ладу. Якщо один комп'ютер вийде перестане працювати то тисячі інших підтримуватимуть мережу[6].

Ethereum — це, по суті, єдина децентралізована система, яка керує комп'ютером під назвою віртуальна машина Ethereum (EVM). Кожен вузол містить копію цього комп'ютера, тобто будь-яка взаємодія має бути перевірена, щоб кожен міг оновити свою копію. В інших випадках мережеві взаємодії вважаються «транзакціями» та зберігаються в блоках блокчейну Ethereum. Майнери перевіряють ці блоки перед тим, як передати їх у мережу та використовувати як історію транзакцій або цифрову книгу. Майнінг для перевірки транзакцій відомий як консенсусний метод підтвердження роботи (PoW). Кожен блок має унікальний 64-значний код, який його ідентифікує. Майнер витрачає свої комп'ютерні потужності на пошук цього коду, доводячи його унікальність. Їхня комп'ютерна потужність є «доказом» цієї роботи, і майнери отримують винагороду в ETH за свої зусилля.[19]

Хоча Ethereum платформа здається ідеальною, вона має кілька ключових проблем, які потрібно вирішити[4]:

- перша - це масштабованість. Засновник уявляв Ethereum таким, яким зараз є Інтернет, з мільйонами користувачів, які взаємодіють одночасно. Однак завдяки алгоритму консенсусу PoW така взаємодія обмежена часом перевірки блоку та платою за газ. Крім того, заважає децентралізація. Центральна організація, як-от Visa, керує всім і вдосконалила процес транзакцій.
- друга – це доступність. На момент написання Ethereum дорогий у розробці та складний у взаємодії для користувачів, які не знайомі з його технологією. Для деяких платформ потрібні спеціальні гаманці, а це означає, що потрібно перемістити ETH зі свого поточного гаманця на потрібний гаманець.

Загалом Ethereum — це потужна блокчейн-платформа, яка дозволила створювати широкий спектр децентралізованих програм і смарт-контрактів. Його гнучкість і універсальність зробили його популярним вибором для розробників і компаній, які прагнуть створювати децентралізовані програми та цифрові активи.

1.4.3 Основні відмінності Bitcoin та Ethereum протоколів

І Bitcoin, і Ethereum засновані на розподілених книгах і шифруванні, але мають значні технічні відмінності. Наприклад, біткойн в основному використовується як цифрове сховище вартості, тоді як криптовалюта Ethereum, ефір, використовується для живлення його мережі та програм[9].

Bitcoin та Ethereum дозволяють створювати нові токени, але вони використовують різні стандарти. Bitcoin використовує платформу рівня Omni, яка в основному була прийнята для стейблкоїнів. Ethereum, з іншого боку, використовує стандарт ERC-20, який визначає правила для токенів у мережі та вимагає від розробників впровадження функцій перед запуском своїх токенів.

Транзакції Bitcoin можуть містити примітки та повідомлення, а транзакції Ethereum можуть містити виконуваний код для смарт-контрактів і dApps.

Таблиця 1.1 – Порівняльна таблиця Bitcoin та Ethereum

Особливість	**Bitcoin**	**Ethereum**
Криптовалюта	Bitcoin (BTC)	Ether (ETH)
Призначення	Цифрова валюта, засіб збереження вартості	Смарт-контракти та dApps
Максимальна пропозиція	21 мільйон	Не зафіксовано
Швидкість транзакції	7 tps	15-45 tps
Час утворення блоку	10 хвилин	13-15 секунд
Адреса гаманця	Починається з 1, 3, "bc1"	Починається з "0x"
Алгоритм консенсусу	Proof-of-Work (PoW)	Перехід від PoW до PoS
Алгоритм майнінгу	SHA-256	Ethash
Використання	Сховище вартості, цифрове золото, грошові перекази	Децентралізовані фінанси (DeFi), NFT, DApps

1.5 Основні вразливості публічних блокчейн протоколів

Публічні блокчейн протоколи не можна вважати повністю невразливими до певних уразливостей, якими можуть скористатись зловмисники. Ці вразливості варіюються від слабких місць смарт-контрактів до проблем масштабованості, управління та безпеки. Розуміння кожної з цих вразливостей має вирішальне значення для користувачів і компаній, котрі задіяні в екосистемі блокчейну, щоб переконатися, що для зменшення ризиків та захисту своїх активів необхідне вживання відповідних заходів[8].

1.5.1 Атака 51%

Атака 51% — це тип атаки на протокол блокчейну, який відбувається, коли один суб’єкт або група контролює понад 51% обчислювальної потужності мережі. Цей контроль дозволяє зловмиснику маніпулювати блокчейном, скасовуючи транзакції, запобігаючи підтвердженню нових транзакцій або навіть створюючи нові блоки та додаючи їх до блокчейну[13].

Атака 51% може бути руйнівною для мережі блокчейн, оскільки вона підриває фундаментальну безпеку та довіру до мережі. Це може дозволити зловмисникам подвоїти витрати, викрасти кошти або маніпулювати блокчейном для власної вигоди. У деяких випадках атака 51% може призвести до повного знищення мережі блокчейн.

Наслідки, до яких може призвести успішне проведення Атаки 51%[13]:

- Подвійне витрачання монет: зловмисник може надіслати транзакцію одній стороні, а потім швидко створити іншу транзакцію, надсилаючи ті самі монети іншій стороні. Оскільки зловмисник контролює більшу частину хеш-рейту мережі, він може запобігти підтвердженню початкової транзакції, зробивши подвійно витрачену транзакцію єдиною дійсною.
- Скасування транзакцій: зловмисник може скасувати раніше підтверджені транзакції, створивши новий блок з іншою історією транзакцій. Це може призвести до плутанини та потенційно зашкодити користувачам, які покладалися на ці транзакції.
- Запобігання транзакціям: зловмисник також може запобігти підтвердженню транзакцій, що призведе до накопичення непідтверджених транзакцій і зниження продуктивності мережі.
- Шкода репутації мережі: успішна атака 51% може завдати шкоди репутації мережі блокчейн і призвести до втрати довіри користувачів до неї, що призведе до зниження рівня впровадження та зниження цінності.

Щоб запобігти атакам 51%, багато протоколів блокчейну використовують консенсусні алгоритми, які ускладнюють контроль над мережею для будь-якої окремої організації. Наприклад, протокол Bitcoin використовує алгоритм консенсусу Proof of Work (PoW), який вимагає від майнерів вирішення складних математичних задач для додавання нових блоків у блокчейн. Це ускладнює контроль над мережею будь-якій одній організації, оскільки для здійснення Атаки 51% їм потрібно буде контролювати більшість обчислювальної потужності в мережі.

Незважаючи на ці заходи, атаки 51% залишаються проблемою для багатьох блокчейн-мереж, особливо невеликих мереж, які можуть бути вразливими до атак.

1.5.2 Уразливості смарт-контрактів

Для виконання угоди, при якій всі сторони можуть бути впевнені в результаті без необхідності довіряти одна одній – використовують смарт-контракти. Вони гарантують, що виконання угоди буде відповідати логіці, прописаній в ньому, та після виконання попередньо визначеної логіки кінцевий стан мережі залишиться незмінним.

Але, на жаль, правильне виконання коду смарт-контракту не може гарантувати його повну безпеку. Насправді аналіз існуючих смарт-контрактів показує, що значна частина з них дійсно вразлива. Варто розглянути найпоширеніші проблеми з безпекою смарт-контрактів і слабкі їх сторони.

До ключових вразливостей смарт-контрактів відносяться[4]:

- Помилки кодування: смарт-контракти написані на таких мовах програмування, як Solidity, що вимагає від розробників обережності та точності. Помилки в коді можуть призвести до небажаних наслідків, зокрема до втрати коштів або несанкціонованого доступу.
- Атаки повторного входу: цей тип атаки відбувається, коли зловмиснику вдається неодноразово викликати функцію в смарт-контракті до завершення її початкового виконання. Це може призвести до виснаження коштів або інших небажаних наслідків.
- Обмеження газу: смарт-контракти покладаються на обмежену кількість обчислювальних ресурсів, відомих як «газ» у мережі Ethereum. Якщо для виконання контракту потрібно занадто багато газу, він може перестати реагувати або взагалі вийти з ладу.
- Маніпуляції з часовими мітками: майнери контролюють часові позначки блоків, які вони видобувають, якими потенційно можна

маніпулювати, щоб вплинути на результати смарт-контрактів, які залежать від умов, заснованих на часі.

- Відсутність конфіденційності: оскільки смарт-контракти зберігаються в загальнодоступному блокчейні, інформація, яку вони містять, доступна для перегляду всім. Це може спричинити проблеми з конфіденційністю, особливо коли йдеться про конфіденційну інформацію.
- Можливість оновлення та незмінність контракту: після розгортання смарт-контракту його код, як правило, залишається незмінним, що ускладнює виправлення помилок або оновлення контракту. Існують деякі методи створення смарт-контрактів, які можна оновлювати, але вони можуть створювати додаткові ризики для безпеки[16].
- Ризики централізації: хоча блокчейни децентралізовані за своєю природою, деякі смарт-контракти можуть покладатися на централізовані служби або компоненти, які можуть створювати єдині точки відмови або довіри.

У підсумку, смарт-контракти мають потенціал для революції в різних галузях шляхом автоматизації транзакцій і угод у децентралізований і прозорий спосіб. Однак, щоб повністю використати їхній потенціал, важливо усунути притаманні їм слабкі місця. Зменшуючи ризики, пов’язані з помилками кодування, атаками, обмеженнями газу, залежністю від даних, конфіденційністю, незмінністю, централізацією та нормативними проблемами, розробку та впровадження смарт-контрактів можна зробити більш безпечними та ефективними.

1.5.3 Уразливості алгоритму консенсусу

Алгоритми консенсусу блокчейну — це протоколи, які гарантують, що всі вузли в мережі погоджуються щодо вмісту розподіленої книги. Існує кілька консенсусних алгоритмів, кожен зі своїми сильними та слабкими сторонами. Варто розглянути два найпоширеніших консенсусних алгоритмів і їхні потенційні вразливості[7]:

1. Proof of Work (PoW): У PoW майнери змагаються у розв’язанні складної математичної задачі, і той, хто першим її розв’яже, додає наступний блок до ланцюжка. Хоча PoW є найбільш широко використовуваним механізмом консенсусу (наприклад, Bitcoin, Ethereum), він має деякі вразливості:

- Енергоспоживання: PoW є ресурсномістким і потребує значної кількості електроенергії, що робить його менш екологічним.
- Централізація: Високі вимоги до обчислень можуть призвести до централізації майнінгу, оскільки лише добре фінансовані організації можуть дозволити собі необхідне обладнання.

2. Proof of Stake (PoS): У PoS валідатори вибираються для створення нових блоків на основі їх частки (кількості криптовалюти), що зберігається, та інших факторів. PoS є більш енергоефективним, ніж PoW, але має свої вразливості[17]:

- Проблема «Нічого не поставлено на карту»: валідатори можуть не мати стимулу діяти чесно, оскільки мало що можна втратити, перевіривши кілька конфліктуючих ланцюжків, що потенційно може призвести до нестабільності мережі.
- Централізація: заможні зацікавлені сторони можуть накопичувати більше голосів, роблячи мережу більш централізованою та менш безпечною.
- Далекі атаки: зловмисник, який отримує старі закриті ключі, потенційно може створити альтернативний ланцюжок, починаючи зі старого блоку, що призведе до реорганізації ланцюжка та атак подвійного витрачання.

Хоча ці вразливості існують, поточні дослідження та розробки технології блокчейн спрямовані на підвищення безпеки, ефективності та децентралізації консенсусних алгоритмів для створення більш стійких мереж.

1.5.4 Фрагментація мережі

Фрагментація мережі блокчейну означає тимчасовий або постійний поділ мережі блокчейну на окремі підмережі, які не з’єднані між собою. Це може статися через різні причини, включаючи помилки програмного забезпечення, затримку мережі, DDoS-атаки або навіть навмисні спроби порушити роботу мережі. До причин виникнення фрагментації можна віднести наступне[11]:

- Помилки програмного забезпечення або розбіжності протоколів: несумісність між різними версіями клієнтського програмного забезпечення або оновленнями протоколів може спричинити розбіжності вузлів у їх інтерпретації правил блокчейну. Це може призвести до того, що деякі вузли не прийматимуть блоки від інших, що спричинить поділ мережі на окремі підмережі.
- Затримка мережі або розділення: висока затримка або розділення мережі можуть спричинити затримки в поширенні блоків, що призведе до тимчасової фрагментації. Протягом цього періоду вузли в різних підмережах можуть незалежно створювати конфліктні блоки, що може призвести до кількох конкуруючих ланцюжків[17].
- DDoS-атаки: розподілені атаки типу «відмова в обслуговуванні» (DDoS), націлені на ключові вузли або мережеву інфраструктуру, можуть спричинити перевантаження мережі або її збої, що призведе до тимчасової фрагментації мережі.
- Навмисне порушення роботи: зловмисники можуть навмисно намагатися фрагментувати мережу, використовуючи вразливі місця або створюючи суперечливі транзакції, які призводять до розбіжностей між вузлами.

Розглянувши можливі причини фрагментації мережі, доцільно розібрати наслідки. Отже, до основних, які тягне за собою фрагментована мережа, можна віднести наступне[12]:

- Атаки подвійного витрачання: зловмисник може використати фрагментацію для проведення атак подвійного витрачання, витрачаючи однакові монети в обох підмережах.
- Неузгоджена історія транзакцій: фрагментація може призвести до неузгодженості в історії транзакцій у підмережах, спричиняючи плутанину та можливі суперечки між користувачами.
- Знижена продуктивність: фрагментація може призвести до зниження продуктивності, оскільки загальні ресурси мережі розподіляються між підмережами. Це може призвести до сповільнення обробки транзакцій і зниження ефективності мережі.
- Проблеми з відновленням: повторне підключення фрагментованих підмереж може бути складним процесом, особливо якщо є невідповідності в історії транзакцій або численні конкуруючі ланцюжки. Це може вимагати ручного втручання, яке може зайняти багато часу та бути схильним до помилок.

1.5.5 Помилка користувача

Помилка користувача – одна з найпоширеніших вразливостей у мережі блокчейн, яка виникає через помилки користувачів під час взаємодії з системами на основі блокчейну. Незважаючи на високий рівень безпеки та незмінність блокчейну, помилка користувача може призвести до значних наслідків, таких як втрата коштів, розкриття конфіденційної інформації або компрометація всієї мережі.

Доцільно розглянути більш детально, до яких вразливостей приводить помилка користувача[15]:

- Керування приватними ключами: приватні ключі є важливими компонентами систем на основі блокчейну та використовуються для підписання транзакцій. Якщо користувач втратить свій приватний ключ, він втратить доступ до своїх коштів, що може призвести до значних фінансових

втрат. Крім того, якщо закритий ключ потрапляє в чужі руки, зловмисник може отримати доступ до коштів користувача, скомпрометувавши всю мережу.

- Фішингові атаки: фішингові атаки – це поширений тип помилок користувача, коли зловмисник використовує фальшивий веб-сайт або електронну пошту, щоб обманом змусити користувача розкрити свій закритий ключ або іншу конфіденційну інформацію. Це може призвести до втрати коштів або розкриття особистої інформації, що може скомпрометувати всю мережу[16].
- Неправильне введення адреси: під час переказу коштів між адресами блокчейну користувачі повинні вводити правильну адресу. Якщо користувач введе неправильну адресу, кошти можуть бути втрачені назавжди, що може поставити під загрозу всю мережу.
- Відсутність резервних копій: користувачі повинні переконатися, що вони мають резервні копії своїх особистих ключів та іншої конфіденційної інформації. Якщо користувач не зробить резервну копію своєї інформації, він може втратити доступ до своїх коштів або наражатися на інші вразливості.

Загалом помилка користувача є значною вразливістю в мережі блокчейн, тому під час взаємодії з системами на основі блокчейну обережність і дотримування найкращих практик, таких як:

- безпечне керування приватними ключами,
- перевірка автентичність веб-сайтів і електронних листів,
- перевірка деталей транзакції.

Висновки до розділу 1

У першому розділі проведено ознайомлення з основними поняттями блокчейн технологій та вразливостями, які їм притаманні.

Дані, які зберігають різні блокчейн протоколи в своїй структурі є однаковими, тож було проведено огляд структури блокчейну та п’яти рівнів, на

яких вона базується. До таких рівнів відносяться: апаратний, рівень даних, мережевий, консенсусу та прикладний, кожен з них відповідає за окрему частити роботи, а разом води забезпечуються цілісність та високий рівень безпеки блокчейну.

Порівняння двох найпопулярніших протоколів, Bitcoin та Ethereum, дозволило визначити їх основні властивості та особливості роботи, щоб надалі зосередитись на одному, для аналізу мережі.

Окрім цього, було проведено огляд основних вразливостей публічних блокчейн протоколів. Бо кожен з них, не є ідеальним та має власний набір недоліків.

2 ОЦІНКА ЕФЕКТИВНОСТІ БЛОКЧЕЙН ФОРЕНЗІКИ

Після ознайомлення з базовими теоретичними відомостями про блокчейн технологію та її вразливостями, постає задача визначити основні методи розслідування протиправних дій та їх запобігання[9].

Процес аналіз транзакцій блокчейну для виявлення та розслідування підозрілих дій стосується блокчейн криміналістики. Це все включає відстеження руху коштів, ідентифікацію залучених сторін і розуміння мети та характеру транзакцій.

Основна мета блокчейн криміналістики полягає в запобіганні та розслідуванні шахрайських дії, таких як відмивання грошей, фінансування тероризму та інші незаконні фінансові дії, які можуть відбуватися в мережах блокчейнів. Процес аналізу блокчейн транзакцій може виявити закономірності та взаємозв’язки між транзакціями, які можуть свідчити про злочинну діяльність, що може допомогти правоохоронним органам та іншим регуляторним органам вжити заходів проти зловмисників.

Також, блокчейнів форензіка важлива для забезпечення цілісності самого блокчейну шляхом виявлення та усунення вразливостей, якими можуть скористатися зловмисники. Це включає виявлення та відстеження руху вкрадених або незаконно отриманих цифрових активів, а також роботу з запобігання подібним атакам у майбутньому[17].

2.1 Принцип роботи блокчейн форензіки

Оскільки, популярність блокчейн технологій стрімко росте, то потреба в ефективних інструментах та техніках блокчейн форензіки для запобігання та розслідування фінансових злочинів стає все більш критичною. Принцип роботи блокчейн форензіки зосереджений на аналізі транзакцій блокчейну для виявлення підозрілих дій[20].

Процес блокчейн форензіки складається з кількох етапів, а саме:

- збір даних;
- аналіз даних;
- візуалізація результатів;
- представлення доказів;
- закриття розслідування.

На етапі збору даних відбувається вилучення даних з блокчейну, децентралізованої цифрової книги, яка записує транзакції безпечним і прозорим способом. Дані блокчейна є загальнодоступними, що дозволяє аналітикам отримувати доступ і перевіряти записи транзакцій, адреси та позначки часу.

Наступний етап – це аналіз отриманих даних для виявлення закономірностей і аномалій, які можуть вказувати на шахрайство або злочинну діяльність. Цей аналіз може передбачати використання методів інтелектуального аналізу даних, таких як кластеризація та класифікація, щоб ідентифікувати групи транзакцій, які пов’язані з підозрілою діяльністю[2].

На третьому етапі відбувається візуалізація отриманих результатів, для легкого розуміння результатів аналізу даних. Під цю категорію підпадають: діаграми, мережеві діаграми та інші візуальні представлення.

Останніми етапами є представлення доказів та закриття розслідування на основі проведеного аналізу. Результати аналізу представлені у спосіб, який є прийнятним у суді чи іншому судовому процесі. Це може включати підготовку звітів, представлення доказів і надання експертних свідчень.

Уже після завершення розслідування результати використовуються для вибору найкращого курсу дій. Це може призвести до звернення до суду, повернення викраденого майна та вживання інших заходів для запобігання фінансовим злочинам.

Таким чином, суть блокчейн форензіки полягає в її здатності забезпечувати прозорість, безпеку та цілісність екосистеми блокчейну шляхом виявлення, аналізу та дослідження транзакцій і дій у мережах[2].

2.2 Огляд методів проведення аналізу даних блокчейну

Технологія блокчейн, яка лежить в основі таких криптовалют, як Bitcoin та Ethereum, відома своєю безпекою, децентралізацією та прозорістю. Розподілена книга, яку він надає, дозволяє бачити всі транзакції кожному учаснику мережі, створюючи безпрецедентний рівень фінансової відкритості. Проте, незважаючи на те, що ця відкритість забезпечує численні переваги, це також створює проблеми, особливо щодо розуміння та інтерпретації величезних обсягів даних, які створюють блокчейни. Крім того, псевдонімна природа транзакцій блокчейну створює унікальний набір проблем, коли справа доходить до виявлення незаконної діяльності, шахрайства та інших форм неправомірного використання. Це породило аналіз даних блокчейну, також відомий як блокчейн форензіка[7].

Криміналістична експертиза блокчейну передбачає застосування різних методологій та інструментів для аналізу даних блокчейну з метою відстеження потоків транзакцій, виявлення закономірностей і вилучення корисної інформації. Ця сфера відіграє важливу роль у таких сферах, як кібербезпека, фінансове регулювання, правоохоронна діяльність та аналіз ринку.

Варто розглянути ключові методології, які використовуються в блокчейн форензіці, включаючи аналіз графів транзакцій, кластерний аналіз, аналіз часу, аналіз ринків та інтеграцію з зовнішніми дані ланцюга. Кожна з цих методологій надає унікальний погляд на дані блокчейну, і разом вони утворюють комплексний набір інструментів для розуміння та інтерпретації активності блокчейну[2].

2.2.1 Аналіз графу транзакцій

У криміналістиці блокчейнів аналіз графіка транзакцій – це метод, який широко використовується, цей метод передбачає дослідження того, як утворюються транзакції в блокчейні, на графіку.

На орієнтованому графі транзакцій блокчейну кожен вузол представляє адресу блокчейну, а кожне ребро представляє транзакцію між адресами. Напрямок краю показує, куди рухається криптовалюта від відправника до одержувача.

Цей метод аналізу може бути використаний кількома способами[12]:

1. Аналіз посилань: використовує відстеження транзакцій, щоб відстежувати, як криптовалюта рухається через мережу. Це може допомогти відстежувати гроші від моменту їх отримання до моменту їх повернення, і це може бути особливо корисним для виявлення можливого відмивання грошей або іншої незаконної діяльності.

2. Міри центральності: метри центральності дозволяють аналітикам визначити важливі вузли (адреси) у мережі. Наприклад, велика біржа або особа чи організація, яка має велику кількість криптовалюти — можуть бути прикладами вузлів із високим ступенем центральності. Це може бути корисним для розуміння того, як працює мережа.

3. Виявлення спільноти: визначення групи вузлів, які мають більші зв’язки один з одним, ніж решта мережі. Визначення цих спільнот може допомогти визначити групи адрес, які, можливо, підпорядковані одній організації.

4. Тимчасовий аналіз: через те, що кожна транзакція в блокчейні має часову мітку, аналітики можуть відстежувати графік транзакцій з часом, щоб виявити тенденції та закономірності. Це може допомогти визначити періоди високої активності, повторювані транзакції та інші пов’язані з часом закономірності.

5. Візуалізація мережі: потужний інструмент для кращого розуміння структури та динаміки мережі. Це може допомогти виділити шаблони або структури, які інакше було б важко виявити, тому це може бути особливо корисним, коли використовується разом з іншими методами аналізу.

За допомогою цього аналізу можна отримати значне розуміння процесів і потоку транзакцій, які відбуваються в блокчейні. Однак слід пам’ятати, що анонімність більшості блокчейнів складає проблему для остаточного встановлення

зв’язку між адресами та справжніми користувачами. Таким чином, аналіз графів транзакцій зазвичай використовується разом з іншими методами для підвищення точності та надійності аналізу.

2.2.2 Кластерний аналіз

У криміналістиці блокчейну кластерний аналіз використовується для групування адрес блокчейну за певними ознаками або поведінкою. Після цього ці кластери можна проаналізувати, щоб дізнатися про моделі транзакцій і, можливо, з’ясувати, хто контролює ці адреси. Кластерний аналіз базується на наступних основних елементах[2]:

1. Кластеризація адрес: концепція полягає в тому, що якщо дві або більше адрес є вхідними даними для однієї транзакції, вони, швидше за все, контролюються одним і тим же суб’єктом. По суті, людина, яка має кілька адрес, може використовувати ці адреси як вхідні дані в одній транзакції. Згрупувавши ці адреси, можна виявити одного користувача чи організацію, відповідального за кілька транзакцій[11].
2. Кластеризація спільних витрат: кілька адрес є частиною одного гаманця та, отже, єдиної сутності, що полегшує введення транзакції. Це типова евристика, яка використовується в кластерному аналізі.
3. Інтеграція даних поза мережею: додавання даних поза ланцюгом, таких як дані з ринків даркнету, соціальних мереж або бірж криптовалют, додає контексту до кластерів і може допомогти визначити, хто їх контролює. Це може бути особливо корисним для правоохоронних органів, які борються з незаконними діями.
4. Машинне навчання: алгоритми машинного навчання можуть використовуватися для групування адрес у розширених методах кластеризації. Це може бути особливо корисним, коли справа доходить до великих наборів даних, оскільки машинне навчання здатне виявити складні закономірності, які простіші методи можуть пропустити.

Хоча кластерний аналіз є ефективним інструментом для блокчейн форензіки, він має деякі обмеження. Блокчейн-транзакції є псевдонімами, тому дані транзакцій не пов’язані безпосередньо з людьми в реальному світі. Крім того, можна маскувати сліди транзакцій і ускладнювати кластеризацію за допомогою таких методів, як поєднання сервісів і монет конфіденційності. Таким чином, результати кластерного аналізу слід обережно інтерпретувати, а найкраще перевірити їх за допомогою інших методів або джерел даних[12].

2.2.3 Аналіз часу

Аналіз часу є невід’ємним аспектом блокчейн форензіки. Кожна транзакція, яка відбувається в блокчейні, супроводжується міткою часу, що забезпечує хронологічний запис усіх дій, що відбуваються. Ця важлива інформація дозволяє нам зрозуміти та інтерпретувати моделі транзакцій і поведінку протягом певного періоду часу. Під час проведення аналізу часу, варто звернути увагу на наступні моменти[15]:

1. Час транзакцій. Аналіз часу транзакцій може пролити світло на загальні закономірності в діяльності блокчейну. Наприклад, якщо користувач часто виконує транзакції в певний час або в певний день, це може свідчити про повторюваний шаблон, який може надати інформацію про особу користувача або його географічне розташування на основі часового поясу.

2. Кореляція ринкових подій: час торгівлі можна порівняти з помітними ринковими подіями. Наприклад, великі операції або сплески активності, які передують значним коливанням цін на криптовалюту, можуть свідчити про потенційне маніпулювання ринком або інсайдерську торгівлю. Ця кореляція може допомогти виявити незаконну діяльність.

3. Швидкість транзакцій. Аналіз швидкості транзакцій також може надати цінну інформацію. Швидке переміщення великих сум криптовалюти між кількома адресами може свідчити про спробу приховати сліди транзакції,

яка часто пов’язана з незаконною діяльністю або відмиванням грошей. Виявлення таких моделей допомагає виявити та запобігти шахрайству.

4. Інтервальні закономірності: ретельний аналіз часових інтервалів між транзакціями може виявити характерні закономірності. Регулярні проміжки часу можуть вказувати на автоматизований процес, наприклад звичайний платіж або переказ, тоді як нерегулярні проміжки часу можуть означати трансакцію, контрольовану людиною.

Використання вищезазначеної інформації для аналізу часу, допоможе більш глибоко розуміти поведінку користувачів і моделей транзакцій у блокчейні. Однак, як і у випадку з усіма методами блокчейн форензіки, необхідно дотримуватися прав користувачів на конфіденційність і забезпечити етичне використання цих даних.

2.2.4 Інтеграція з даними поза мережею

Інтеграція з автономними даними є цінним підходом до аналізу блокчейну. Концепція по суті передбачає поєднання аналізу даних транзакцій блокчейну з даними із зовнішніх джерел. Цей комбінований аналіз може надати більш повну картину транзакційної активності та потенційно ідентифікувати реальні особи, що стоять за адресами блокчейну. Ось деякі конкретні аспекти інтеграції даних поза ланцюгом у блокчейн-криміналістику[15]:

1. Соціальні медіа та онлайн-форуми: відкриті обговорення в різних соціальних мережах і онлайн-форумах можуть надати уявлення про поведінку певних адрес у блокчейні. Наприклад, користувачі можуть ділитися своїми власними блокчейн-адресами, згадувати транзакції, в яких вони брали участь, або обговорювати поведінку інших адрес. Зіставляючи ці дані, певні блокчейн-адреси можна пов’язати з конкретними особами чи організаціями.

2. Обмін криптовалюти та послуги гаманців: при реєстрації на біржах криптовалют або в службах гаманців користувачі зазвичай надають особисту ідентифікаційну інформацію. Ці дані поза ланцюгом можна використовувати

для пов’язування транзакцій у ланцюзі з ідентифікаторами реального світу. Однак важливо зазначити, що доступ до цих даних зазвичай обмежено через закони та норми про конфіденційність, і для отримання може знадобитися судовий процес.

3. Інтернет речей (IoT) та інші зовнішні джерела даних: зовнішні джерела даних також можуть бути корисними в певних контекстах. Наприклад, якщо пристрої IoT виконують транзакції в блокчейні, дані з цих пристроїв можна використовувати для виявлення шаблонів або аномалій у пов’язаних даних блокчейну.

Завдяки об’єднанню даних у ланцюзі та за його межами, криміналістика блокчейну може надати більш багате та повне уявлення про діяльність блокчейну. Однак цей метод також викликає серйозні занепокоєння щодо конфіденційності, тому його слід застосовувати з дотриманням прав особи на конфіденційність і відповідних законів і правил.

2.3 Основні метрики блокчейн форензіки

Блокчейн форензіка передбачає використання аналітичних методів та інструментів для дослідження та відстеження транзакцій у блокчейні. Перед початком проведення аналізу, варто визначити основі криміналістичні показники блокчейну.

Основні метрики блокчейну форензіки охоплюють ряд ключових аналітичних методів та інструментів, які використовуються для розслідування та відстеження транзакцій у мережі блокчейн. Він включає низку показників, включаючи обсяг транзакції, вартість транзакції, позначку часу транзакції, баланс адреси, розмір блоку, швидкість хешування та складність мережі. Ці показники можна використовувати для визначення моделей діяльності, відстеження руху коштів і оцінки безпеки мережі блокчейн[18].

Аналіз цих показники, блокчейн форензіки можуть виявити потенційну злочинну діяльність і надати докази правоохоронним органам.

Однак важливо зазначити, що блокчейн форензіка є складною галуззю, яка постійно розвивається, і в конкретних розслідуваннях можуть використовуватися додаткові показники та інструменти[14].

Таблиця 2.1 – Основні метрики блокчейн форензіки

№	Показник	Опис	Призначення	Цільові показники
1	Обсяг транзакції	Загальний обсяг транзакцій у мережі блокчейн за певний період.	Уявлення про загальну діяльність, тенденції та потенційні аномалії.	Раптові стрибки або падіння обсягу транзакцій.
2	Вартість транзакції	Загальна кількість транзакцій за певний період або за певною адресою.	Оцінка торгівельної діяльність, виявлення спроб приховати операції або зберегти анонімність.	Незвично висока або низька кількість транзакцій.
3	Баланс адреси	Кількість криптовалюти, що зберігається адресою в певний час.	Виявлення великих інвесторів або скупчення кіберзлочинців, виявлення раптових зміни балансу.	Великі залишки або раптові зміни балансу.
4	Забруднення	Відсоток «заплямованих» коштів у транзакції, отриманих із відомих незаконних джерел.	Визначення зв'язку коштів із незаконною діяльністю або встановлювати зв'язки між адресами.	Високий відсоток псування транзакцій.
5	Коефіцієнт кластеризації	Ступінь взаємопов’язаності адрес або вузлів у графі транзакцій.	Визначення потенційної змови або скоординовану діяльність.	Високі значення коефіцієнта кластеризації.
6	Оцінка виявлення аномалії	Оцінка, призначена транзакціям або адресам на основі відхилення від типової поведінки.	Сигналізування про потенційну незаконну діяльність, виявлення незвичайні закономірності чи зв’язки.	Високі показники виявлення аномалій.

Кінець таблиці 2.1

7	Оцінка ризику	Оцінка, присвоєна транзакціям або адресам на основі зв’язку з підозрілою чи незаконною діяльністю.	Визначення рівеня ризику, допомога у дотриманні AML та інших нормативних актів.	Високий рівень ризику.
8	Час підтвердження транзакції	Час, який потрібен, щоб транзакція була включена в блок і підтверджена мережею.	Визначення ефективність мережі та перевантаження, оцінка можливі затримки в обробці транзакцій.	Тривалий час підтвердження або нерегулярні шаблони.
9	Комісія за транзакцію	Комісія, пов’язана з транзакцією, сплачена майнерам або валідаторам за обробку та підтвердження транзакції.	Оцінка транзакційних витрат, визнення можливих маніпуляції з комісіями.	Незвично високі або низькі комісії за транзакції.

Використання цих метрик та методів дає можливість отримати цінну інформацію про діяльність, що відбувається в мережі блокчейн, і допомогти підтримувати цілісність і безпеку екосистеми.

2.4 Побудова алгоритму аналізу блокчейн мережі на основі протоколу Ethereum

Перед тим як безпосередньо перейти до побудови алгоритму форензіки блокчейн мережі Ethereum, варто визначити, яка інформація ляже в основу аналізу, а саме hash транзакції.

2.4.1 Структура гешу транзакції

Транзакції в Ethereum є однією з основних функцій, які відіграють роль єдиної речі, яка може змінювати або оновлювати стани Ethereum.

Геш/ідентифікатор транзакції (часто скорочено як tx hash або txn hash) — це унікальний ідентифікатор, схожий на квитанцію, який служить доказом того, що транзакцію було перевірено та додано до блокчейну. У багатьох випадках для визначення місцезнаходження коштів потрібен геш транзакції. Він також може бути використаний для надання підтвердження здійснення транзакції (подібно до отримання квитанції про покупку, коли ви купуєте щось у магазині).

Ідентифікатор транзакції містить наступні елементи:

- transaction nonce – це порядковий номер транзакцій, надісланих із заданої адреси. Кожного разу, коли ви надсилаєте транзакцію, значення nonce збільшується на одиницю. Крім того, nonce запобігає повторній атаці на блокчейн Ethereum.
- адреса гаманця відправника;
- адреса гаманця одержувача;
- підпис - використовується для автентифікації відправника. Транзакція підписується закритим ключем відправника;
- сума транзакції;
- дата та час проведення транзакції;
- газ, тобто комісія за виконання транзакції;
- ліміт газу;
- дані - це деякі довільні дані (для зберігання в блокчейні або введення у функцію смарт-контракту) або код необмеженого розміру. У випадку розгортання контракту транзакції це поле містить байт-код смарт-контракту.
- ідентифікатор ланцюга - використовується для захисту від повторного відтворення в різних ланцюгах. Ідентифікатор основного ланцюга 1.

Загалом, аналіз гешу транзакції передбачає визначення конкретних деталей та характеристик транзакції, які записані у блокчейні.

2.4.2 Алгоритм форензіки блокчейн мережі Ethereum

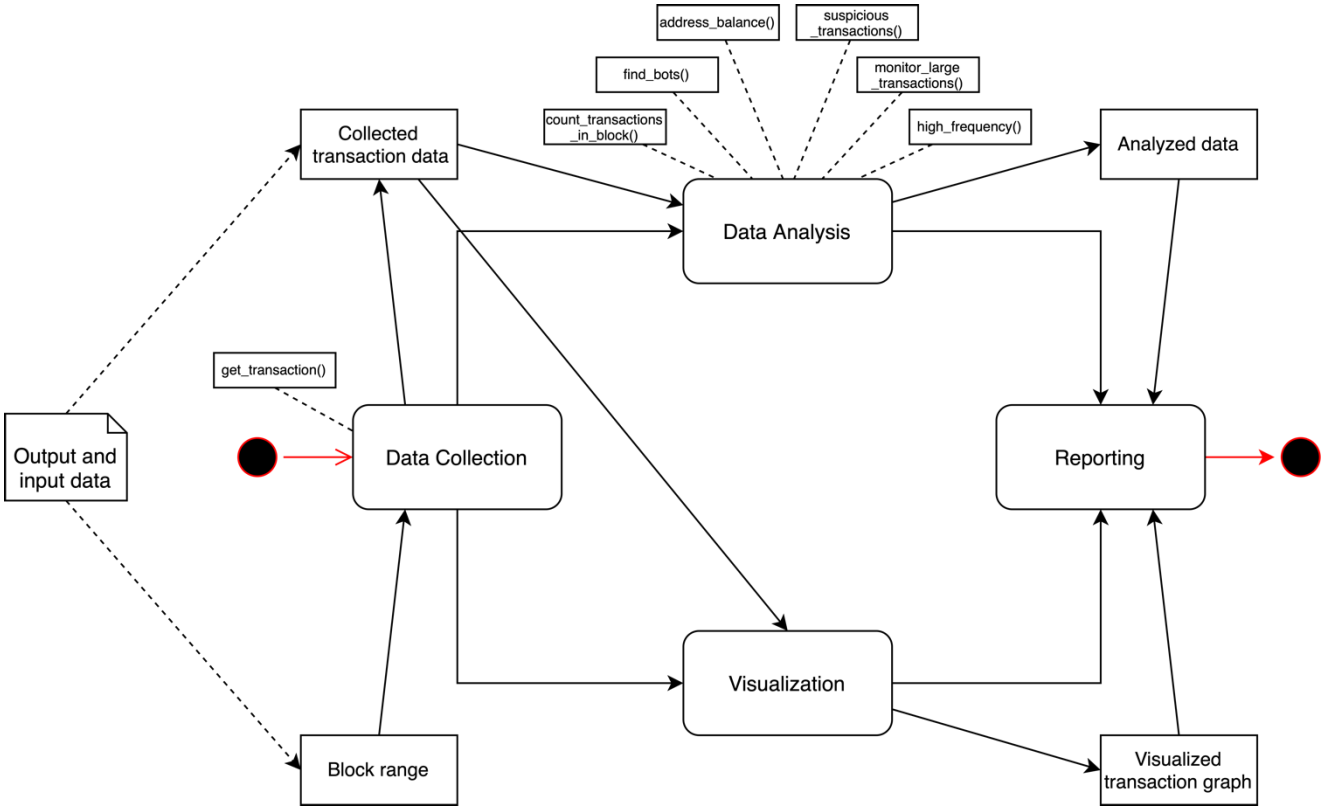

Рисунок 2.1 – Алгоритм форензіки блокчейн мережі Ethereum

Щоб провести аналіз мережі, необхідно визначити основні етапи для цього. Програмна реалізація відбуватиметься з дотриманням алгоритму форензіки, зображеного на Рисунку 2.1, та наступних етапів[17]:

1. Перший етап – збір даних. Використовуючи бібліотеку web3.py, можна точно отримати інформацію про транзакції в певному діапазоні блоків або проміжку часу. Для зручності можна скористатись сервісом infura.io, який надає простий доступ до Ethereum через API – кінцеві точки, що усуває необхідність у завантаженні повних вузлів локально та їх налаштуванні.

Для збору інформації використовується метод get_transaction(), який перебирає блоки транзакцій, розбиває їх та виділяє основні дані кожної транзакції, такі як[2]:

- "hash" – геш транзакції;
- "from" – адреса гаманця відправника;

- "to" – адреса гаманця отримувача;
- "value" – сума проведеної транзакції;
- "gasPrice" – комісія за виконання транзакції;
- "nonce" – це порядковий номер транзакції користувача.

2. Другий етап, основний, сам процес аналізу отриманих даних. Нижче наведені методи, які будуть використані для аналізу[2]:

- *count_transactions_in_block()* – метод, який підраховує кількість отриманих транзакцій з блоку.
- *address_balance()* – метод, який надає дані про баланс адреси.
- *suspicious_transactions()* – метод, який виявляє транзакції, які пов’язані з адресами гаманців з чорного списку.
- *find_bots()* – метод, що знаходить можливу активність боту.
- *monitor_large_transactions()* – метод, який виявляє транзакції, що були проведені на великі суми.
- *high_frequency()* – метод, який виявляє транзакції, які проводяться з великою частотою.

3. Візуалізація графу транзакцій – виявлення порушень в мережі за допомогою аналізу графа транзакцій є одним із ключових етапів. Використання методу мережевої кластеризації, що включає розпізнавання щільно пов'язаних адрес, допоможе виявити закономірності та структури в мережі, які можуть бути важко розпізнати іншими методами. Виявлення цих кластерів може сприяти виявленню координаційної діяльності, потенційно злочинних мереж або інших цікавих моделей. Аналізу графу транзакцій складається з наступних кцетапів:

- візуальний аналіз для виявлення потенційно підозрілих шаблонів або кластерів адрес.

4. Останній, четвертий етап - це створення звітності по проведеному аналізу. Цей етап буде містити:

- створення звіту, який міститиме відфільтровані транзакції та список адрес, які взаємодіють з адресами з чорного списку;

- виділення будь-яких очевидних моделі або незвичайних транзакції для подальшого дослідження.

У цілому, цей алгоритм полягає в дослідженні та розумінні току транзакцій, зв'язків у блокчейні та моделей поведінки. Він спрямований на відстеження та аналіз транзакцій транзакцій, що відбуваються в мережі Ethereum[20].

2.5 Проблеми у відстеженні діяльності кіберзлочинців

Блокчейн форензіка особливо важлива для відстеження незаконних дій, таких як відмивання грошей чи незаконна торгівля, оскільки для виконання таких транзакцій використовується блокчейн протоколи. Однак відстеження цієї діяльності не позбавлене проблем. До ключових проблем відносяться псевдонімність, послуги змішування та перемішування, децентралізація та відсутність стандартизації. Для більш глибшого розуміння проблему відстеженні протиправних дій, варто розглянути кожен приклад окремо[17]:

1. Псевдонімність: кожен користувач ідентифікується за його відкритим ключем, який ніяк не пов'язаний з ідентифікатором реального світу. Тож, розгадати приналежність будь якого гаманця конкретному користувачу стає складною задачею особливо без співпраці з різними біржами, які володіють даною інформацією.

2. Послуги змішування та перемішування: цей метод використовується для маскування сліду транзакцій шляхом змішування багатьох транзакцій разом перед відправленням їх до кінцевого пункту призначення.

3. Децентралізація: блокчейн — це глобальна децентралізована технологія. Таким чином, навіть якщо незаконну діяльність буде виявлено, юрисдикція та міжнародне право можуть ускладнити вжиття заходів[16].

4. Відсутність стандартизації: немає стандартної методології чи нормативної бази для блокчейн форензіки, що ускладнює координацію зусиль між різними юрисдикціями[8].

Навіть незважаючи на ці проблеми, процес блокчейн форензіки весь час розвивається, в свою чергу, співпраця між такими організаціями, як біржі криптовалют, уряди та фірми, що займаються аналізом блокчейнів, зростає. Однак збереження балансу між конфіденційністю та свободою, яку пропонує технологія блокчейн, і забезпеченням того, щоб вона не використовувалася для незаконної діяльності – нелегка задача.

Висновки до розділу 2

У другому розділі проведено аналіз етапів блокчейн форензіки, її методів, які включають у себе великий спекти різних методик аналізу блокчейн протоколів. Блокчейн форензіка складаються з 5 етапів: збір даних, аналіз даних, візуалізація результатів, представлення доказів, закриття розслідування, разом вони дають повну картину про взаємодію користувачів всередині блокчейну, а також можливість ідентифікувати незаконну діяльність. Також було визначено основні проблеми, які можуть виникнути у процесі виявлення кіберзлочинців.

Розгляд методів форензіки, викликав необхідність у визначенні основних метрик, за якими можна ідентифікувати протиправні дії, щоб реалізувати власний алгоритм форензіки.

Задача отримання важливих даних, дещо ускладнена, бо транзакції а блокчейн створюються безперервно, що потребує чіткого розподілення ресурсу та послідовності дій. Щодо процесу створення алгоритму форензіки – було визначено 4 етапи, та основні методи, які будуть використані під час проведення аналізу мережі. А також, одним із етапів було виділено візуалізацію графу транзакцій, щоб визначити кластеризацію мережі, що не дасть допустити централізацію.

3 РОЗРОБКА РІШЕННЯ ДЛЯ ВІДСТЕЖЕННЯ ДІЯЛЬНОСТІ КІБЕРЗЛОЧИНЦІВ У ПУБЛІЧНОМУ БЛОКЧЕЙНІ

3.1 Програмне забезпечення

Програмна реалізація виконана на мові програмування Python 3.10. Для алгоритму форензіки було використано наступні сервіси та бібліотеки:

- infura.io – сервіс, який надає доступ до ноди криптовалюти, без потреби локального налаштування;
- web3 – бібліотека, яка дозволяє взаємодіяти з нодами криптовалют, у моєму випадку – це Ethereum;
- numpy – бібліотека, яка призначена для роботи з двомірними масивами;
- pandas – бібліотека, яка призначена для роботи з data frame.

Тестування програми буде проведено на даних транзакцій отриманих з останнього створеного, на момент запуску, блоку мережі Ethereum.

Операційна система: MacOS.

3.2 Аналіз блокчейн мережі на основі протоколу Ethereum

Перед переходом до безпосереднього аналізу мережі, варто зібрати дані про транзакції та визначити їх кількість в блоці. Необхідно використати метод *get_transaction()*, який може зібрати інформацію про всі транзакції наявні в останньому блоці разом з такою інформацією, як геш транзакції, адреса гаманця відправника, адреса гаманця отримувача, сума проведеної транзакції, комісія за виконання транзакції, порядковий номер транзакції користувача.

А за допомогою метода *count_transactions_in_block()* можна визначити кількість транзакцій в поточному блоці блокчейну. Сама реалізацій полягає лише в отриманні довжини масиву транзакцій з методу *get_transaction()*. На рисунку 3.1 наведено реалізацію методів збору даних та визначення кількість транзакцій за допомогою зазначених раніше методів:

```python
def get_transaction(w3, block_number):
    block = w3.eth.get_block(block_number, full_transactions=True)
    transactions = block["transactions"]

    with open("transactions.txt", "w") as f:
        for tx in transactions:
            f.write(f"Transaction hash: {tx['hash'].hex()}\n")
            f.write(f"From address: {tx['from']}\n")
            f.write(f"To address: {tx['to']}\n")
            f.write(f"Value: {w3.from_wei(tx['value'], 'ether')} ether\n")
            f.write(f"Gas price: {w3.from_wei(tx['gasPrice'], 'gwei')} gwei\n")
            f.write(f"Nonce: {tx['nonce']}\n")
            f.write("-----------------------------------------------------\n")

    return transactions


def count_transactions_in_block(transactions):
    return len(transactions)
```

Рисунок 3.1 – Програмна реалізація методу *get_transaction()* та *count_transactions_in_block()*

Також на рисунку 3.1, що данні записуються в для їх використання в визуалізації графу транзакцій.

3.2.1 Визначення балансу адрес

Використовуючи вже отримані дані з методу *get_transaction()*, можна скористатися значенням адреса відправників (“from”) та отримувачів (“to”), та використавши метод з бібліотеки web3 – *get_balance()*, який поверне значення балансу на гаманці кожного учасника транзакції. Отримані дані будуть зберігатись у масив, щоб відсортувавши, можна було визначити адреси, які мають на своєму балансі велику суму грошей. Це також дозволить виявити незаконну діяльність, бо нараз зберігання великих коштів на гаманці є досить ризиковим та може призвести до втрати кошті. Наразі рекомендується збереження коштів на «холодних гаманцях», а саме спеціальних флешках. На русинку 3.2 наведено реалізацію методу отримання балансу адрес гаманців відправників та одержувачів:

```python
def address_balance(transactions):
    address_balance_from = np.empty(shape=[0,2])
    address_balance_to = np.empty(shape=[0,2])
    start_time = time.time()
    print(green_plus + f"Getting address balance started")

    with open("address_balance.txt", "w") as f:
        for tx in transactions:
            address_from = tx["from"]
            balance_from = w3.eth.get_balance(address_from)
            balance = w3.from_wei(balance_from, "ether")
            f.write(f"[FROM] Address: {address_from}, Balance: {balance} ETH\n")
            address_balance_from = np.append(address_balance_from, [[address_from, balance]], axis=0)
        for tx in transactions:
            address_to = tx["to"]
            balance_to = w3.eth.get_balance(address_to)
            balance = w3.from_wei(balance_to, "ether")
            f.write(f"[TO] Address: {address_to}, Balance: {balance} ETH\n")
            address_balance_to = np.append(address_balance_to, [[address_to, balance]], axis=0)

    print(green_plus + f"Getting address ended in {round(time.time() - start_time)} seconds")
    return address_balance_from, address_balance_to
```

Рисунок 3.2 – Метод визначення балансу адрес гаманців

3.2.2 Визначення взаємодії з чорним списком гаманців

Наразі, вже є сформовано список адреса гаманців користувачів, які входять до чорного списку. Ці адреси могли бути спіймані на спамі або фішингу, тому дуже доречним є перевірити отримані адреси з блоку на взаємодію з цими адресами, бо це може вказувати на потенційний зв’язок власників даних гаманців. Імплементація досить проста, і полягає в порівнянні всіх отриманих з блоку адрес з адресами з чорного списку гаманців. На русинку 3.3 наведено реалізацію методу виявлення взаємодії з чорним списком:

```python
def suspicious_transactions(transactions):
    start_time = time.time()
    print(green_plus + f"Finding suspicious transactions started")

    for tx in transactions:
        if tx["from"] in known_malicious_addresses or tx["to"] in known_malicious_addresses:
            print(red_x + f"\tSuspicious_transaction: {tx}")

    print(green_plus + f"Finding suspicious transactions ended in {time.time() - start_time} seconds")
```

Рисунок 3.3 – Метод перевірки на взаємодію з чорним списком адрес

3.2.3 Виявлення активності ботів

Світ криптовалюти не виключає наявності ботів. Так, як блок створюється дуже швидко, варто проаналізувати поточний блок на наявність адреси на яку відправлені кошти хоча б два рази. Звісно, це не буде 100% свідчити про те, що це бот, але зібравши більше інформації про задану адресу, можна зробити висновки. У реалізації варто лише творити словник, та збільшувати значення “value” на один, кожен раз коли поточний гаманець зустрічається повторно. На русинку 3.4 наведено реалізацію методу виявлення активності ботів:

```python
def find_bots(transactions):
    start_time = time.time()
    print(green_plus + f"Finding bots activity started")

    toFromPairs = {}
    transactionCount = {}
    for tx in transactions:
        if tx["to"] != None:
            if tx.to in toFromPairs:
                if toFromPairs[tx["to"]] == tx["from"]:
                    transactionCount[tx["to"]] = transactionCount[tx["to"]] + 1
            elif tx["to"] not in toFromPairs:
                transactionCount[tx.to] = 1
                toFromPairs[tx["to"]] = tx["from"]

    for key, value in transactionCount.items():
        if value == 2:
            print("\t" + red_x + f"Bot: {toFromPairs[key]}")

    print(green_plus + f"Finding bots activity ended in {time.time() - start_time} seconds")
```

Рисунок 3.4 – Метод виявлення активності ботів

3.2.4 Виявлення великих транзакцій

Разовий платіж на суму більше 20 ETH, що еквівалентно 1 409 931.06 UAH може визвати підозри. Тому не завадить проаналізувати блок, на наявність таких транзакцій, щоб визначити є сліди незаконної діяльності через виведення великих коштів. На русинку 3.5 наведено реалізацію методу виявлення транзакцій на великі суми коштів:

```python
def monitor_large_transactions(transactions):
    start_time = time.time()
    print(green_plus + f"Finding large transactions started")

    large_amount = 20
    for tx in transactions:
        value_ether = w3.from_wei(tx["value"], "ether")
        if value_ether > large_amount:
            print("\t" + red_x + f"Large transaction found:")
            print(f"\t\tFrom: {tx['from']}")
            print(f"\t\tTo: {tx['to']}")
            print(f"\t\tValue: {value_ether} ether")

    print(green_plus + f"Finding large transactions ended in {time.time() - start_time} seconds")
```

Рисунок 3.5 – Метод виявлення великих транзакцій

3.2.5 Виявлення транзакцій, з великою частотою

Один з основних методів, це виявлення гаманців, які проводять транзакції з високою частою. Висока активність також може свідчити про незаконну діяльність. Реалізація полягає в отриманні адрес з декількох блоків з подальшим доданням транзакцій в словник та підрахунком кількості транзакцій кожного гаманця. На русинку 3.5 наведено реалізацію методу виявлення гаманців, що часто проводили транзакції:

```python
def high_frequency(w3, start_block, end_block):
    start_time = time.time()
    print(green_plus + f"Finding high frequency transactions started")

    transactions = []
    for i in range(start_block, end_block):
        block = w3.eth.get_block(i)
        for transaction in block.transactions:
            tx = w3.eth.get_transaction(transaction)
            transactions.append({'from': tx['from'], 'to': tx['to']})

    df = pd.DataFrame(transactions)

    print(df['from'].value_counts())
    print(df['to'].value_counts())

    print(green_plus + f"Finding high frequency transactions ended in {time.time() - start_time} seconds")
```

Рисунок 3.6 – Метод транзакцій з високою частотою

3.3 Візуалізація графу транзакцій

Для візуалізації графу транзакцій буде використано програму Gephi, для цього знадобляться адреси гаманців відправників та отримувачів, які будуть виступати вершинами, а їх взаємодія – це ребра графу. Для візуалізації вже отримано дані з алгоритму, тож можна приступити. Варто лише завантажити два .csv файл, один просто з адресами всіх гаманців, другий з їх взаємодією (тобто від кого кому надходити кошти) до програми та буде отримано результат.

1. Спочатку завантажую лише адреси всіх гаманців, без вказування на їх взаємодію. На рисунку 3.7, що отримано лише вершини графу.

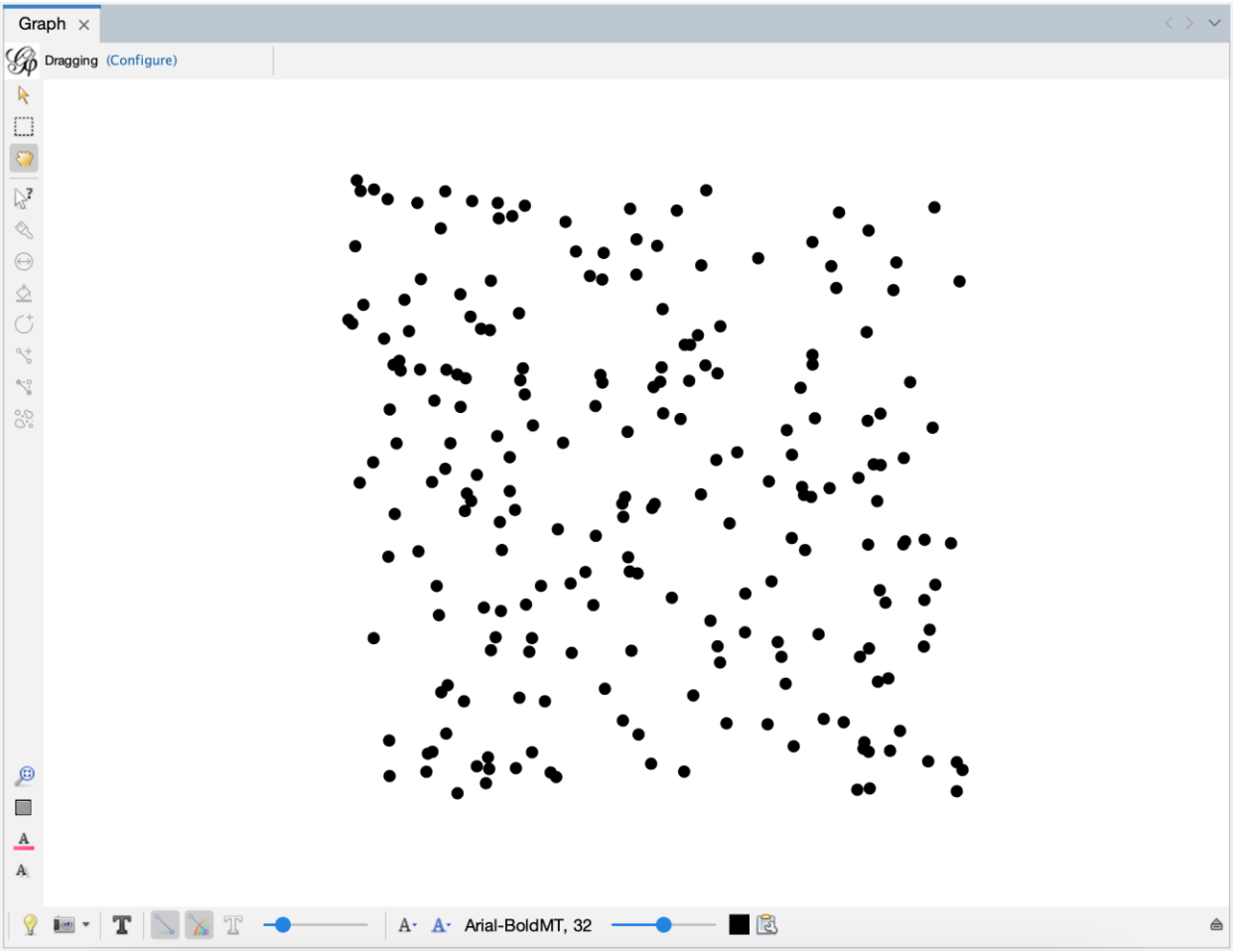

Рисунок 3.7 – Вершини графу транзакцій

2. Далі завантажую файл з вказівками, від якого гаманця до якого були направлені кошти та отримую кінцевий результат графу транзакцій, який зображено на рисунку 3.8:

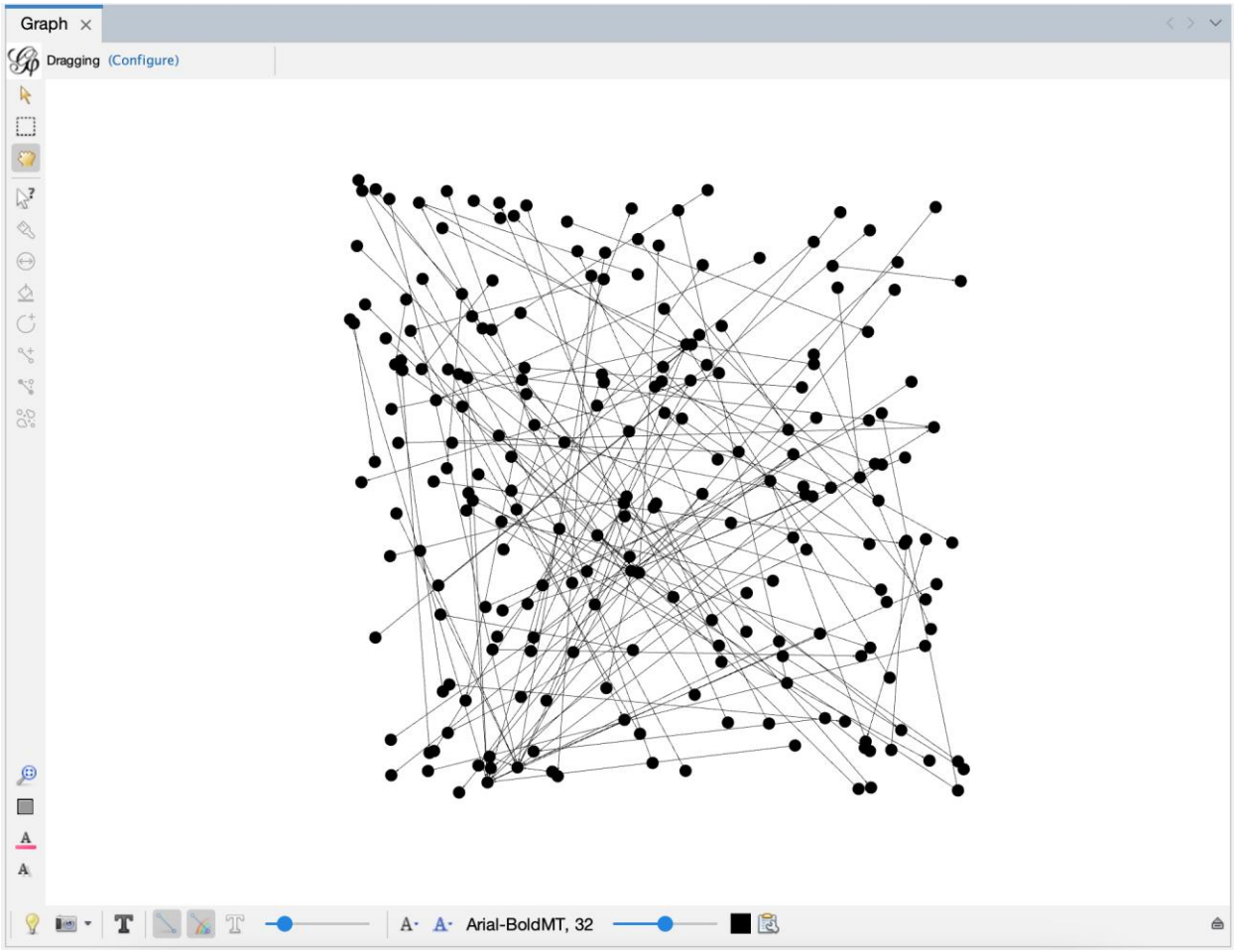

Рисунок 3.8 – Візуалізація графу транзакцій

І останній етап, це провести огляд графу задля виявлення кластеризації. Скориставшись можливостями Gephi, на русинку 3.9 видно, що виділено три адреси, які мають найбільшу кількість ребер (взаємодій з іншими гаманцями) в графі транзакцій. Це може вказувати на кластеризацію мережі. Проте аналіз проводиться на дуже незначному об’ємі даних, щоб робити висновки, щодо кластеризації мережі Ethereum.

Рисунок 3.9 – Кластеризація мережі

3.4 Визначення зловмисних адрес

При проведенні аналізу мережі Ethereum за допомогою програмної реалізації (Додаток А) алгоритму форензіки, отримали результат (рисунок 3.7), тобто адреси, які потенційно можуть бути зловмисними. Можна побачити, що в поточному блоці № 17405986 проведено 138 транзакцій, адрес з великим балансом більше 20 тис ETH нараховано 10, знайдено одну велику транзакцію на суму 37 ETH, а також виявлено активність одного бота. Проте, отримані дані треба перевірити.

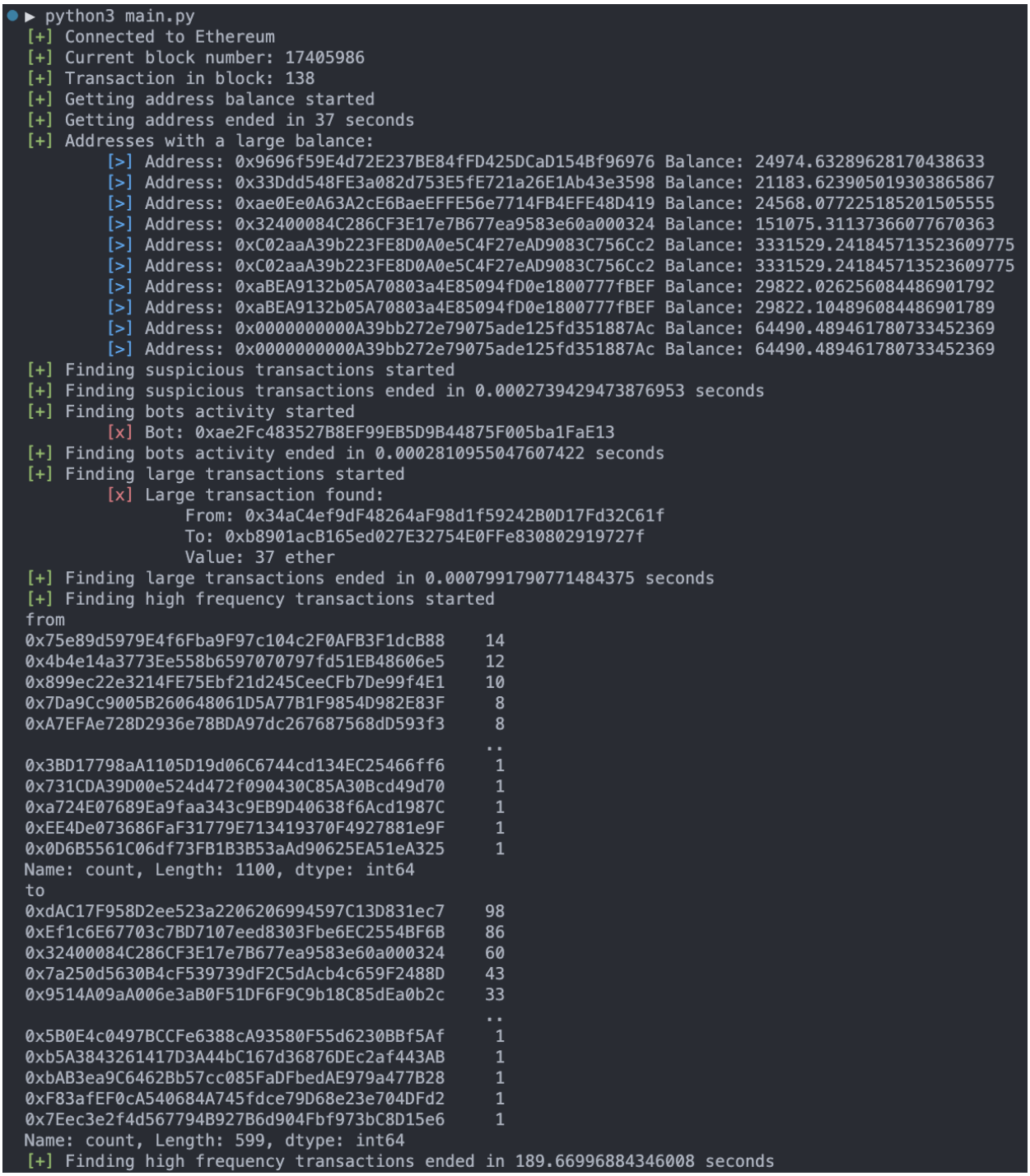

Рисунок 3.10 – Результат роботи алгоритму форензіки

Скориставшись сервісом etherscan.io, який дозволяє отримати інформацію про будь-який гаманець, таку як баланс, усі дані транзакцій, можна перевірити результат аналізу блокчейн мережі на основі протоколу Ethereum.

Для початку, потрібно перевірити відповідність балансу знайдених адрес. Дивлячись на рисунок 3.7, можна взяти декілька адрес гаманців та перевірити їх

баланс з використанням сервісу etherscan.io. На рисунку 3.8 можна побачити отримані результати перевірки чотирьох адрес і можна зробити висновок, що вони співпадають з даними аналізу мережі.

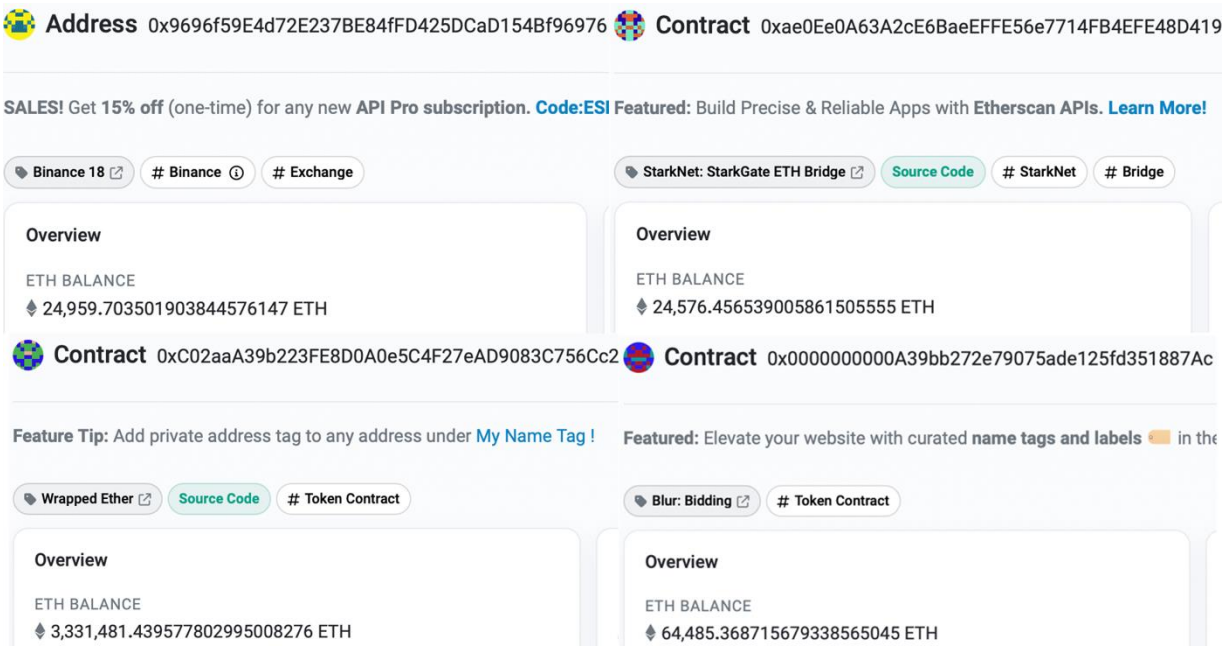

Рисунок 3.11 – Баланси знайдених адрес

Так, як знайдено активність одного бота, варто перевірити всі його транзакції, щоб впевнитись у правильності роботи алгоритму. Перевіривши адресу: 0xae2Fc483527B8EF99EB5D9B44875F005ba1FaE13, на рисунку 3.9 можна побачити, що, дійсно, з цієї адреси було багато переказів на один і той самий гаманець, з дуже маленьким інтервалом часу. І також видно, що кошти були переказані на гаманець з назвою MEV Bot, тож правильність визначення ботів в мережі також можна підтвердити.

ETH Price: $1,900.22 (-0.15%) Gas: 20 Gwei

0xae2Fc483527B8EF99EB5D9B44875F005ba1FaE13

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0xc1462a3285f7e9597...	0xad341e2c	17406125	32 secs ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.06177573
0x9770842888d5fbff9a...	0xad753e2c	17406125	32 secs ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00450771
0x512702677c6c805ea...	0xa82f1f82	17406120	1 min ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.01079076
0x663dd0cee34467181...	0xa86b3f82	17406120	1 min ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00238997
0x6f5abe0c665c9a2fbb...	0xa36b3e8a	17406115	2 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.01411613
0x3a73f1f92d9a107c12...	0xa32f1e8a	17406115	2 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00222577
0xbd9d3f4501ac90687...	0xa36b3e8a	17406115	2 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00229109
0x0e21f1c233030612a...	0xa175397d	17406113	2 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.01238468
0x023791f061039c765...	0xa134197d	17406113	2 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00286952
0xbafcc30495ed8d5b6...	0x9f6b3cdb	17406111	3 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00201387
0x29232f5295639a61e...	0x9f2f1cdb	17406111	3 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00217675
0x7abfb285b4ae3a0b1...	0x9e7538da	17406110	3 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.01132045
0x3245a220176f22edb...	0x9e3418da	17406110	3 mins ago	jaredfromsubway.eth	OUT MEV Bot: 0x6b7...A80	0 ETH	0.00305071

Рисунок 3.12 – Активність бота

Також було знайдено одну велику транзакцію на суму 37 ETH, що еквівалентно 2 608 372.47 UAH. Також, аби впевнитись у правильності знайденого, потрібно перевірити знайдену транзакцію. На рисунку 3.10 видно6 що така транзакація існує, проте вона не є зловмисною6 це лише перекидання коштів на інший блокчейн протокол.

From: 0x34aC4ef9dF48264aF98d1f59242B0D17Fd32C61f

To: 0xb8901acB165ed027E32754E0FFe830802919727f (Hop Protocol: Ethereum Bridge)

Transfer 0.000046972587758992 ETH From 0xDD378a...ABda5434 To Arbitrum: Delayed Inbox

Transfer 0.000046972587758992 ETH From Arbitrum: Delayed Inbox To Arbitrum: Bridge

Value: 37 ETH ($70,277.80)

Transaction Fee: 0.0025784182669782 ETH ($4.90)

Gas Price: 19.574994435 Gwei (0.000000019574994435 ETH)

Рисунок 3.13 – Інформація про велику транзакцію

І останнє, це перевірка великої частоти транзакцій, для цього було взято інформацію з останній 10 блоків мережі Ehereum. Як видно на рисунку 3.7, то знайдено 5 гаманців, які виконали більше 30 транзакцій, проте найцікавішими будуть лише перші два гаманця.

- Адреса 0xdAC17F958D2ee523a2206206994597C13D831ec7 здійснила 98 транзакцій за останні 10 створених блоків. На рисунку 3.11 видно, що лише за 40 секунд було здійснено 14 транзакцій.

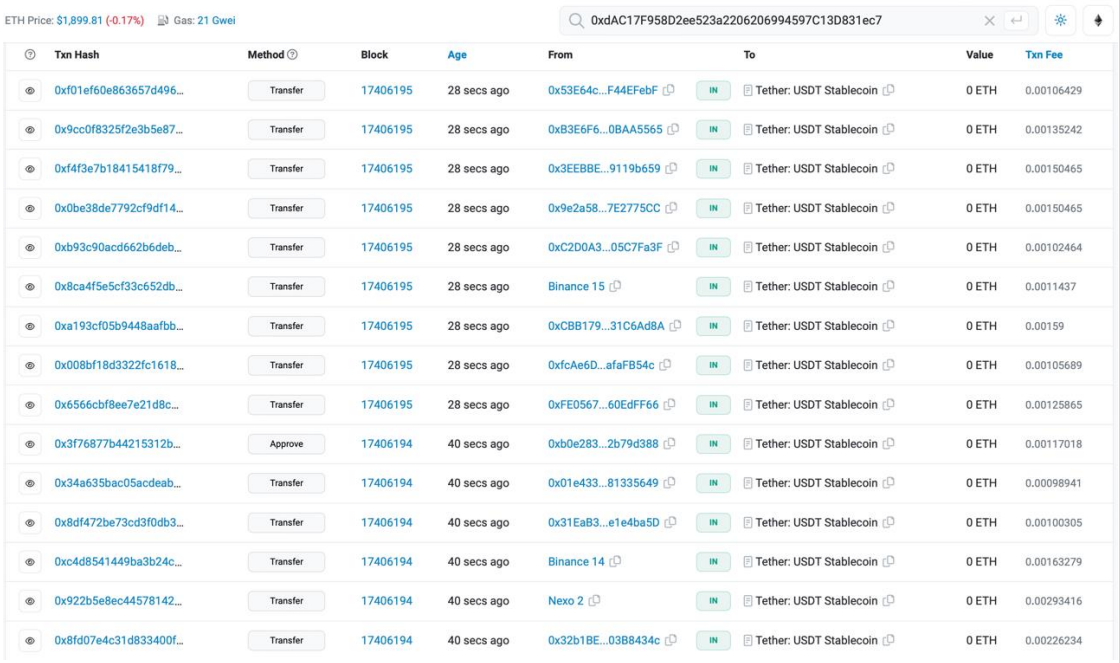

Рисунок 3.14 – Транзакції обраного гаманця

- Адреса 0xEf1c6E67703c7BD7107eed8303Fbe6EC2554BF6B здійснила 86 транзакцій за останні 10 створених блоків. На рисунку 3.12 видно, що лише за 20 секунд було здійснено 14 транзакцій.

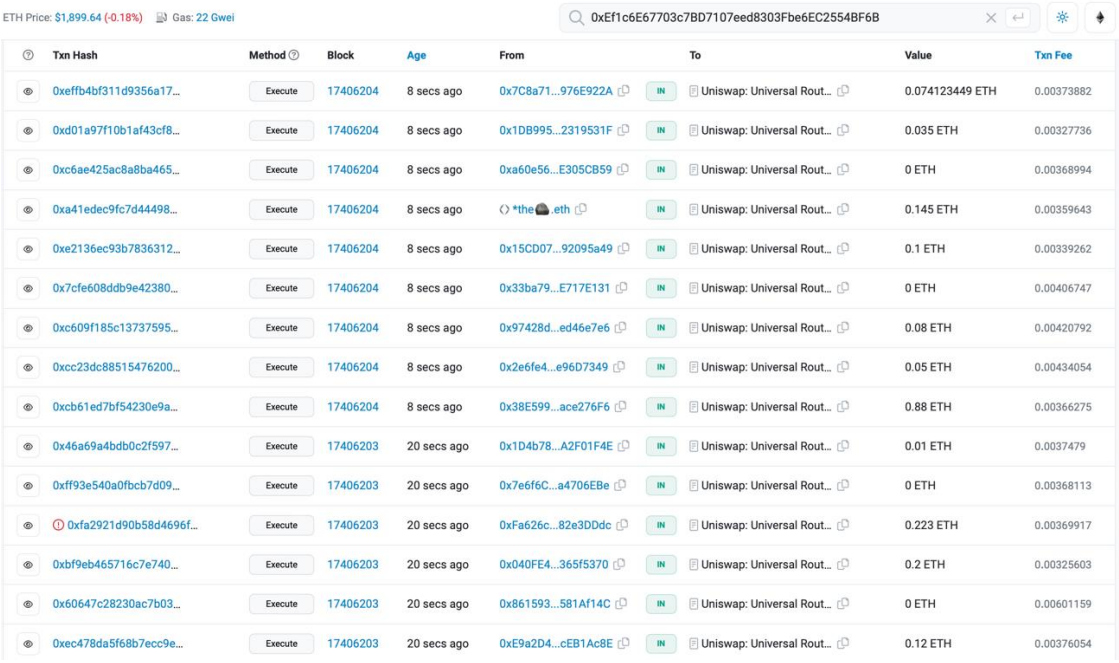

Рисунок 3.15 – Транзакції обраного гаманця

Проте жодна з цих транзакцій не несе кримінального характеру, бо це лише обмін криптовалюти або зміна протоколу.

Отже, можна впевнитись, що робота алгоритму форензіки коректна та запропонована реалізацій може буду використана для аналізу блокчейн мережі на основі протоколу Ethereum.

Висновки до розділу 3

За результатами реалізації алгоритму форензіки мережі Ethereum було проаналізовано блок транзакцій і як результат, отримано набір адрес, які потенційно можуть бути задіяні в незаконній діяльності.

Отримані адреси, було використано для візуалізації графу транзакцій, щоб виявити кластеризацію адрес мережі. Було отримано три потенційні кластеризації, проте за цими результатними не можна 100% говорити про появу центраралізації в мережі.

Даний алгоритм форензіки спроможний вдало виявити зловмисні адреси та в подальшому може застосовуватись для покращення мережі та запобігання подальшій зловмисній активності.

ВИСНОВКИ

У ході виконання дипломної роботи було досліджено та оцінено потенціал блокчейн технологій з особливим акцентом на публічних блокчейнах. Було вивчено архітектуру, переваги та вразливості популярних публічних протоколів блокчейну, щоб зрозуміти, чи доцільно проводити моніторинг кіберзлочинної діяльності в цих мережах.

Детально було досліджено принци роботи блокчейн форензіки, особлива увага була привернута до різних методів аналізу даних блокчейну. Незважаючи на децентралізованість та псевдонімність певні шаблони, метрики, можна використовувати для відстеження незаконних дій.

Згодом, було розроблено запропонований алгоритм форензіки для виявлення незаконної діяльності в мережі блокчейну Ethereum. Це передбачало створення програмного забезпечення, здатного аналізувати мережу блокчейну, візуалізувати графік транзакцій і ідентифікувати зловмисні адреси.

Висновки можна сформувати за виконаними завданнями:

1. Розглянуто принцип роботи, основні вразливості блокчейн мережі на основні протоколу Ethereum. Було проведено огляд основних понять протоколу Ethereum та вразливостей, які найчастіше зустрічаються в ньому.

2. Визначено основні метрики ідентифікації незаконної діяльності, що дозволило більш ефективно провести аналіз мережі публічного блокчейну.

3. Побудовано схему оптимального алгоритму форензіки та дослідження блокчейн мережі, який включає аналіз транзакцій та візуалізацію графу транзакцій на предмет незаконної діяльності, який забезпечує безпеку мережі криптовалюти.

4. Програмно реалізовано запропонований алгоритм форензіки, який допоміг виявити та проаналізувати блок № 17405986, який містив 10 адрес з великим балансом (більше 20 тис. ETH), одну велику транзакцію на суму 37 ETH, а також активність одного бота.

5. Виконано візуалізацію графу транзакцій та в ході аналізу, виявлено три потенційні кластеризації.

Дослідження показало, що хоча технологія блокчейну надає можливості для інновацій, але з іншого боку також присутні можливості для зловживання, тому можна підвищити безпеку публічних блокчейн протоколів.

Доцільно зауважити, що наразі алгоритм форензіки працює лише з протоколом Ethereum та має в основі обмежений спектр метрик ідентифікації зловмисників, проте, за умови вдосконалення, результати дослідження можуть слугувати сходинкою до широкого застосування алгоритму форензіки

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. What Is Blockchain Technology? [Електронний ресурс] – Режим доступу: https://aws.amazon.com/what-is/blockchain/.

2. Абдуллаєва Е. В., Гальчинський Л. Ю. Алгоритм форензіки блокчейн мережі Ethereum для виявлення незаконної діяльності [Електронний ресурс] // Теоретичні та прикладні проблеми фізики, математики та інформатики – 2023 – С. 225-227 – Режим доступу: http://conf.ipt.kpi.ua/.

3. What Is Blockchain Technology? [Електронний ресурс] – Режим доступу: https://www.ibm.com/topics/blockchain/.

4. Топчій М. А., Гальчинський Л. Ю. Підвищення рівня безпеки смарт-контрактів від шахрайства за рахунок використання реверсивних токенів [Електронний ресурс] – 2022 – С. 225-227 – Режим доступу: https://ela.kpi.ua/.

5. Що таке блокчейн? [Електронний ресурс] – 2019 – Режим доступу: https://academy.binance.com/.

6. Salisu S., Filipov V., Penne B. Blockchain Forensics: A Modern Approach to Investigating Cybercrimes in the Age of Decentralisation [Електронний ресурс] – 2022 – С. 9-10 – Режим доступу: https://osf.io/dbf4n.

7. Venkat Narayana Rao T., Purva Pravin Likhar, Muralidhar Kurni, Saritha K. Blockchain: A new perspective in cyber technology [Електронний ресурс] – 2022 – С. 33-66 – Режим доступу: https://www.sciencedirect.com/science/.

8. Kovalcik T. Digital forensics of cryptocurrency wallet [Електронний ресурс] – 2022 – С. 14-22 – Режим доступу: https://www.diva-portal.org/.

9. Goyal H., Shekhar B. Blockchain Forensics in Policing and It's Global Scenario [Електронний ресурс] // Lupine Publishers – 2022 – Режим доступу: https://lupinepublishers.com/forensic-and-genetics-journal/.

10. Blockchain Protocols and Their Working [Електронний ресурс] – 2022 – Режим доступу: https://www.geeksforgeeks.org/blockchain-protocols-and-their-working/.

11. Detailed analysis of Ethereum network on transaction behavior, community structure and link prediction [Електронний ресурс] // PeerJ Computer Scienc – 2021 –

Режим доступу: https://www.geeksforgeeks.org/blockchain-protocols-and-their-working/.

12. Cryptocurrencies activity as a complex network: Analysis of transactions graphs [Електронний ресурс] // Peer-to-Peer Networking and Applications – 2021 – Режим доступу: https://link.springer.com/article/10.1007/s12083-021-01220-4.

13. 51% Attack: Definition, Who Is At Risk, Example, and Cost [Електронний ресурс] – 2023 – Режим доступу: https://www.investopedia.com/terms/1/51-attack.asp.

14. Blockchain Analytics: 14 On-Chain Metrics to Know [Електронний ресурс] – 2021 – Режим доступу: https://www.mlq.ai/blockchain-analytics-terms/.

15. Digital forensics of cryptocurrency wallets [Електронний ресурс] – 2022 – Режим доступу: https://www.diva-portal.org/smash/get/diva2:1671204/FULLTEXT02.

16. Blockchain Forensics and Crypto-Related Cybercrimes [Електронний ресурс] // SSRN – 2023 – Режим доступу: https://papers.ssrn.com/sol3/.

17. Blockchain Technology a new domain for Cyber Forensics [Електронний ресурс] // HALMSTAD UNIVERSITY – 2018 – С. 13-21 – Режим доступу: https://www.diva-portal.org/smash/get/diva2:1259867/FULLTEXT01.pdf.

18. On-Chain Analytics: Metrics for Analyzing Blockchains [Електронний ресурс] – 2022 – Режим доступу: https://www.relataly.com/seven-metrics-for-on-chain-analysis-in-python/10098/.

19. Difference between Public and Private blockchain [Електронний ресурс] – 2022 – Режим доступу: https://www.geeksforgeeks.org/difference-between-public-and-private-blockchain/.

20. A blockchain-based forensic model for financial crime investigation: the embezzlement scenario [Електронний ресурс] – 2021 – Режим доступу: https://link.springer.com/article/10.1007/s42521-021-00035-5.

Додаток А Лістинг програми

main.py

```
from web3 import Web3
import time
from termcolor import colored
import numpy as np
import pandas as pd

green_plus = colored("[+] ", "green")
red_x = colored("[x] ", "red")
blue = colored("[>] ", "blue")

known_malicious_addresses = [
    "0x3E0DeFb880cd8e163baD68ABe66437f99A7A8A74",
    "0x3E0DeFb880cd8e163baD68ABe66437f99A7A8A74",
    "0x0E2fC0B302bde3110858CD882cFc9690E67e2D13",
    "0x2f77f4523a13138b472Ac6fAeF624ccE68DA2c46",
    "0x7613a475b7fE61775f579Bc148300C8171EcCaE9",
    "0x39cf57b4dECb8aE3deC0dFcA1E2eA2C320416288",
    "0xE5E6FB7fEA83FeD8C2e7917599317568D945d34E",
    "0x65Bb455e9a94622E0856Ac55cB8597D108c6FA71",
    "0xeEff1a3c98d97536B641b794D69Ddc3704786d57" ]

def get_transaction(w3, block_number):
    block = w3.eth.get_block(block_number, full_transactions=True)
    transactions = block["transactions"]
    with open("transactions.txt", "w") as f:
        for tx in transactions:
```

```
            f.write(f"Transaction hash: {tx['hash'].hex()}\n")
            f.write(f"From address: {tx['from']}\n")
            f.write(f"To address: {tx['to']}\n")
            f.write(f"Value: {w3.from_wei(tx['value'], 'ether')} ether\n")
            f.write(f"Gas price: {w3.from_wei(tx['gasPrice'], 'gwei')} gwei\n")
            f.write(f"Nonce: {tx['nonce']}\n")
            f.write("----------------------------------------------------\n")
    return transactions

def count_transactions_in_block(transactions):
    return len(transactions)

def address_balance(transactions):
    address_balance_from = np.empty(shape=[0,2])
    address_balance_to = np.empty(shape=[0,2])
    start_time = time.time()
    print(green_plus + f"Getting address balance started")
    with open("address_balance.txt", "w") as f:
        for tx in transactions:
            address_from = tx["from"]
            balance_from = w3.eth.get_balance(address_from)
            balance = w3.from_wei(balance_from, "ether")
            f.write(f"[FROM] Address: {address_from}, Balance: {balance} ETH\n")
            address_balance_from = np.append(address_balance_from, [[address_from,
balance]], axis=0)
        for tx in transactions:
            address_to = tx["to"]
            balance_to = w3.eth.get_balance(address_to)
            balance = w3.from_wei(balance_to, "ether")
            f.write(f"[TO] Address: {address_to}, Balance: {balance} ETH\n")
```

```
        address_balance_to = np.append(address_balance_to, [[address_to, balance]], axis=0)
    print(green_plus + f"Getting address ended in {round(time.time() - start_time)} seconds")
    return address_balance_from, address_balance_to

def suspicious_transactions(transactions):
    start_time = time.time()
    print(green_plus + f"Finding suspicious transactions started")
    for tx in transactions:
        if tx["from"] in known_malicious_addresses or tx["to"] in known_malicious_addresses:
            print(red_x + f"\tSuspicious_transaction: {tx}")
    print(green_plus + f"Finding suspicious transactions ended in {time.time() - start_time} seconds")

def find_bots(transactions):
    start_time = time.time()
    print(green_plus + f"Finding bots activity started")
    toFromPairs = {}
    transactionCount = {}
    for tx in transactions:
        if tx["to"] != None:
            if tx.to in toFromPairs:
                if toFromPairs[tx["to"]] == tx["from"]:
                    transactionCount[tx["to"]] = transactionCount[tx["to"]] + 1
            elif tx["to"] not in toFromPairs:
                transactionCount[tx.to] = 1
                toFromPairs[tx["to"]] = tx["from"]
    for key, value in transactionCount.items():
```

```
        if value == 2:
            print("\t" + red_x + f"Bot: {toFromPairs[key]}")
    print(green_plus + f"Finding bots activity ended in {time.time() - start_time} seconds")

def monitor_large_transactions(transactions):
    start_time = time.time()
    print(green_plus + f"Finding large transactions started")
    large_amount = 20
    for tx in transactions:
        value_ether = w3.from_wei(tx["value"], "ether")
        if value_ether > large_amount:
            print("\t" + red_x + f"Large transaction found:")
            print(f"\t\tFrom: {tx['from']}")
            print(f"\t\tTo: {tx['to']}")
            print(f"\t\tValue: {value_ether} ether")
    print(green_plus + f"Finding large transactions ended in {time.time() - start_time} seconds")

def high_frequency(w3, start_block, end_block):
    start_time = time.time()
    print(green_plus + f"Finding high frequency transactions started")
    transactions = []
    for i in range(start_block, end_block):
        block = w3.eth.get_block(i)
        for transaction in block.transactions:
            tx = w3.eth.get_transaction(transaction)
            transactions.append({'from': tx['from'], 'to': tx['to']})
    df = pd.DataFrame(transactions)
    print(df['from'].value_counts())
    print(df['to'].value_counts())
```

```
    print(green_plus + f"Finding high frequency transactions ended in {time.time() - start_time} seconds")

def great_balance(address_balance_from, address_balance_to):
    print(green_plus + f"Addresses with a large balance:")
    for i in range(1, len(address_balance_from)):
        if int(address_balance_from[i-1][1]) > 20000 and address_balance_from[i-1][0] != address_balance_from[i][0]:
            print("\t" + blue + f"Address: {address_balance_from[i-1][0]} Balance: {address_balance_from[i-1][1]}")
    for i in range(1, len(address_balance_to)):
        if int(address_balance_to[i-1][1]) > 20000 and address_balance_to[i-1][0] != address_balance_to[i][0]:
            print("\t" + blue + f"Address: {address_balance_to[i-1][0]} Balance: {address_balance_to[i-1][1]}")

if __name__ == "__main__":
    w3 = Web3(Web3.HTTPProvider("https://mainnet.infura.io/v3/82f635ea8f9241e3a15feeb1e71e8efe"))

    if w3.is_connected():
        current_block = w3.eth.block_number
        transactions = get_transaction(w3, current_block)
        transactions_in_block = count_transactions_in_block(transactions)
        print(green_plus + f"Connected to Ethereum")
        print(green_plus + f"Current block number: {current_block}")
        print(green_plus + f"Transaction in block: {transactions_in_block}")
        address_balance_from, address_balance_to = address_balance(transactions)
        great_balance(address_balance_from, address_balance_to)
```

```
    suspicious_transactions(transactions)
    find_bots(transactions)
    monitor_large_transactions(transactions)
    high_frequency(w3, current_block-10, current_block)
else:
    print(red_x + f"Not connected")
```