МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри комп'ютеризованих систем захисту інформації
_____ Михайло СТЕПАНОВ
«_____»_____ 2023 р.

На правах рукопису
УДК 004.087.5:004.056.5

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: «Програмний модуль моніторингу підозрілих на шахрайство транзакцій на базі технології блокчейн»

Виконавець: Михайло СУДНІЦИН
Керівник: к.т.н., доцент Іван ПАРХОМЕНКО
Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент Тетяна ДМИТРУХА
Нормоконтролер: к.т.н., доцент Іван ПАРХОМЕНКО

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютеризованих систем захисту інформації
_____ Михайло СТЕПАНОВ
«_____»_____ 2023 р.

ЗАВДАННЯ

на виконання кваліфікаційна роботи

здобувача вищої освіти Судніцина Михайла Олександровича

1. Тема: *Програмний модуль моніторингу підозрілих на шахрайство транзакцій на базі технології блокчейн*
затверджена наказом ректора від «15» вересня 2023 р. № 1814/ст

2. Термін виконання: з 16.10.2023 р. по 31.12.2023 р.

3. Вихідні дані: проаналізувати принципи роботи блокчейн операцій, види шахрайства, які існують в роботі з блокчейнами, на основі проведеного аналізу розробити програмний модуль моніторингу підозрілих на шахрайство транзакцій в блокчейні.

4. Зміст пояснювальної записки: Аналіз існуючих засобів ідентифікації шахрайських операцій в блокчейні. Розробка програмного модулю моніторингу підозрілих на шахрайство транзакцій в блокчейні та його експериментальне дослідження

5. КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ з/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	16.10.2023	*Виконано*
2.	Аналіз літературних джерел	20.10.2023 - 01.11.2023	*Виконано*
3.	Обґрунтування вибору рішення	02.11.2023 - 04.11.2023	*Виконано*
4.	Збір інформації	05.11.2023 - 10.11.2023	*Виконано*
5.	Огляд розвитку та викликів криптовалюти, як привабливої сфери для шахраїв сьогодення	11.11.2023 - 16.11.2023	*Виконано*
6.	Аналіз механізмів криптовалютних операцій	17.11.2023 - 25.11.2023	*Виконано*
7.	Розробка програмного модуля та його експериментальне дослідження	26.11.2023 - 10.11.2023	*Виконано*
8.	Апробація роботи на X міжнародній конференції “Інформаційні технології та впровадження (сателітна)”,	21.11.2023	*Виконано*
9.	Перевірка на антиплагіат	11.12.2023	*Виконано*
10.	Оформлення і друк пояснювальної записки	15.12.2023	*Виконано*
11.	Оформлення презентації	15.12.2023	*Виконано*
12.	Отримання рецензій від рецензента	22.12.2023	*Виконано*

6. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти Михайло СУДНІЦИН

(підпис, дата)

Керівник кваліфікаційної роботи Іван ПАРХОМЕНКО

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів та висновків до них, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 94 сторінок, 7 сторінок додатків, має 38 рисунків. Список використаних джерел містить 58 найменування і займає 7 сторінок.

Мета роботи – заключається в розробці програмного модуля, який надає можливість відслідковувати підозрілі на шахрайство криптовалютні операції.

Предметом дослідження є безпека криптовалютних операції та технологія блокчейн в цілому.

У вступі обґрунтовується актуальність теми роботи, визначаються мета дослідження та завдання, які необхідно вирішити для досягнення поставленої мети, можливі результати дослідження.

У першому розділі було розглянуто перспективи криптовалют, як альтернативи фіатній валюті, правове регулювання криптовалют в Україні. Крім цього приділена увага видам кіберзлочинів, пов'язаних з блокчейнами.

У другому розділі проводиться аналіз роботи криптовалютних операцій та проблематика у їх відслідковуванні. Крім цього наведено аналіз наявних застосунків, котрі надають змогу ідентифікувати підозрілі на шахрайство операції, та визначення ключових критеріїв для виявлення шахрайства для використання в програмному модулі.

У третьому розділі ми розглянули програмну розробку моделі виявлення та моніторингу підозрілих на шахрайство операцій в блокчейні та провели його експериментальне дослідження.

У четвертому розділі було розглянуто термін екологічна культура та необхідність побудови світогляду людей у напряму догляду за навколишнім середовищем.

ТЕХНОЛОГІЯ БЛОКЧЕЙН, ОПЕРАЦІЇ З КРИПТОВАЛЮТАМИ, ПРАВОВЕ РЕГУЛЮВАННЯ КРИПТО АКТИВІВ, ШАХРАЙСТВО, БЕЗПЕКА В ОПЕРАЦІЯХ З КРИПТОВАЛЮТОЮ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕК – електронні кошти;

НБУ – Національний банк України;

ПЗ – програмне забезпечення;

ETH – криптовалюта Ефіріум;

BTC – криптовалюта Біткоїн;

NFT – невзаємозамінний токен;

P2P – мережа рівного до рівного;

API – прикладний програмний інтерфейс;

AWS – сервіс надання хмарних послуг Amazon;

БД – база даних;

UI – інтерфейс користувача;

TPS – кількість транзакцій в секунду;

ТестНет – тестова мережа;

ВСТУП

На сьогоднішній день, в усьому світі відзначається величезний інтерес до криптовалюти та технології блокчейну, що лежить в основі її створення. Проте, ставлення до віртуальних грошей офіційних інституцій влади все ж залишається доволі скептичним та настороженим. В останні місяці на державному рівні в Україні активізувалися дискусії щодо перспектив легалізації криптовалютного ринку та можливості використання його інструментів у діяльності економічних операторів. 14 вересня Верховна Рада України ухвалила законопроєкт №7410-1, який вносить зміни до Податкового кодексу України щодо оподаткування операцій з віртуальними активами. Законопроєкт передбачає, що з 1 січня 2024 року фізичні особи будуть сплачувати податок на прибуток у розмірі 18% від інвестиційного прибутку, отриманого від операцій з віртуальними активами.

Блокчейн представляє собою величезну глобальну базу даних, яка не належить жодній особі та розподілена настільки широко, що змінити її надзвичайно складно, навіть для тих, хто займається зберіганням даних. Відома своїм зв'язком з криптовалютами, блокчейн тепер привертає увагу фахівців, які досліджують його потенційне застосування в різних секторах економіки, не обмежуючись лише фінансами.

Експерти в області блокчейну бачать в ній потенціал для заміни банків як посередників у фінансових транзакціях. Однак, саме банки демонструють найбільшу зацікавленість у використанні технології блокчейну.

Хоча криптовалютні активи та блокчейн пропонують компаніям, організаціям і деяким державам переваги, які можуть спростити доступ до фінансових продуктів, збільшити фінансові можливості та знизити ризики корупції та шахрайства, існує значний ризик, що злочинці можуть використовувати технологічні переваги цифрових валют на свою користь.

Незважаючи на падіння ринку у 2022 році, обсяг незаконних транзакцій зростав другий рік поспіль, досягнувши історичного максимуму в $20.1 млрд, та

судячи з аналізу, цього року зазнає значного зростання. Не кажучи вже про те, що Україна посідає перше місце серед країн за рівнем криптовалютної активності. Вважається, що понад 6,5 мільйонів українців володіють криптовалютою, що становить приблизно 15,72% від загальної кількості населення, яке отримує цей цифровий актив.

Навіть якщо брати до уваги, що інформація про кожну транзакцію фіксується в блокчейні, ці дані не прямо пов'язані з іменами, адресами або іншими відомостями, які дозволяють ідентифікувати особу. Це надає цифровим валютам певний рівень анонімності та утруднює зусилля правоохоронних органів щодо виявлення та встановлення зв'язку між індивідуальними транзакціями та їх користувачами [1].

Злочинці та корупціонери з легкістю можуть переміщувати свої цифрові активи через багато рахунків, щоб уникнути відповідальності за їхнє походження, а потім приховують це походження, використовуючи численні транзакції, які створюють складну мережу, яку важко швидко проаналізувати людським оком. Згідно з декларацією державних службовців за 2020 рік, 652 українські чиновники володіють приблизно 46 351 біткоїном, що на сьогодні становить 1.6 мільярда доларів США. Можна зробити висновок, що з 46 351 BTC 40 849 BTC, або 88,1 %, належать лише десятьом державним службовцям.

Криптовалютні операції відбуваються надзвичайно швидко, що дає можливість злочинцям миттєво переміщувати активи між гаманцями. Ця швидкість робить складними спроби відслідковування фінансових потоків через ручний аналіз та контроль транзакцій. Тому, створення ефективного методу слідкування за блокчейн-платежами є важливою задачею в сучасному світі.

Вказані вище обставини визначили практичну значущість та актуальність обраної теми кваліфікаційної роботи.

Метою кваліфікаційної роботи є розробка програмного модуля, який надає можливість відслідковувати криптовалютні операції, що мають на меті шахрайські дії на базі технології блокчейн.

Завдання роботи:

- Провести класифікацію та аналіз шахрайських схем у криптовалютному світі сьогодення;
- Розглянути проблематику відслідковування блокчейн транзакцій та здійснити аналіз існуючих моделей та методів ідентифікацій та відслідковування підозрілих на шахрайство транзакцій у блокчейні;
- Розробка критеріїв та метрик для виявлення шахрайських транзакцій, для використання в програмному модулі;
- Розробити та здійснити тестування програмного модуля для відслідковування підозрілих на шахрайство транзакцій в блокчейні.

Галузь застосування: розроблена модель відносяться до галузі інформаційної безпеки і можуть бути використані для аналізу та ідентифікації потенційно шахрайських операцій з криптовалютними активами.

Об'єктом дослідження є процес роботи блокчейну та криптовалютних операцій, міжнародна та українська практики правового регулювання криптовалютних активів та криптовалютних операцій та види шахрайства в блокчейнах.

Предметом дослідження: є безпека криптовалютних операції та технологія блокчейн в цілому.

Методи дослідження: базуються, на основі побудови моніторингової системи для відслідковування підозрілих на шахрайство транзакцій в блокчейні та об’єктно-орієнтованого програмування.

Новизна одержаних результатів: полягає у створенні програмного модуля, що впроваджує новітні методи моніторингу та ідентифікації підозрілих на шахрайство операцій з криптовалютними активами, забезпечуючи при цьому високу точність та ефективність у протидії фінансовим злочинам у цифровій сфері.

Практичну базу роботи: становить програмний модуль моніторингу та ідентифікації шахрайських операцій в блокчейні.

Практичне значення одержаних результатів дослідження: полягає в тому, що результатом роботи є програмний модуль, в якого на даний момент не

існує аналогів. Він дозволяє користувачам відслідкувати шляхи відмивання коштів від введеного гаманця до кінцевих акаунтів на які їх було перенаправлено, та ідентифікувати гаманці в ланцюзі операцій, що раніше були задіяні в протизаконних діях. Завдяки визначені основних критеріїв та пріоритетності у визначенні потенційно шахрайських дій, даний програмний модуль надає можливість комплексного аналізу блокчейн транзакцій.

Апробація: Основні положення роботи доповідалися та обговорювалися на X міжнародній сателітній науково практичній конференції Conference, 21 листопада 2023 р. та опубліковано статтю та тези доповіді: Sudnitsyn Mykhailo, Diadiuk Olena, “MONEY LAUNDERING AND FRAUD DETECTION: THE CHALLENGES OF BLOCKCHAIN TRANSACTION ANALYSIS", X International Conference Information Technology and Implementation (Satellite), Nov. 2023.

РОЗДІЛ 1. ОГЛЯД РОЗВИТКУ ТА ВИКЛИКІВ КРИПТОВАЛЮТИ, ЯК ПРИВАБЛИВОЇ СФЕРИ ДЛЯ ШАХРАЇВ СЬОГОДЕННЯ

1.1 Можливості криптовалютних активів, як потенційна заміна фіатної валюти

Криптовалюти стали одним із найпопулярніших фінансових інструментів у світі. Вони пропонують ряд переваг перед традиційними валютами, зокрема децентралізацію, безпеку та низькі комісії. Україна є одним із лідерів у розвитку криптовалютного ринку в Європі. За даними аналітичної компанії Chainalysis, у 2022 році Україна посіла 13-е місце у світі за обсягом інвестицій у криптовалюти [3].

Стан криптовалютного ринку в Україні за останній рік характеризується наступними тенденціями:

- Ріст популярності криптовалют. За оцінками Мінцифри, обіг криптовалют в Україні становить близько 1 млрд грн на добу;
- Зростання кількості криптовалютних бірж та майнерів. У 2022 році в Україні було зареєстровано понад 50 крипто-бірж та майнерських ферм;
- Запровадження регулювання криптовалют. 14 вересня Верховна Рада України ухвалила законопроєкт №7410-1, який вносить зміни до Податкового кодексу України щодо оподаткування операцій з віртуальними активами. Законопроєкт передбачає, що з 1 січня 2024 року фізичні особи будуть сплачувати податок на прибуток у розмірі 18% від інвестиційного прибутку, отриманого від операцій з віртуальними активами [2].

Буквально за останні декілька місяців законодавство України до криптовалют зазнало наступних змін:

- 21 вересня Національна комісія з цінних паперів та фондового ринку (НКЦПФР) затвердила положення про проведення ринків віртуальних активів. Положення визначає порядок реєстрації, діяльності та припинення діяльності суб'єктів ринку віртуальних активів, а також вимоги до їх діяльності [4];
- 28 вересня НКЦПФР видала перші ліцензії на діяльність з випуску та торгівлі віртуальними активами. Ліцензії отримали дві компанії: "Українська біржа криптовалют" та "Українська біржа з торгівлі віртуальними активами" [4];
- Було запроваджено єдиний реєстр віртуальних активів. Реєстр буде вестися Національною комісією з цінних паперів та фондового ринку та міститиме інформацію про емітентів, виробників та постачальників послуг віртуальних активів;
- Також, було запроваджено обов'язок для крипто-бірж та обробників криптовалют повідомляти про свої операції до НБУ. Цей обов'язок має на меті запобігти легалізації доходів, отриманих злочинним шляхом.

Дана актуальність зумовлена також і тим, що Україна посідає одне з перших місце серед країн за рівнем криптовалютної активності. Вважається, що понад 6,5 мільйонів українців володіють криптовалютою, що становить приблизно 15,72% від загальної кількості населення, яке отримує цей цифровий актив. Згідно з декларацією державних службовців за 2020 рік, 652 українські чиновники володіють приблизно 46 351 біткоїном, що на сьогодні становить 1,6 мільярда доларів США. Можна зробити висновок, що з 46 351 BTC 40 849 BTC, або ж 88,1% [11], належать лише десятьом державним службовцям (рис. 1.1).

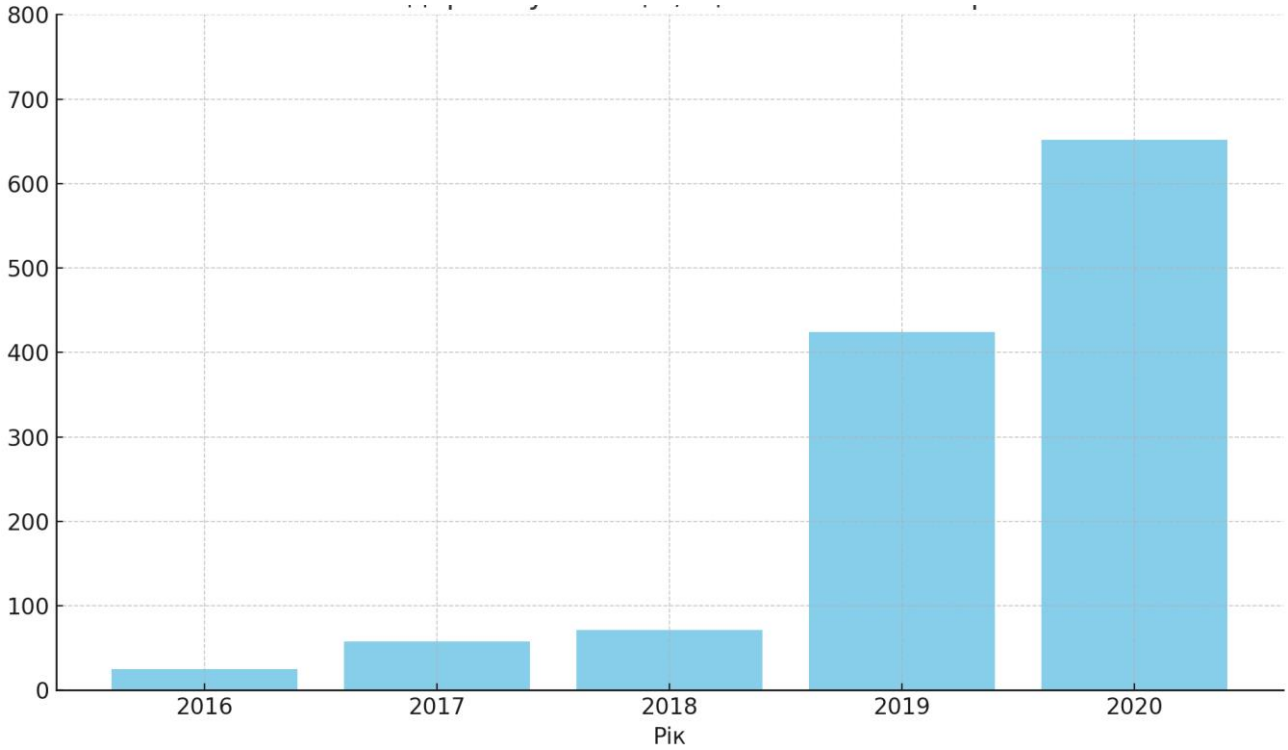

Рис. 1.1. Кількість держслужбовців, які задекларували криптовалюту

Ключовою особливістю криптовалют є відсутність внутрішнього і зовнішнього регулювальника. З цієї причини банки, податкові служби, суди та інші державні чи приватні органи не можуть втручатися в операції, які здійснюють окремі учасники платіжної системи. Все це забезпечує безперебійні операції – ніхто не може втручатися, блокувати, скасовувати транзакцію, не маючи доступу до приватного ключа власника [5].

Одна з головних відмінностей між електронними грошима та криптовалютами полягає в тому, що традиційні гроші спочатку мають бути зараховані на фізичний рахунок, щоб вони з’явилися на електронному рахунку, наприклад через банк або платіжний термінал. У випадку звичайної валюти електронна форма є лише однією з форм оплати, це просто форма грошей. Криптовалюта споживається безпосередньо в Інтернеті і не пов’язана з традиційною валютою чи державною грошовою системою [6]. Крім, окремих випадків коли ми говоримо про стабільні монети, такі як USD монета, котрі мають повну прив’язку до курсу валюти, у даному випадку долара і як правило котируються один до одного.

У загальному переваги та недоліки операцій у криптовалюті можна поділити на 2 етапи – це безпека та зручність і довіра та збереження вартості.

Переваги та недоліки у безпеці та зручності операцій:

- Переваги:
    - Менший ризик втрати коштів через злам або хакерську атаку блокчейну;
    - Неможливість внесення змін до ланцюжку блокчейнів;
    - Складність у викраденні коштів з приватного гаманця (оскільки доступ до нього є лише у власника ключа);
    - Для деяких блокчейнів, відносно невелика плата за комісію при проведенні криптовалютної операції;
    - Рахунок у криптовалюті неможливо заблокувати або відмовити в обслуговуванні з певних причин (до прикладу політичних). За винятком коли кошти зберігаються на криптовалютних біржах, які співпрацюють з тими чи іншими державними органами;
    - Відносна анонімність, якщо порівнювати з традиційними операціями;
    - Можливість переказу коштів в будь яку точку планети за лічені хвилини;
    - Усунення посередників між платником і одержувачем при здійсненні платежу.
- Недоліки:
    - Для деяких блокчейнів відносно високий розмір комісії за проведення операції;
    - Негативний вплив на навколишнє середовище, при видобутку криптовалюти, через те що прилади для майнінгу споживають велику кількість енергії;

- Не мають статусу законного платіжного засобу у деяких країнах світу, що ускладнює оплату даним способом;
- Лише невелика кількість білих бізнесів приймає криптовалюту, як спосіб оплати;
- Втрата усіх коштів у разі неможливості отримати доступ до рахунку;
- Незворотність операцій, у разі помилки (у відправленій сумі чи адресі отримувача) операцію відмінити неможливо;
- Відсутність регулювання державними інститутами, що зумовлює неможливість захисту вкладень інвесторів.

Переваги та недоліки у довірі та збережені вартості:

- Переваги:
  - Відносна стійкість до інфляції, оскільки існує обмежена емісія монет та можливість знищення відсотку за допомогою методу спалювання;
  - Менший ризик дефолту крипто компаній, через децентралізацію у її правлінні.
- Недоліки:
  - Можливість дефляції для деяких криптовалют;
  - Суперечлива репутація, оскільки нерідко криптовалютні активи використовуються у злочинних схемах по відмиванню коштів;
  - Ризик заборони регуляторами влади.

Отже можна прийти до висновку, всі власники криптовалютних активів стикаються з проблемою, що й користувачі традиційних форм фіатних валют – необхідністю забезпечення безпеки своїх збережень та операцій. Впровадження та розвиток криптовалюти призводить до появи додаткових зобов'язань, ризиків та витрат, які повинно вирішити законодавство та інституції влади [5].

Проте, незважаючи на велику кількість недоліків, ринок крипто активів продовжує рости та з кожним днем удосконалюватись, намагаючись усунути більшість з них. Недаремно кажуть, що криптовалюти є сучасним етапом еволюції платіжних засобів [6].

1.2 Механізм функціонування технології блокчейн

Блокчейн - це криптографічно захищений ланцюг блоків, заснований на анонімному консенсусі через розподілену P2P-мережу. Кожен блок в блокчейні складається із серії транзакцій. Кожна транзакція публікується у вигляді хеш-значення, а потім усі хеш-значення поєднуються в блок (рис. 1.2). Заголовок блоку містить агрегований хеш, тобто хеш поточного блоку та хеш попереднього блоку [7].

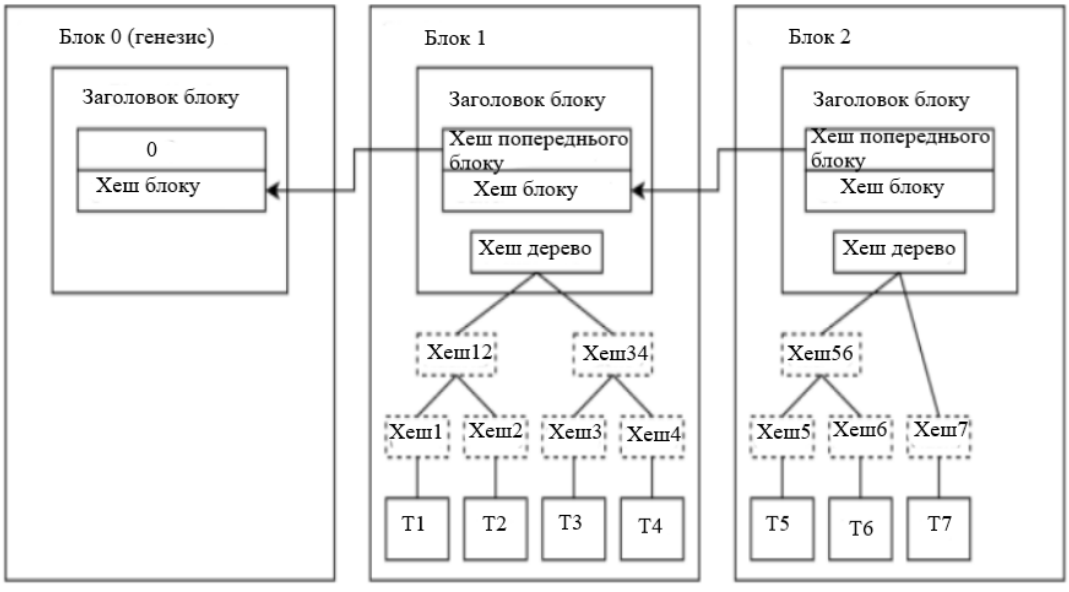

Рис. 1.2. Структура блоків (де Т – позначення транзакції)

Таким чином, всі блоки в блокчейні тісно пов'язані між собою, та для зміни будь-якої його частини потрібна зміна всіх його всіх складових, що є практично неможливим, за винятком згоди більшості майнерів блокчейну.

Це робиться для підтримки, так званого процесу консенсусу, тобто узгодження того, що блок і транзакції, з яких він складається, є дійсними.

Консенсус досягається, якщо більшість вузлів мережі, які працюють як видобувачі криптовалюти, голосують за визнання достовірності даного блоку транзакцій. Таким чином коли створюється транзакція, дана подія записується в базу даних блокчейну та передається по всій мережі для перевірки вузлами майнінгу. При отримані вузол, або як його ще називають нода, перевіряє її на справжність. Чим більше вузлів здійснило перевірку, тим більша вірогідність, що транзакція є достовірною.

Важливою особливістю масштабування Bitcoin є те, що блок зберігається в багаторівневій структурі даних. "Хеш" блоку - це насправді лише хеш заголовка блоку, приблизно 200-байтовий фрагмент даних, який містить мітку часу, хеш попереднього блоку і кореневий хеш структури даних, яка називається деревом Меркла, що зберігає всі транзакції в блоці [19]. Дерево Меркла - це тип бінарного дерева, що складається з набору вузлів з великою кількістю листкових вузлів внизу дерева, що містять основні дані, набору проміжних вузлів, де кожен вузол є хешем двох його дочірніх вузлів, і, нарешті, одного кореневого вузла, також сформованого з хешів двох його дочірніх вузлів, що представляє "вершину" дерева [42].

Мета дерева Меркла полягає в тому, щоб дозволити доставляти дані в блоці по частинах: вузол може завантажити тільки заголовок блоку з одного джерела, невелику частину дерева, що має відношення до нього, з іншого джерела, і при цьому бути впевненим, що всі дані коректні. Причина, по якій це працює, полягає в тому, що хеші поширюються вгору: якщо зловмисник спробує підмінити фальшиву транзакцію в нижній частині дерева Меркла, ця зміна викличе зміну у вузлі вище, а потім зміну у вузлі ще вище, в результаті чого змінюється корінь дерева і, відповідно, хеш блоку, що змусить протокол зареєструвати його як зовсім інший блок.

Концепція блокчейна була представлена людиною на прізвисько Сатоші Накамото [18]. Спочатку блокчейн був націлений на вирішення таких проблем,

як "подвійна витрата" і "візантійська стійкість до відмови", що лежать в основі криптовалюти Bitcoin. Проте згодом, розвиток блокчейну став основним напрямком для криптовалют чи підприємств. Для подальшого застосування, з'явилася блокчейн-платформа Ethereum, керована технологією смарт-контрактів. Яка перетворила стандарте бачення блокчейну та дала можливість створенню децентралізованих додатків (DApps) [42].

Будучи одноранговою розподіленою технологією (P2P), криптовалюти історично залежать від комп'ютерної мережі, зі спеціально встановленим ПЗ, яке виконує основні функції криптовалютної екосистеми.

Криптовалюта створює економічну систему, яка заохочує учасників інвестувати в ресурси та отримувати прибуток від своїх інвестицій (комісії за транзакції та криптовалюту). Комп'ютери, на яких встановлено це програмне забезпечення (ПЗ), є "майнерами", які створюють криптовалюту, підтверджуючи транзакції в блокчейні та підтримують цілісність публічної збірки рахунків [19].

Майнери отримують винагороду за свої інвестиції в роботу програмного забезпечення блокчейну, постійно вираховуючи хеш значення, створюючи саму криптовалюту. Проте варто зазначити, що у випадку з біткоїном та деякими іншими блокчейнами, присутній процес халвінгу, який запрограмовано зменшує кількість винагороди майнера за кожен видобутий блок в два рази кожні чотири роки.

Потрібно також зазначити, що з кожним видобутим блоком видобуток наступного ускладняється відповідно до арифметичної складової. Складність перераховується для кожного блоку з параметром висота блоку, рівним n, де □-1 - кратне 2016, t - час у хвилинах, витрачений на отримання останніх 2016 блоків. Дерево перевіряється на відповідність параметрів ”Хеш Блоку” та ”Хеш Попереднього Блоку” структурі дерева, де дочірній блок повинен слідувати одразу за батьківським [43]. Всі блоки в дереві T, всі адреси, транзакції, суми, підписи та відкриті ключі повинні бути узгоджені. А отже складність кожного блоку повинна задовольняти наступній формулі:

$$a = b \times \frac{20,160}{t}, \tag{1.1}$$

де a - складність видобутку нового блоку;

b - складність видобутку попереднього блоку

t - дерево блоків

Вони також можуть отримувати комісію за схвалення транзакцій в блокчейні. Наприклад, учасники криптовалюти Ripple запускають програмне забезпечення для валідації транзакцій (за що і отримують свої комісійні), на добровільній основі, в обмін на згоду надати обчислювальні ресурси для запуску майнингового ПЗ [24].

В загальному, майнери запускають ПЗ, яке виконує 3 основні функції: випуск нових монет (якщо це дозволено емісією), перевірка транзакцій на правильність та управління БД блокчейну (яка зберігається локально на комп'ютері майнера).

До прикладу (рис. 1.3), коли покупець намагається придбати якийсь товар чи оплатити послугу за допомогою криптовалюти (в даному прикладі, розглядається Bitcoin), спеціальне ПЗ з гаманця нашого клієнта передає дані про здійснену транзакцію до пулу вузлів майнінгу криптовалюти, які потім перевіряють дану транзакцію на правильність [22].

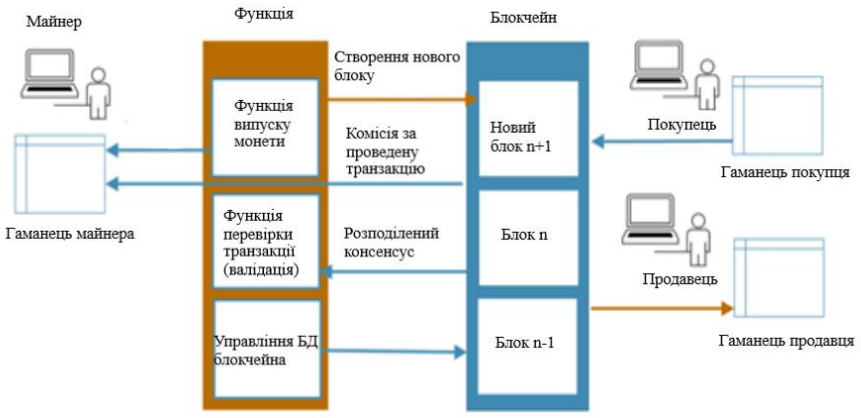

Рис. 1.3. Приклад простої криптовалютної операції

Транзакція в блокчейні між двома користувачами, може закінчитись в одному з трьох станів [24]:

- Підтвердження успішного завершення транзакції, яке не може відбутися поки, в середньому, 6 послідовних блоків транзакцій не будуть створені, таким чином підтверджуючи, що транзакція є дійсною. Блокчейн вимагає такої перевірки, за для того, щоб вузли майнера досягли консенсусу щодо всіх транзакцій в блоці;
- Незавершена транзакція. Дана ситуація може трапитись, якщо вузли майнерів, які отримали транзакцію найпершими її відхилили, через недійсність або перевантаженість перевіркою іншими транзакціями. Мережа вимагатиме, щоб близько 20-50 підтверджень, що повинно займати лише декілька хвилин, якщо брати до уваги швидкість створення нового блоку в мережі Ethereum, або до години, якщо розглядати Bitcoin блокчейн;
- Неперевірена транзакція. Вони поміщаються в спеціальному контейнері і будуть передані для встановлення в наступний блок після його створення.

Тепер, давайте розглянемо основний принцип роботи, блокчейн транзакції, який можна визначити як повідомлення між учасниками операції, що складається з трьох головних сегментів:

- Цифровий підпис ініціатора транзакції, зроблений його закритим ключем для того, щоб вузли майнери змогли переконатись, що дане повідомлення і справді надходить від ініціатора;
- Вхідні дані – список підписів транзакцій, які були внесені до публічної збірки рахунків, для того щоб переконатись у наявності необхідної суми перед її надсиланням. Також до вхідних даних відноситься сума яку ініціатор використав у теперішній транзакції;
- Вихідні дані – список того, як будуть розподілені кошти ініціатора, при виконанні транзакції.

Кожна криптовалютна транзакція має свій унікальний хеш ключ. Маючи це значення, її можна легко знайти та дослідити використовуючи блокчейн дослідник.

Якщо розглядати блокчейн Bitcoin, то у ньому уся сума яка знаходиться у гаманці ініціатора повинна бути занесена до вихідних даних і лише тоді коли необхідна сума буде відправлена одержувачу, різниця буде повернена у гаманець як залишок. Тобто транзакція повинна мати однакову кількість криптовалюти у вхідному і вихідному списках даних [24].

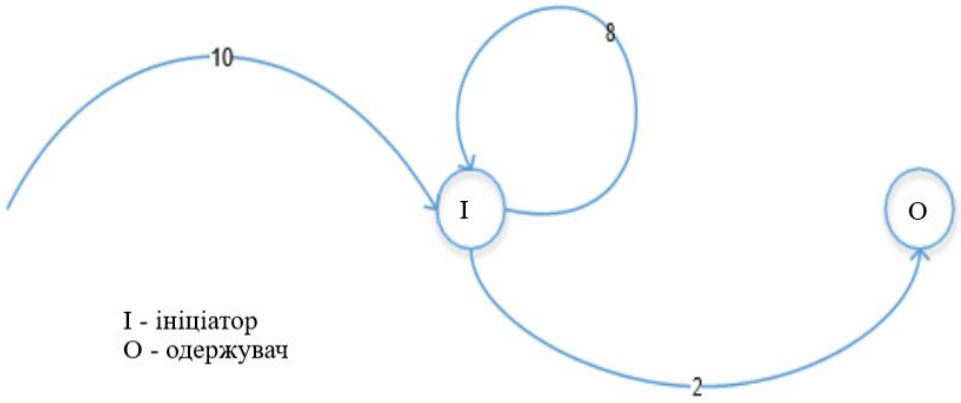

Рис. 1.4. Принцип роботи транзакцій у блокчейні Bitcoin

До прикладу, ініціатор маючи 10 BTC захоче відправити 2 із них отримувачу, дана транзакція призведе до того, що ініціатор отримає на свій гаманець 8 BTC, а одержувач 2 (рис. 1.4).

1.3 Правова сторона регулювання криптовалюти в Україні та огляд закордонної реалізації правового поля

Відмиванням коштів часто називають процесом приховування походження незаконно отриманих активів та їх інтеграції в основну фінансову систему, для того щоб надати їм вигляду законно отриманого доходу. Відмивання грошей вважається однією з найбільших загроз для стабільної економіки та громадської безпеки [37]. Процес відмивання коштів має три етапи:

- розміщення, що передбачає введення незаконно отриманих коштів у фінансову систему;
- нашарування, на даному етапі незаконні кошти, раніше внесені у фінансову систему, приховуються за допомогою складних транзакцій, щоб унеможливити їх відстеження під час аудиту;
- інтеграція, що передбачає собою введення коштів, які виглядають легітимними, в основний потік інвестицій.

Відтоді, як фінтех-індустрія запровадила нові платіжні технології, що дозволяють здійснювати складні грошові операції, відмивання грошей було визначено як "кібер-відмивання". Якщо в процесі відмивання грошей використовуються криптовалюти, це називається "крипто-відмиванням" або "віртуальним відмиванням грошей". Як наслідок, криптовалюти стали новим інструментом для злочинних угруповань для відмивання незаконно отриманих активів.

Після наведених аргументів можна прийти до висновку, що криптовалютні активи можна використовувати лише в неправових операціях або маючи на меті шахрайські дії, що прямо лінійно впливатиме на рівень корупції, збільшуючи її в державі, наголошуючи на анонімності користувачів криптовалют.

Також потрібно зазначити, що більшість із форм хабарів мають на увазі передачу фізичного предмету або ж фізичних купюр від особи до особи, які можна з легкість відслідкувати або знищити. Крім цього, вони потребують особистої зустрічі або використання послідовників для передачі активів, що ставить під ризик учасників операції.. Криптовалюта ж відбирає необхідність даних дій і також спрощує процес зберігання хабаря, у різній його формі. Хоча корумпований агент все одно повинен знайти відповідну особу, яка порушила свої обов'язки на користь корумпованого агента, цей пошук тепер також може відбуватися в Інтернеті [11]. Отже, криптовалюти та онлайн-середовище знижують транзакційні витрати корупції, полегшуючи контакт між сторонами корупційного контракту. Все це може призвести до розширення корупційних практик.

Однак потрібно також взяти до уваги, що всі блокчейни, крім приватних, за будовою надають інформацію про кожну транзакцію яка була проведена, а також дані про одержувача і відправника та суму з якою операція була проведена. Дану технологію можна буде імплементувати у сервіси для прозорого моніторингу коштів які надійшли на ті чи інші органи влади, для зменшення ймовірності їх нелегального використання.

У воєнний час вкрай важливо наповнювати бюджет України та вести діяльність для суб'єктів господарювання, щоб підтримати економіку держави. Світ вже давно обговорює криптовалюту, зокрема, щодо її офіційного використання як засобу платежу та офіційного використання в якості платіжного засобу.

Україна також рухається у цьому напрямку, та ще з листопада 2014 року НБУ, вперше зазначив про правовий режим біткоїна, як основної криптовалютної одиниці, та криптовалюти в цілому. Було зазначено, що використання криптовалюти пов'язане з підвищеними ризиками через анонімність та децентралізований характер операцій. А також зазначено, що ця сфера є привабливою для незаконної діяльності, в тому числі для відмивання грошей, отриманих злочинним шляхом, або для фінансування тероризму, адже весь світ бореться за прозорість транзакцій та ідентифікацію їх учасників, тому вкрай важливо, щоб усі перекази здійснювалися прозоро. Ще на момент 2019 року, згідно зі статистикою Україна входила у топ-5 країн за кількості користувачів різних криптовалютних гаманців, проте все ж не мала ніякого юридичного значення для криптовалютних активів [5].

У 2016 році, була ще одна спроба обговорення легалізації та встановлення правового режиму над крипто валютними активами, проте висунуті законопроєкти можна охарактеризувати лише, як спроби виключно оподаткування обігу криптовалют, а не її прийняття, як віртуального активу [6].

Позиція законодавців та податкових органів при формуванні проєктів нормативно-правової бази для оподаткування криптовалют базувалася на тому, що такі відносини пов'язані з обігом певних цінностей, а отже, з отриманням

певної вигоди під час або в результаті такого обігу. Еволюція визначення криптовалют у згаданих вище законопроєктах йшла по низхідній: від наділення їх властивостями фіатних грошей до повної відмови від цієї ідеї.

Проте, 17 лютого 2022 року Верховна Рада України все ж прийняла Закон України "Про віртуальні активи" № 2074-IX, який Президент України підписав 15 березня 2022 року. [12] Цей закон повністю легалізує обіг криптовалют в Україні на законодавчому рівні. Хоча потрібно зазначити, що визначення поняття "криптовалюта" в законодавстві України відсутнє. Цей термін подається як узагальнююче поняття, а також використовується термін "віртуальний актив".

Після набуття чинності цим законом з'явиться можливість отримувати податкові відрахування до бюджету від оподаткування операцій з віртуальними активами. Згідно з пунктом 1 розділу VI "Прикінцеві та перехідні положення" Закону №2074, сам закон набуде чинності:

- з набранням чинності Закону України "Про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами";
- запровадження Державного реєстру постачальників послуг, пов'язаних з обігом віртуальних активів, що додатково зазначено у пункті 2 розділу VI Прикінцевих та перехідних положень, як обмеження у можливості застосування санкцій, передбачених статтею 23 Закону 2074.

Таким чином, разом з набуттям чинності цього закону необхідно буде сплачувати податки з доходів, отриманих від операцій з криптовалютою. Чинний закон регулює правовідносини, що виникають з криптовалютою, і розглядає такі види віртуальних активів, як забезпечені і незабезпечені. Державними органами, які регулюватимуть діяльність з віртуальними активами, є: Національна комісія з цінних паперів та фондового ринку (незабезпечені активи) та Національний банк України (забезпечені активи) [12]. Буде створено Державний реєстр надавачів послуг, пов'язаних з обігом віртуальних активів, де можна буде знайти

інформацію про відповідних надавачів послуг, отримання дозволу буде обов'язковим для надання послуг.

Потрібно також зазначити, про законопроєкт "Про регулювання ринків крипто активів" (MiCA) був представлений 5 січня 2022 року в Європейському союзі та став основою для регулювання криптовалют в ЄС [28]. Крім того, 10 жовтня 2022 року члени Комітету з економічних та монетарних питань Європейського парламенту прийняли законопроєкт про регулювання криптовалют, підтримавши таким чином регулювання MiCA та всі відповідні положення. Ці два фактори стали причиною призупинення введення в дію відповідного Закону №2074, що регулює криптовалюти. Оскільки Україна отримала статус кандидата на вступ до Європейського Союзу 23 червня 2022 року, норми вітчизняного законодавства, в тому числі ті, що стосуються віртуальних активів, мають бути адаптовані до європейських стандартів, і регламент MiCA не є винятком.

Розглядаючи криптовалютне регулювання в країнах Європейського союзу, необхідно зазначити, що країни ЄС регулюють операції з криптовалютами по-різному. Станом на січень 2023 року, деякі з країн Європейського Союзу мають певний рівень регулювання криптовалют, але це не завжди означає повну легалізацію. Ось декілька прикладів країн ЄС, де криптовалюта регулюється або використовується в певній мірі [8]:

- У Німеччині криптовалюта визнана, як "частка капіталу", що дозволяє використання криптовалют, але з певними податковими та регуляторними обмеженнями;
- Естонія, відома своїм прогресивним підходом до криптовалют та блокчейну, з суворими правилами щодо боротьби з відмиванням грошей;
- У Мальті, яку часто називають "острів блокчейну", діють одні з найпрогресивніших законів щодо криптовалют в ЄС;
- Франція, має певні регуляції для криптовалют, включаючи податкові положення;

- Республіка Кіпр, володіє відносно ліберальним підходом до криптовалют, проте все ж деякі регуляторні рамки присутні, в забезпеченні операцій з криптовалютними активами;
- Словенія, є відносно дружня країна до криптовалютного світу, оскільки має декілька законів для підтримки використання активу;
- Нідерланди, має регуляцію крипторинку, та особливу увагу приділяє питанню боротьби з відмиванням грошей та фінансуванням тероризму, наркотрафіку в країні.

Ці країни мають різні рівні регулювання, і це не означає, що вони повністю "легалізували" криптовалюту в контексті традиційних валют (рис. 1.5).

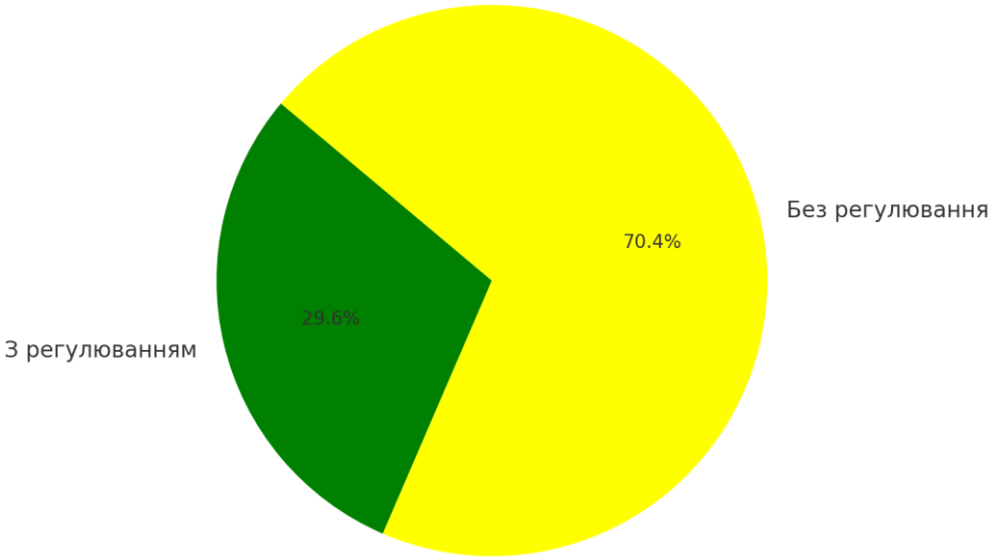

Рис. 1.5. Регулювання криптовалютних активів у країнах ЄС

В деяких країнах Європейського Союзу, для того щоб користуватись криптовалютними активами та здійснювати операції з ними, у разі необхідності, потрібно надати інформацію про підтвердження права на використання криптовалюти, а також документи, що вказують на джерело походження і право використовувати, володіти і розпоряджатися відповідною валютою. Таким чином, у багатьох державах ЄС зникає суттєва ознака криптовалютних транзакцій - анонімність, яка має вирішальне значення для багатьох учасників таких транзакцій. Тому перевагою криптовалюти над традиційними валютами

залишається лише швидке зростання її вартості в таких країнах, у зв’язку з відсутністю повного світового регулювання, з’являється й висока волатильність, що слугує цьому причиною.

Потрібно також зазначити, що все ж існує складність в оподаткуванні криптовалюти, у разі використання крипто гаманців, а не офіційних бірж бенефіціарів, у зв’язку з відсутністю даних про власників гаманців. Особи, які володіють, користуються та розпоряджаються криптовалютою, можуть бути об'єктом оподаткування такими податками: на доходи та на приріст капіталу.

Незабаром криптовалюта стане необхідною для здійснення платежів та інших операцій у більшості країн світу. Криптовалютні активи та електронні гроші в цілому, ймовірно, витісняють готівку з обігу і стануть якщо не єдиною, то провідною платіжною системою у світі. Досвід правового забезпечення криптовалют у країнах-членах ЄС різниться за рівнем лібералізму та податковими ставками [6]. Однак загальна тенденція на прикладі Мальти, Франції, Чехії та Естонії свідчить про застосування пільгового оподаткування порівняно з оподаткуванням доходів від діяльності в інших сферах і галузях економіки та оподаткуванням домогосподарств. У деяких європейських країнах інформація про власників криптовалютних одиниць вноситься до комп'ютерних реєстрів, що усуває анонімність як одну з найважливіших характеристик криптовалютних транзакцій.

1.4 Характеристика видів шахрайства які зустрічаються в криптовалютному світі та методи оцінки ризиків операцій

Криптовалютний світ, хоча і надає безліч переваг для користувачів, такі як унікальні можливості для інвестування, швидкість оброблення транзакцій, також привертає увагу шахраїв, які використовують недосвідченість користувачів та відсутність централізованого регулювання у своїх цілях.

Шахрайство в криптовалютному просторі може приймати різноманітні форми, від прямих крадіжок до складних махінацій. Розуміння цих видів шахрайства та методів їх виявлення є критично важливим для забезпечення безпеки активів та довіри до криптовалютного ринку.

Фішинг є одним з найбільш поширених способів шахрайства, що використовується для крадіжки конфіденційної інформації, такої як логіни, паролі до криптовалютних бірж або ж особисті ключі у випадку з використанням гаманців. У криптовалютному контексті фішинг часто включає розсилку фальшивих електронних листів або створення веб-сайтів, які імітують законні біржі, гаманці або сервіси.

Шахраї можуть пропонувати фальшиві рекламні акції або "ексклюзивні інвестиційні можливості", спонукаючи жертву ввести свої приватні дані на фішингових сторінках. Як тільки користувач вводить свої дані, шахраї отримують доступ до його криптовалютних коштів.

Іноді введення даних не є необхідністю, часто зустрічаються випадки коли шахраї створюють сайт, який виглядає схожим на популярний криптовалютний обмінник або ж NFT колекцію та залучають користувачів через спам-повідомлення з посиланнями на офіційних мережах, тим самим привертаючи увагу потенційних жертв і переконуючи їх відвідати фішинговий сайт.

Оскільки в криптовалютному світі адреса гаманця слугує певною ідентифікацію користувача, не є необхідністю проходити реєстрацію на кожному із сайтів, достатньо лише скористатись авторизацією через застосунок крипто-гаманця. Шахраї цим користуються та просять увійти в свій крипто гаманець здійснивши підпис в смарт контракті. У разі успішного підпису жертвою, смарт-контракт, який був ініціалізований даним підписом (часто без її розуміння про реальні умови), автоматично переводить кошти на контрольований шахраями гаманці.

Фішингові атаки можуть бути особливо складними для виявлення, оскільки вони постійно еволюціонують і стають більш хитромудрими. Вони часто включають соціальну інженерію та психологічні маніпуляції для

обдурення жертв, змушуючи їх вірити, що вони взаємодіють з законним сервісом.

Первинна пропозиція монет (ICO) - ще один метод, який використовується як і на етапі розшарування для обміну відмитої криптовалюти на новостворені монети так і як вид махінації для обману користувачів. ICO (Initial Coin Offerings), є одним із найбільш небезпечних видів шахрайства у криптовалютному світі. Ці проекти імітують законні пропозиції, надаючи інвесторам можливість придбати токени нової криптовалюти. Вони часто супроводжуються блискучими маркетинговими кампаніями, обіцянками високих доходів та розробкою переконливих, але фальшивих бізнес-планів.

Шахраї, які стоять за скам-проектами, зазвичай використовують такі методи:

- Створення професійних веб-сайтів, які мають вигляд легітимних (законних) проектів з детальною інформацією про продукт, команду, дорожню карту та інше;
- Часто також здійснюється створення псевдо команди та радників, логотипи та обличчя яких беруться без відома офіційних представників;
- Скам-проекти часто активні у соціальних мережах, де вони створюють штучний інтерес до своїх ICO. Такі проєкти, використовуючи техніки соціальної інженерії намагаються підсилити почуття втраченої вигоди або можливих великих заробітків залучаються людей до свого проєкту;

Інвестори, які все ж поведуться на дані махінації вкладають свої кошти в скам-проекти, навіть не розуміючи того, що ризикують їх повною втратою, оскільки після збору певної суми шахраї зникають.

Для відмивання цих коштів в фіатну валюту, або відбілювання криптовалютних активів злочинці використовують сервіси "змішування" і "тумблери", у такому випадку відстежити нелегальне походження монет стає в рази складніше. Сервіси "змішування" додають додатковий рівень невідомості

до криптовалютних транзакцій, крім існуючої псевдо анонімності, яка стоїть за адресою крипто гаманця. Після вирахування комісії за транзакцію вони об'єднують криптоактиви від кількох користувачів і доставляють змішані монети на випадкові адреси гаманців одержувачів. Різниця між цими двома сервісами полягає в тому, що "тумблери" переказують на гаманець клієнта ту саму криптовалюту, а "міксери" доставляють окрему криптовалюту, що ускладнює аналіз блокчейну. Щоб ускладнити кореляційний аналіз для слідчих, деякі сервіси "міксерів" і "тумблерів" використовують випадковий час затримки і випадкову суму надіслану в транзакції. Також, для того щоб зробити криптовалюту ще більш замаскованою, вони можуть конвертуватись в так звані, приватні монети, які мають додаткові шари надання конфіденційності власнику.

Відмивання грошей за допомогою криптовалют має схожі етапи з відмиванням фіатних валют. На етапі розміщення криптовалюта купується на нерегульованих криптовалютних біржах, у банкоматах або на офлайн обмінниках, де криптовалютою обмінюються однодумці. Злочинні угруповання також наймають, так званих, грошових мулів, які купують криптовалюту від їхнього імені, цим заплутуючи правоохоронні органи (рис. 1.6).

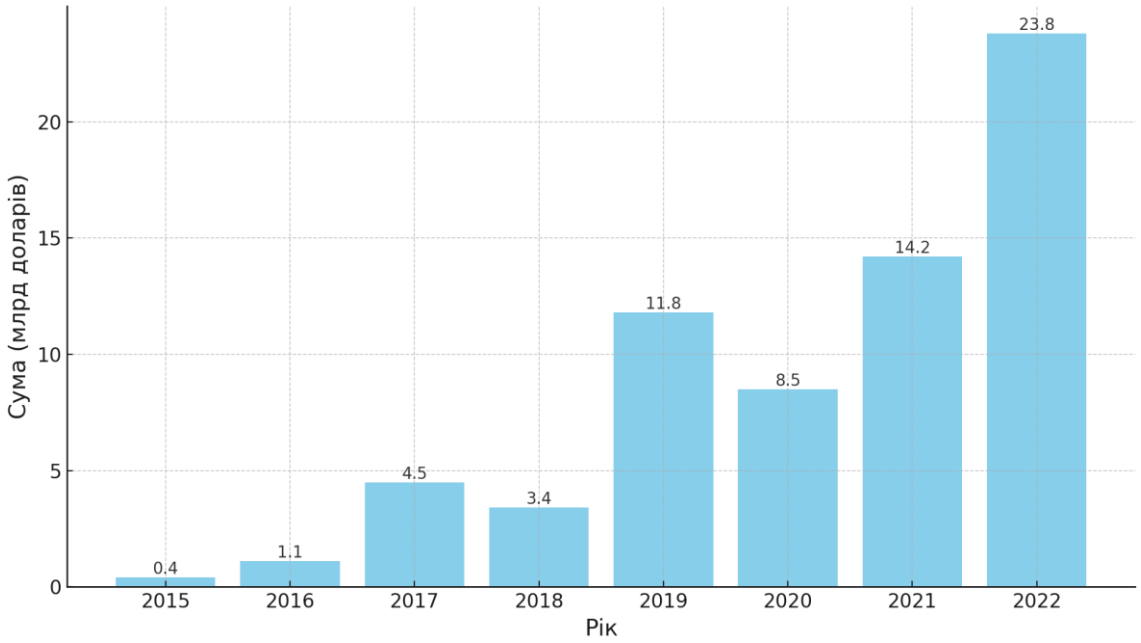

Рис. 1.6. Сума відмитих коштів в криптовалюті за роками

Ще однією стратегією є використання невзаємозамінних токенів (NFT) на етапі розшарування, що викликає занепокоєння щодо їхнього потенціалу у відмиванні криптовалют. Ці токени є предметами колекціонування, які представляють собою витвір цифрового мистецтва в блокчейні. Зловмисники купують самостійно створені NFT, використовуючи анонімний обліковий запис, а потім заявляють, що продали свій витвір мистецтва тому, хто запропонував вищу ціну. Через свою нестабільну вартість NFT є ідеальним інструментом для відмивання незаконних доходів. На етапі інтеграції грошові мули переводять очищені монети в готівку на регульованій криптовалютній біржі, яка пропонує обмін криптовалюти на фіатні валюти.

Якщо говорити про методи оцінки ризиків операцій, то можна виділити головні, а саме оцінка історії криптовалютної адреси та аналіз операції які мають бути проведені.

Оцінка репутації та історії валютних адрес є ключовим елементом у забезпеченні безпеки в криптовалютному світі. Цей процес включає аналіз історії транзакцій і взаємодій, пов'язаних з конкретною криптовалютною адресою, щоб визначити її надійність та законність.

Також потрібно зазначити і про аналіз патернів транзакцій, що є критично важливим інструментом у виявленні шахрайства у криптовалютному просторі. Цей метод базується на вивченні поведінкових шаблонів транзакцій та ідентифікації аномалій, які можуть вказувати на шахрайські діяльності. Використання евристичних методів, які ґрунтуються на використанні досвіду та інтуїтивних правил для виявлення підозрілих патернів у транзакціях. Ці методи можуть включати певні тригери, які спрацьовують при виявленні потенційно шахрайських активностей. Даними тригерами, можуть виступати:

- Незвичайні часові мітки, або ж транзакції, які відбуваються у нетипові для користувача часи, можуть вказувати на автоматизовані шахрайські схеми або спроби крадіжки коштів з криптовалютного гаманця жертви;

- Якщо говорити про криптовалютні біржі, де є інформація про користувача, а саме його географічні дані. Можна здійснити побудову тригера відповідно до операцій, що відбуваються з місць, які раніше не були пов'язані з користувачем;
- Використовуючи базу даних про криптовалютні шахрайські операції, можна здійснити визначення схожого патерну з серії транзакцій, котрі відбуваються за схожим сценарієм, що можуть свідчити про автоматизоване шахрайство.

1.5 Висновки до першого розділу

У першому розділі, було проведено огляд сучасного стану криптовалют та їхнього впливу на фінансовий ринок. Була приділена увага можливостям криптовалютних активів в майбутньому виступати потенційною заміною фіатних коштів, наведено порівняльний аналіз та переваги та недоліки даного рішення. Криптовалютні активи виступають цифровою валютою, яка не відмінну від долара та інших фіатних валют не має фізичного вираження, але захищена від підробок та копіювання та збільшення емісії якої неможливе.

У даному розділі, було теоретично розглянуто механізм функціонування технології блокчейн, яка лежить в основі більшості криптовалют. Були досліджені її основні характеристики, такі як незмінність, прозорість та безпека.

Також важливою частиною роботи у першому розділі, є аналіз правового поля криптовалюних активів, зокрема в контексті українського законодавства, а також з порівнянням з законодавством інших країн. Відносно нещодавно в Україні було обговорено введення законопроєкту №10225 від 07.11.2023 року, який повинен легалізувати ринок криптовалют та визначити правила їх оподаткування в Україні. Цей пункт є важливим, адже рахується одним із

головних умов введення в силу Закону України про “Віртуальні активи” від 17.02.2022 року №2074-IX.

Особлива увага була приділена характеристиці видів шахрайства, що часто зустрічаються у сфері криптовалют та способів відмивання коштів. Вивчення цього аспекту дозволило не лише ідентифікувати основні ризики, але й розробити методи оцінювання для їх мінімізації.

РОЗДІЛ 2. АНАЛІЗ БЛОКЧЕЙН ТЕХНОЛОГІЙ ТА МЕХАНІЗМІВ КРИПТОВАЛЮТНИХ ОПЕРАЦІЙ

2.1 Аналіз принципів роботи криптовалютних операцій

До прикладу для аналізу принципів криптовалютних операцій було взято блокчейн Ethereum, оскільки на сьогоднішній день він вважається найпопулярнішим серед користувачів для проведення транзакцій та підрахунків.

Блокчейн, можна назвати базою даних транзакцій, до якої надається глобальний доступ. Це означає, що кожен учасник має право читати та переглядати записи в даній базі даних, просто проводячи операції в мережі. Для зміни даних в базі даних блокчейну, оператор повинні створити так звану транзакцію, яка повинна бути прийнята всіма іншими учасниками мережі. Крім того, поки здійснена транзакція не буде застосована до глобальної бази даних блокчейну, жодна інша транзакція не може її змінити в порядку.

Блокчейну базу даних можна представити у вигляді таблиці, в якій перераховані залишки на всіх рахунках в електронній валюті. Якщо запитується переказ з одного рахунку на інший, транзакційна природа бази даних гарантує, що якщо сума віднімається з одного рахунку, вона завжди додається до іншого рахунку, з вирахуванням комісії яка перераховується валідаторам за підтвердження операції [22].

Крім того, транзакція завжди криптографічно підписується ініціатором, що дозволяє легко захистити доступ до певних модифікацій бази даних. У прикладі з електронною валютою проста перевірка гарантує, що тільки особа, яка має ключі від рахунку, може переказувати гроші з нього.

В блокчейні Ethereum стан складається з об'єктів, відомих як криптовалютні рахунки або гаманці, кожен з яких має 20-байтову адресу,

переходи між якими вважаються передачею інформації між рахунками. В акаунті Ethereum присутні чотири поля [42]:

- лічильник, який використовується для того, щоб гарантувати, що кожна транзакція може бути завершена лише один раз;
- поточний баланс криптовалюти ETH на рахунку;
- код контракту аккаунта (якщо присутній);
- сховище аккаунта (за замовчуванням порожнє).

Основною валютою для оплати за комісії транзакції, слугує ETH - це основне внутрішнє криптопаливо Ethereum. Загалом, існує два типи облікових записів: зовнішні облікові записи, якими керують за допомогою приватних ключів, і контрактні облікові записи, які керуються кодом розумного контракту.

Зовнішній обліковий запис не має коду, і з нього можна надсилати повідомлення, створюючи і підписуючи транзакцію. У випадку контрактного облікового запису, контрактний обліковий запис отримує повідомлення, його код активується, що дозволяє йому читати і записувати у внутрішнє сховище, а також надсилати інші повідомлення або створювати контракти по черзі.

Зверніть увагу, що розумні контракти в мережі Ethereum не слід розглядати як щось, що повинно бути виконано або дотримано, скоріше, вони більше схожі на автономних агентів, які живуть всередині середовища віртуальних машин Ethereum, завжди виконуючи певний фрагмент коду, коли їх підписує ініціатор повідомлення або транзакція, і мають прямий контроль над власним балансом ефіру і власним сховищем ключів/значень, щоб відстежувати постійні змінні [42].

Термін транзакція використовується в блокчейні Ethereum для позначення підписаного пакету даних, який зберігає повідомлення, що надсилається з зовнішнього облікового запису. Транзакції містять, як правило містять:

- одержувача повідомлення, або ж криптовалютну адресу одержувача;
- підпис, що ідентифікує відправника, або ж криптовалютну адресу ініціатора транзакції;

- кількість криптовалюти ефіру для переказу від відправника до одержувача;
- необов'язкове поле даних, або ж коментар до транзакції;
- значення “STARTGAS”, що представляє максимальну кількість обчислювальних кроків, які дозволяється зробити при виконанні транзакції. Дана сума буде означати максимальну ціну комісії за операцію, яка визначається до її проведення, базуючись на даних з блокчейн дослідника [42];
- значення “GASPRICE”, що представляє плату, яку відправник сплачує за кожен обчислювальний крок [42];

Поле одержувача, ініціатора та кількості криптовалютних активів в транзакції є основними, без яких проведення операції не є можливим. Поле даних не має функції за замовчуванням, але віртуальна машина має код операції, за допомогою якого контракт може отримати доступ до цих даних. До прикладу якщо контракт діє як служба реєстрації доменів у блокчейні, він може інтерпретувати дані, що передаються йому, як такі, що містять два поля, перше з яких являється домен для реєстрації, а друге це IP-адреса, на яку він реєструється. Контракт буде зчитувати ці значення з даних повідомлення і зберігати їх відповідним чином.

Поля “STARTGAS” і “GASPRICE” є критично важливими для парадигми захисту від відмови в обслуговуванні Ethereum [42]. Щоб уникнути ненавмисних або шкідливих нескінченних циклів або інших обчислювальних витрат в коді, кожна транзакція повинна обмежувати кількість зменшувати до мінімум кількість кроків виконання коду, які вона може використовувати.

У випадку з Monero блокчейном, де кожна операція проводиться з використанням новоствореної невидимої адреси, для гарантування, що всі вихідні адреси в транзакції з p виходами будуть різними навіть у випадках коли та сама адреса ініціатора використовується двічі, Monero використовує індекс виходу.

Кожен вихід транзакції має індекс $t \in \{1, \ldots, p\}$. Додаючи це значення до спільного секрету перед хешуванням, що й надає можливість забезпечити унікальність отриманих одноразових адрес [42]:

$$K_t^0 = H_n(rK_t^u, t)G + K_t^s = (H_n(rK_t^u, t) + k_t^s)G$$
$$k_t^o = H_n(rK_t^u, t) + k_t^s \ , \tag{2.1}$$

де K_t^0 – відкритий ключ одноразового виведення для транзакції за час t;

k_t^o – публічний ключ відповідний приватному K_t^0;

H_n– хеш-функція, яка виводить скалярне число, що використовується в операціях з еліптичною кривою;

r – випадково вибране скалярне число, котре діє як закритий ключ транзакції;

G – базова точка еліптичної кривої, яка використовується в Monero;

K_t^u – представляє відкритий ключ передбачуваного одержувача для транзакції в момент часу t;

K_t^s та k_t^s– приватні та публічні ключі відправника за час t.

Аналізуючи дану формулу, можна прийти до висновку, що одноразовий відкритий ключ K_t^0 згенерований хешуванням значення, пов'язаного з відкритим ключем одержувача rK_t^u з функцією H_nпомноживши його на базову точку еліптичної кривої G, та потім додавши компонент відкритого ключа відправника K_t^s . Результатом є унікальна адреса, яку тільки одержувач може розпізнати, як свою власну і використовувати за допомогою відповідного приватного ключа, котрий генерується схожим методом.

Фундаментальною одиницею обчислень в кожному блокчейні є газ, або ж комісія за транзакцію, як правило, обчислювальний крок коштує один газ, хоча деякі дії коштують більше газу, оскільки вони більш обчислювально складні або збільшують кількість даних, які повинні зберігатися як частина стану. Існує також плата в розмірі 5 газів за кожен байт в даних транзакції. Мета системи оплати полягає в тому, щоб змусити зловмисника платити пропорційно за кожен ресурс, який він споживає, включаючи обчислення, пропускну здатність і

зберігання [22]. Отже, будь-яка транзакція, яка призводить до споживання мережею більшої кількості будь-якого з цих ресурсів, повинна мати плату за газ, приблизно пропорційну збільшенню.

Контракти мають можливість надсилати "повідомлення" іншим контрактам. Повідомлення - це віртуальні об'єкти, якім не призначається ідентифікаційний номер, та існують тільки в віртуальному середовищі машин Ethereum. По суті, повідомлення схоже на транзакцію, за винятком того, що воно створюється контрактом, а не зовнішнім актором [19]. Повідомлення створюється, коли код контракту, що виконується в даний момент, виконує операційний код “CALL”, який створює і виконує повідомлення. Як і транзакція, повідомлення призводить до того, що обліковий запис одержувача виконує його код. Таким чином, контракти можуть мати зв'язки з іншими контрактами точно так само, як і зовнішні суб'єкти.

Зауважте, що квота на газ, призначена транзакцією або контрактом, застосовується до загального обсягу газу, спожитого цією транзакцією та всіма під транзакціями. Наприклад, якщо зовнішній актор A надсилає транзакцію B, витративши 1000 газу, і B витрачає 600 газу до відправлення повідомлення C, а внутрішнє виконання C витрачає 300 газу до повернення, то B може витратити ще 100 газу до того, як закінчиться газ.

Якщо розглядати комісії в блокчейні більш детально, можна прийти до висновку, що оскільки кожна транзакція, опублікована в блокчейні, накладає на мережу витрати, пов'язані з необхідністю її завантаження та перевірки так званими валідаторами [42], існує потреба в певному регулятивному механізмі, який, як правило, включає в себе комісію за транзакції, щоб запобігти зловживанням.

Підхід за замовчуванням, який використовується в біткоїні, полягає в тому, що комісія є суто добровільною і покладається на майнерів, які виступають в ролі контролерів і встановлюють динамічні мінімуми.

Цей підхід був дуже позитивно сприйнятий крипто-спільнотою, особливо тому, що він є ринковим, дозволяючи попиту і пропозиції між майнерами і

відправниками транзакцій визначати ціну. Однак проблема в тому, що обробка транзакцій не є ринком, хоча інтуїтивно привабливо трактувати обробку транзакцій як послугу, яку майнер пропонує відправнику, насправді кожна транзакція, яку майнер включає, повинна бути оброблена кожним вузлом мережі, тому переважну частину витрат на обробку транзакцій несуть треті сторони, а не майнер, який приймає рішення про те, чи включати її чи ні [42]. Таким чином, дуже ймовірно, що виникнуть проблеми, пов'язані з трагедією спільного користування.

Ринковий механізм демонструє унікальну властивість само корекції, коли розглядається певне спрощене припущення. Це явище розгортається наступним чином: По-перше, транзакція ініціює k операцій, приносячи винагороду в розмірі kR майнеру, який її обробляє, де R визначається відправником, а k і R приблизно відомі майнеру заздалегідь. По-друге, обробка кожної операції коштує C для кожного вузла, якщо припустити, що всі вузли мають однакову ефективність. По-третє, є N майнінгових вузлів, кожен з яких має рівну частку загальної обчислювальної потужності, а саме $1/N$ [42]. Нарешті, сценарій припускає відсутність будь-яких повних вузлів, які не майнять.

Майнер буде готовий обробити транзакцію, якщо очікувана винагорода буде більшою за витрати. Таким чином, очікувана винагорода становить kR/N , оскільки майнер має $1/N$ шансів обробити наступний блок, а вартість обробки для нього становить просто kC.

Отже, майнери будуть включати транзакції, де $\frac{kR}{N} > kC$, або $R > NC >$. Потрібно зауважити, що R - це комісія за операцію, яку сплачує відправник, і, таким чином, є нижньою межею вигоди, яку отримує відправник від транзакції, а NC - це вартість обробки операції для всієї мережі разом узятої. Таким чином, майнери зацікавлені в тому, щоб включати в мережу лише ті транзакції, для яких загальна загальна вигода перевищує витрати [42].

2.2 Проблематика відслідковування шахрайських транзакцій в блокчейні

Технологія блокчейн, відома своєю децентралізацією, прозорістю та незмінними характеристиками. Однак потрібно зазначити, що паралельний розвиток анонімних блокчейн-мереж і простота створення численних гаманців створили значні труднощі у відстеженні транзакцій, створивши загадкове середовище для регуляторів, судових аналітиків і фінансових установ.

Як вже було зазначено, створити гаманець у будь якій із блокчейн мереж є доволі легко та не потребує ніякої додаткової верифікації особи, цим самим забезпечуючи псевдо-анонімність. Користувачі можуть без особливих зусиль створити кілька гаманців, кожен з яких має окрему адресу, тим самим фрагментуючи слід своїх транзакцій між численними суб'єктами. Таке розповсюдження затушовує шлях руху коштів і ускладнює відстеження транзакцій до єдиного джерела [19].

Потрібно також зазначити, що швидкість обробки операцій в блокчейні може конкурувати з найкращими банками в Україні, не те що в Європі коли можна очікувати виконання транзакції по декілька днів. У випадку блокчейна операція виконується за лічені секунди і залежить лише від популярності мережі вибраної для роботи та кількості валідаторів, які виступають у ролі емітентів банку в крипто-валютному світі. Потрібно зазначити, що значна швидкість, з якою здійснюються та підтверджуються транзакції в певних мережах блокчейн, ще більше ускладнює відстеження. Високошвидкісні транзакції дозволяють користувачам швидко переказувати активи між кількома гаманцями, заплутуючи сліди транзакцій до того, як можна буде провести всебічний аналіз.

З ростом популярності криптовалюти було також значно збільшено ріст в кількості користувачів які розглядають блокчейн рішення, як єдиний спосіб ведення фінансових операцій. У зв’язку з цим виникли різні способи маскування дій в блокчейні, одним з яких виступає блокчейн міксер.

Блокчейн міксер - це служба, яка змішує криптовалюти з різних джерел, щоб зробити їх походження менш помітним. Це може бути використано для підвищення анонімності користувачів, які хочуть захистити свою приватність або уникнути відстеження правоохоронними органами. Його робота заключається в прийманні криптовалюти від декількох користувачів і об'єднуванні їх у одну транзакцію [40]. Ця транзакція потім розбивається на кілька менших транзакцій, які перераховуються на різні гаманці. Це ускладнює відстеження походження криптовалюти, оскільки важко визначити, хто є відправником і одержувачем кожної окремої транзакції.

Криптовалютні міксери, також відомі як "тумблери", працюють на основі принципів криптографії та анонімності, щоб приховати сліди криптовалютних транзакцій. Як правило, процес включає в себе комбінацію таких методів, як розбиття транзакцій на менші частини, використання декількох гаманців і додавання часових затримок. Ось спрощений концептуальний огляд процесу:

Якщо розглянути весь процес концептуально, то учасник криптовалютної операції надсилає кошти на загальну адресу міксера, перед цим вказавши очікувану адресу отримання, програма в свою чергу розбиває отриману криптовалюту на менші одиниці. Цей процес може бути різним, адже деякі міксери ділять суми випадковим чином, а інші використовують фіксовані номінали запрограмовані в смарт контракті до цього.

Розбиті одиниці потім змішуються з іншими транзакціями всередині програми, тобто надсилаючи кошти між сотнями гаманцями приманок, або ж як їх називають проміжних гаманців, контрольованих міксером. Щоб ще більше заплутати слід, програми часто вводять затримки в часі перед відправкою змішаних монет, який може бути випадковим або визначеним користувачем.

Останнім кроком є отримання змішаної, криптовалюти яка надсилається на адреси призначення, надані користувачами. Ці адреси часто є новими і не пов'язані безпосередньо з початковими адресами користувачів.

Важливо відзначити, що ефективність міксера в забезпеченні анонімності залежить від різних факторів, таких як кількість користувачів, обсяг транзакцій і

протоколи роботи міксера. Крім того, використання міксерів є суперечливим і може бути незаконним у деяких юрисдикціях, оскільки вони можуть бути використані для сприяння відмиванню грошей або іншій незаконній діяльності. Крім того, блокчейн міксери можуть бути атаковані хакерами, які можуть вкрасти криптовалюту [40]. Блокчейн міксери можуть бути використані для різних цілей, включаючи:

- Підвищення анонімності. Блокчейн міксери можуть бути використані для підвищення анонімності користувачів, які хочуть захистити свою приватність;
- Уникнення відстеження. Блокчейн міксери можуть бути використані для уникнення відстеження правоохоронними органами;
- Легалізація доходів отриманих злочинним шляхом. Блокчейн міксери можуть бути використані для легалізації доходів від злочинності.

Потрібно також зазначити, про існування додаткового шару анонімності в блокчейні, як такому, завдяки застосування приватних монет. Монети приватності, або ж як їх ще називають криптовалюти з функціями захисту анонімності, спрямованими на підвищення анонімності та обмеження відстежуваності. Вони функціонують подібно до звичайної готівки, але в межах цифрової економіки. Коли ви знімаєте готівку в банкоматі, банк веде запис, але він не має можливості дізнатися, що ви робите з грошима після даної операції, якщо тільки ви не покладете їх назад в банкомат. Більшість криптовалютних бірж, які пропонують монети конфіденційності, вимагають від користувачів пройти первинну ідентифікацію [41]. Через притаманну монеті приватності функцію конфіденційності, цим біржам складно відстежити або розкрити інформацію про наступні операції з даними валютами.

Хоча приватні монети більш стійкі до відстеження, ніж інші криптовалюти, ніщо не є по-справжньому анонімним. Як наслідок, слідчі з розширеними можливостями відстеження можуть відстежувати переміщення приватних монет.

Анонімність приватних монет призвела до того, що багато хто вважає, що вони в основному використовуються для відмивання грошей, хакерства та фінансування тероризму. Хоча зловмисні дії, безумовно, відбуваються в блокчейні, можна зазначити, що більшість злочинних операцій все ще використовують біткоїн (рис. 2.1), оскільки він є транскордонним, миттєвим і ліквідним. Монети приватності, як правило, не такі ліквідні, як біткоїн, що ускладнює для злочинців їх придбання та переведення у фіатну валюту [41].

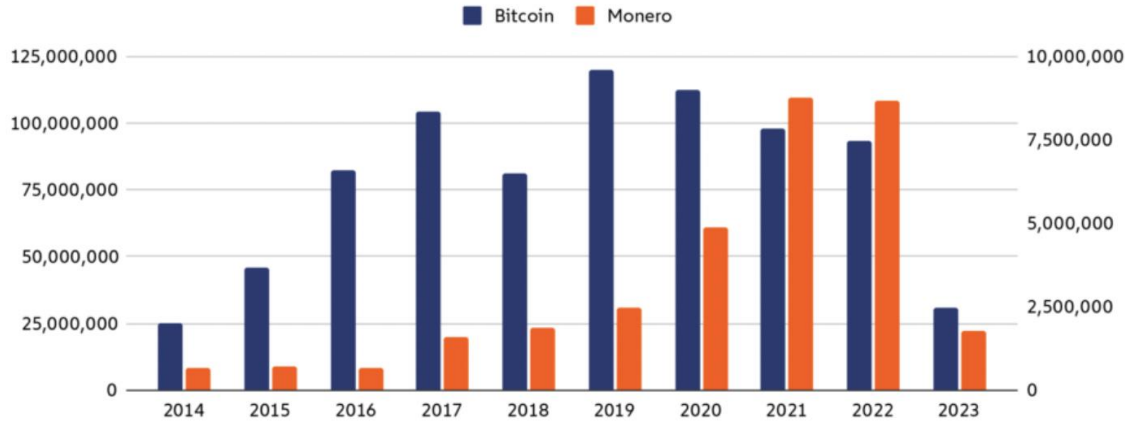

Рис. 2.1. Кількість транзакцій в блокчейнах Bitcoin та Monero

Як одним із найпопулярніших прикладів приватних монет, можна розглянути блокчейн Monero, з його монетою XMR. Monero (XMR) - це криптовалюта, яка використовує різні криптографічні методи для приховування деталей транзакцій, забезпечуючи анонімність як відправника, так і одержувача, а також приховуючи суму транзакції.

Акаунти в блокчейні Monero, на відміну від звичайного блокчейну, мають 2 ключі: ключ витрат і ключ перегляду. Як випливає з їхніх назв, ключ витрат використовується для проведення операцій з криптовалютними коштами з рахунку Monero, а ключ перегляду, для діставання інформації про активи на даному рахунку [43].

Першим у даному списку ключів є ключ витрат, котрий постає як 256-бітове представлення, генеруючи як випадкова послідовність слів. Він є необхідним для створення ключа перегляду, який є хешовим представленням ключа витрат.

Генерацію публічних ключів в Monero блокчейні для адреси витрат та перегляду можна подати у вигляді формули [43]:

$$A = a \times G, \tag{2.2}$$

де A - виступає публічним ключем для адреси перегляду або адреси витрат;

a - приватний ключ витрат або перегляду

G - є базовою точкою криптографії еліптичних кривих, адже Monero використовує пари ключів EdDSA на основі кривої Ed25519, різновиду кривої Едвардса.

В роботі даного блокчейну імплементовані новітні принципи маскування та анонімності, такі як кільцеві підписи і конфіденційні транзакції та приховані адреси задля забезпечення додаткової анонімності учасників операції. Також ведеться обговорення задля реалізації додаткового захисту мережевого рівня для маскування можливого виявлення IP-адрес відправника та одержувача за допомогою технології I2P (проєкт Невидимий Інтернет).

Кільцеві підписи, використовуються для захисту особи відправника, кільцеві підписи об'єднують ключі облікового запису користувача з публічними ключами з блокчейну Monero, утворюючи "кільце" можливих підписантів. Таким чином, сторонні особи не можуть визначити справжнього відправника, що забезпечує анонімність транзакцій. Такий рівень заплутаності створює ризик подвійної витрати, тому кожна транзакція в Monero також генерує образ ключа, тобто унікальний вихідний криптографічний ключ [43]. Оскільки вихідні дані зашифровані, неможливо провести повторну інженерію транзакції на основі її образу ключа. Якщо хтось спробує здійснити атаку з подвійною витратою, протокол виявить її за образом ключа і відхилить другу транзакцію.

Monero також використовує одноразові адреси, коли ініціюється транзакція, генерується одноразова невидима адреса. Доступ до коштів, надісланих на невидима адресу, може отримати тільки одержувач, який має приватний ключ, що робить зв'язок між відправником і одержувачем

нерозрізненим для зовнішніх сторін, що в свою чергу ще більше ускладнює відстеження платіжних потоків.

Для генерацій таких адрес з пари ключів (A та B - як було зазначено вище), процес включає кілька кроків. По-перше, отримується Keccak-256 хеш (префіксу + B + A), де префікс є однобайтовом значенням 0x12, згідно зі стандартом Monero [43]. Далі, до отриманого хешу додається перші 4 байти цього хешу до конкатенації в якості контрольної суми, в результаті чого ми отримуємо 69-байтну послідовність.

Після цього дана 69 байтна послідовність конвертується в cnBase58, варіацію кодування Base58, яка забезпечує фіксовану довжину результату, в даному випадку вона створює адресу Monero довжиною 95 символів.

Цікавим аспектом Monero є використання невидимих адрес, на відміну від традиційних облікових записів у блокчейні, Monero використовує безліч одноразових публічних адрес і зображень ключів, доступ до яких мають лише власники відповідних приватних ключів.

Ще одна імплементована технологія, задля забезпечення анонімності є Кільцеві конфіденційні транзакції (RingCT). Вона працює таким чином, що приховує суму транзакції, застосовуючи криптографічні зобов'язання, які вимагають від відправника довести, що вхідні суми дорівнюють вихідним, не розкриваючи фактичних сум. Все це стало можливим після імплементації 1.0 версії даної технології, де для набору з M входів транзакцій, M входам транзакцій відповідають M кільцевих підписів з розміром кільця O(n) кожна, де n - кількість можливих підписантів [43].

Крім того, чиста сума транзакції (яка повинна дорівнювати нульовому зобов'язанню) також відповідає кільцевому підпису з розміром кільця O(n). Таким чином, Monero RingCT має (M + 1) підписів розміром O(n) кожен. Оскільки великий розмір підпису обмежує кількість n можливих підписантів, значення n в офіційному програмному забезпеченні гаманця Monero коливається лише від 5 до 20 [43].

2.3 Аналіз моделей та методів ідентифікацій та відслідковування підозрілих на шахрайство транзакцій у блокчейні

Дії в мережі блокчейн можна назвати псевдо-анонімними, оскільки майже кожен блокчейн надає доступ до перегляду даних про транзакції, смарт-контракти, адреси та багато іншого він не є повністю конфіденційним. За винятком лиш декількох блокчейнів які пропонують повну анонімність, до прикладу Monero блокчейн який хоч і має відкритий код, все ж не володіє інформацією про дії своїх користувачів в блокчейні.

В даній роботі ми розглядаємо пошук шахрайських платежів у блокчейні Ethereum, який є найчастіше використовуваним із блокчейнів. Оскільки дані з користування ETH блокчейну є публічними, це надає можливість користувачам переглядати інформацію про транзакції, смарт-контракти адреси та багато іншого, за допомогою блокчейн дослідників (Blockchain Explorer), як у пошуковій системі використовуючи хеш транзакції (ID транзакції).

Одним із способів аналізу блокчейн транзакцій є використання блокчейн дослідника, що являє собою спеціальне програмне забезпеченням, яке використовуючи інтерфейс прикладного програмування (API) та вузол (ноду) блокчейна, отримує різну інформацію, заносячи її перед цим до бази даних, та надає її користувачам у зручному для розуміння вигляді. Підсумовуючи, можна сказати, що дослідник – це пошукова система, яка дозволяє отримувати доступ практично до будь якої інформації з блокчейну.

Якщо брати до прикладу, один з найпопулярніших блокчейн дослідників у блокчейні Ethereum, Etherscan, то найчастіше, для чого його використовують, це:

- Проводити обрахунки комісії (газ) за майбутню транзакцію;
- Переглядати та перевіряти ETH контракти, їхню роботу та правильність, чесність у реалізації.

- Переглядати та аналізувати криптовалютні активи, які знаходяться на тому, чи іншому крипто гаманці;
- Переглядати обробку транзакції в блокчейні, які знаходяться в різних станах (виконана, невдала чи незавершена);
- Надавати та забирати доступ вашого гаманця до будь яких програм.

Блокчейн дослідник можна також використовувати, як аналітичну платформу. Кожен користувач, має доступ до аналізу показників мережі, яку обслуговує дослідник, як зміна витрати на комісію в блокчейні, відстеження історії транзакцій на предмет підозрілої активності. Блокчейн дослідники, працюють використовуючи API бази даних та блокчейн вузли (ноди) для доступ та перетворення даних з блокчейну [27].

Використовуючи API, дослідник також має змогу взаємодіяти з іншими комп'ютерами, які використовуються як вузли блокчейну. Спочатку інформація отримується від вузла блокчейну та передається до спеціальної бази даних, де зберігається у форматі таблиць з можливістю проведення пошукових операцій.

Також присутній відповідний UI сервер, котрий є відповідальним за створення веб-сторінки, через яку користувач має змогу взаємодіяти з сервісом, коли він вводить дані для пошуку та відправляє цю інформацію до разом до бекенд серверу. Бекенд сервер, в свою чергу, використовуючи інформацію отриману з вузлів надсилає відповідь у браузер користувача (рис. 2.2).

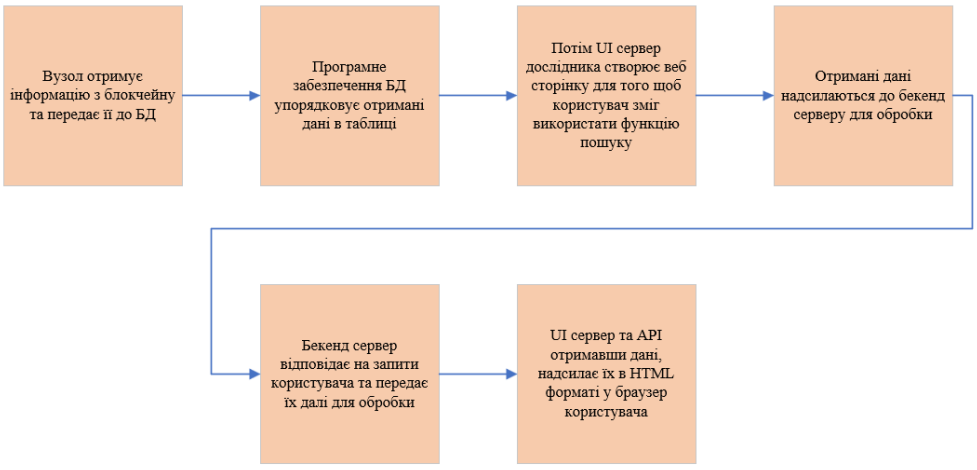

Рис. 2.2. Графічна ілюстрація роботи блокчейн дослідника

Найпопулярнішим серед блокчейн дослідників в крипто мережі є Etherscan, яким можна користуватись безкоштовно, для перегляду інформації про криптовалюні гаманці та транзакції використовуючи їх унікальний хеш.

Користуючись ним, можна захистити себе від можливих шахраїв, виявити підозрілу блокчейн активність та перевірити інформацію яка знаходиться в мережі. Відносно нещодавно також було додано можливість перегляду комісії за криптовалютні операції, яка присутня в даний момент в мережі, що дозволяє учасникам краще планувати витрати операцій [27].

Etherscan є дуже простим у своєму використанні, користуючись пошуковим рядком ми можемо знайти усю необхідну інформацію про баланс рахунку, яка саме криптовалюта на ньому знаходиться на даний момент, список транзакцій, які робив цей гаманець за час його існування (рис. 2.3), а також й інформацію про створений розумний контракт, оскільки кожен із створених програмних застосунків має свою унікальну адресу подібну до адреси криптовалютного гаманця.

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x642fd2aa742f9d16e2f...	Transfer	14866666	38 secs ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000852269622
0xecaeca02ae3967ba2a...	Transfer	14866525	30 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000791166432
0xdf5a7bcfbf7e411aba40...	Transfer	14866509	34 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.001101819544
0xa10c07cd3300ca8b8d...	Transfer	14866441	52 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000662559157
0x113ea21418c9459ceb...	Transfer	14866368	1 hr 8 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000798673397
0x3bba34677ab6db61b4...	Transfer	14866350	1 hr 12 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000949489949
0x2a19d87736fed25843...	Transfer	14866331	1 hr 17 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000699415764
0x585f8f43c82eff5ecbe8...	Transfer	14866291	1 hr 28 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000842399789
0x61df36193fb0966041c...	Transfer	14866250	1 hr 38 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.001016574921
0x28c5c479b31137f9320...	Transfer	14866249	1 hr 39 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.000944171685
0xd165f3b43b9ff6ae502...	Transfer	14866222	1 hr 45 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.001136206442
0x90c1ef9a9b7503c7ca9...	Transfer	14866153	2 hrs 2 mins ago	0x4e824dc4d066cfaf312...	OUT	Tether: USDT Stablecoin	0 Ether	0.001571655816

Рис. 2.3. Список транзакцій

Проте дана система має низку недоліків, серед яких незручність у відслідковуванні великої кількості транзакцій. До прикладу наш зловмисник хотів заховати викрадені кошти, переводячи їх з гаманця на гаманець подекуди розділяючи суму на менші частини та знову відправляючи на інші гаманці. В

такому випадку, відслідковування їх може зайняти години, а можливо й дні, залежить від винахідливості нашого зловмисника. Оскільки нам прийдеться, аналізувати кожну транзакції шукаючи кінцевий гаманець (рис. 2.4).

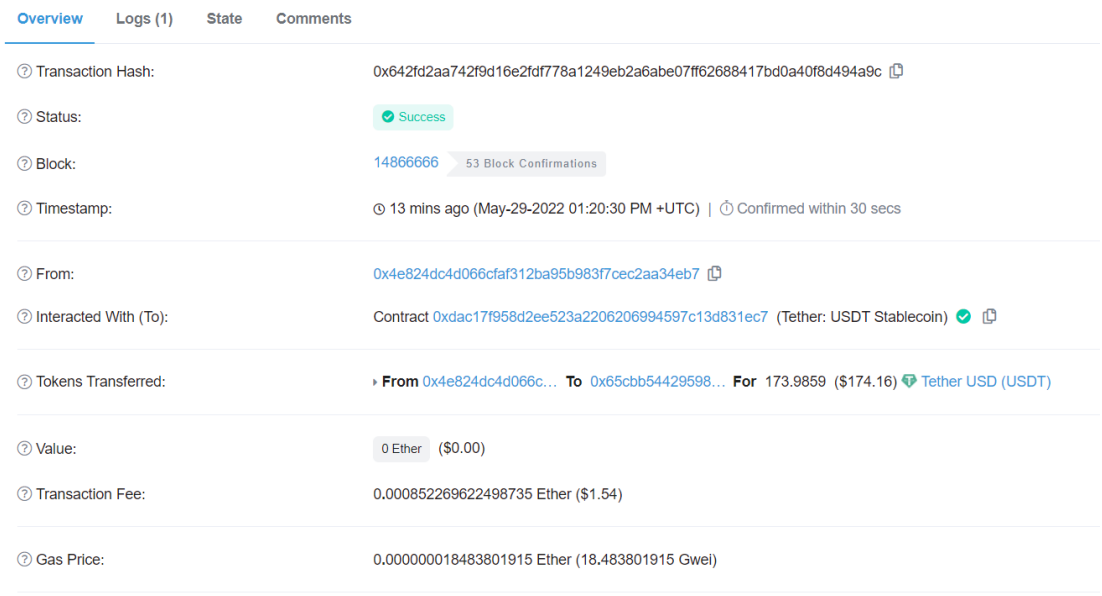

Рис. 2.4. Інформація про транзакцію на Etherscan

Сьогодні, розслідування шахрайства та злочинних дій в області криптовалюти неможливо без використання автоматизованих аналітичних інструментів для блокчейн мереж. До прикладу компанія CryptoLocker розробила власний спосіб аналізу блокчейн інформації [45], розробникам вдалося реалізувати програму на основі штучного інтелекту, що дозволяє ідентифікувати цифрові сліди, які можуть більш детально розкрити інформацію про особистість, що стоїть за безліччю операцій в блокчейн мережах[46].

Наступним аналогом, який можна привести на порівняння до розробленого методу є програмний інструмент SkyTrace від компанії Certik.

Certik є одна з лідируючих компаній серед забезпечення безпеки у світі блокчейн. Одним із найголовніших продуктів компанії є проведення аудиту смарт-контрактів, протоколів блокчейну та додатків Web3 перед їх розгортанням.

Відносно нещодавно компанія презентувала свою нову розробку – інструмент SkyTrace, який являється частковою копією Etherscan, проте з

можливість візуалізувати отриману інформацію, для її легкого сприйняття, та провести фільтрацію за криптовалютним активом який було надіслано або прийнято на той чи інший гаманець (рис. 2.5).

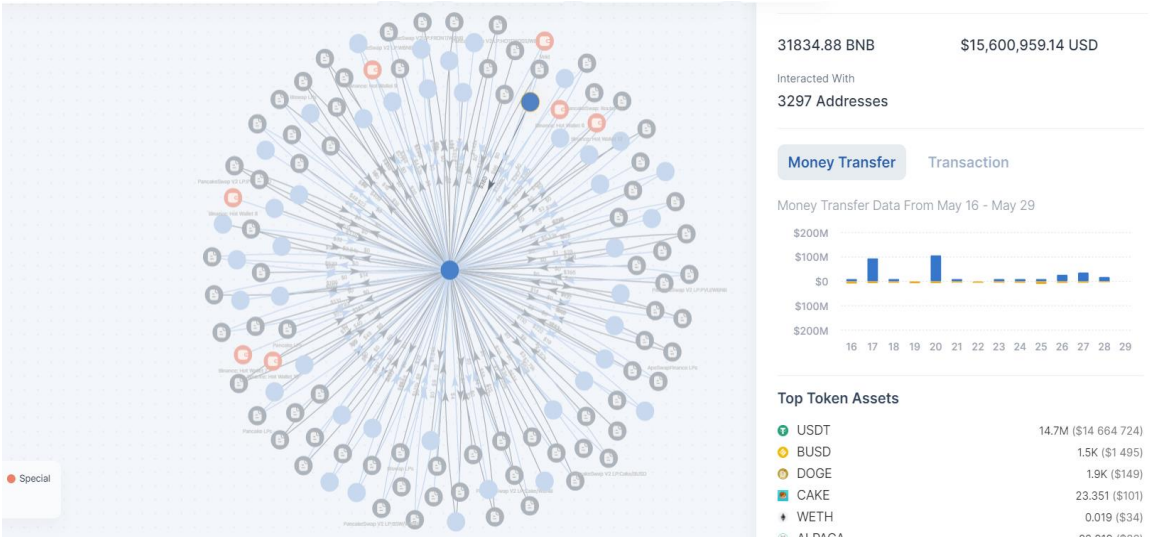

Рис. 2.5. Інтерфейс інструменту SkyTrace

Завдяки партнерству з великою кількість обмінників та бірж, даний інструмент, також надає можливість проаналізувати на чий саме контракт були надіслані криптовалютні активи для подальшого використання (рис. 2.6). Як видно з представленого рисунку, кошти були надіслані на гарячий гаманець криптовалютної біржі Binance.

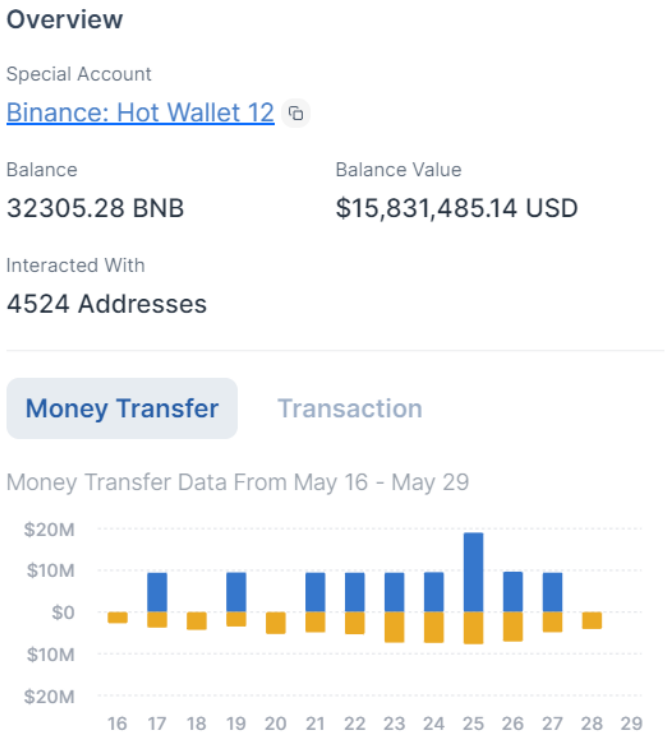

Рис. 2.6. Детальна інформація про контракт отримувача

Сервіс Skynet, який також було інтегровано в пакет Certik, пропонує онлайн-платформу з хмарним програмним забезпеченням, призначеним для проведення оцінки безпеки блокчейн ініціатив і смарт-контрактів (рис. 2.7). З його допомогою, можливо здійснити дослідження домену Web3, отримавши комплексний аналіз в результаті.

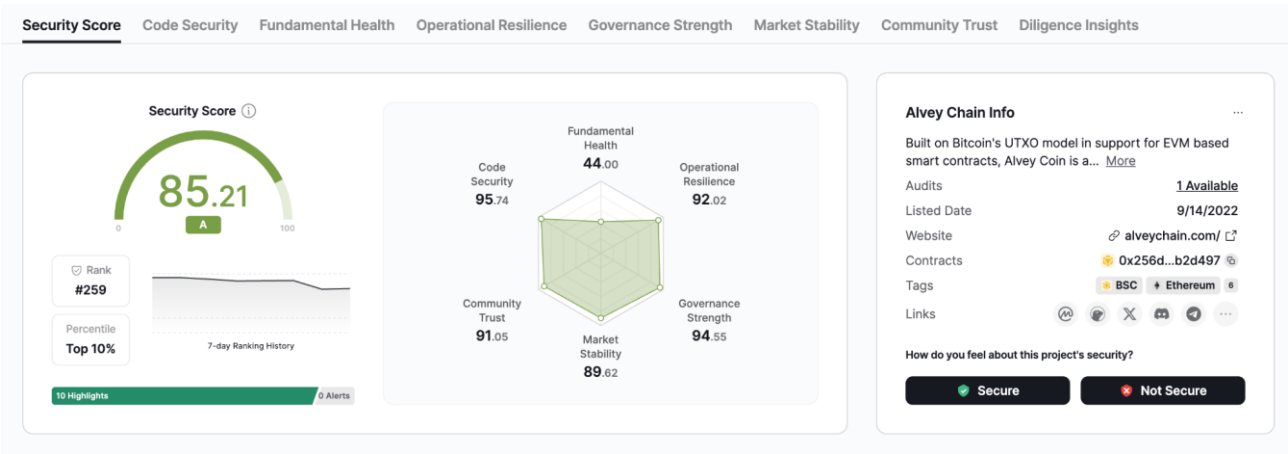

Рис. 2.7. Інтерфейс сервісу Skynet

На додаток, сервіс Skynet надає можливість проводити розгорнутий аналіз смарт контрактів по геопозиції користувачів (рис. 2.8) та довірі від власників криптовалютних активів того чи іншого проєкту.

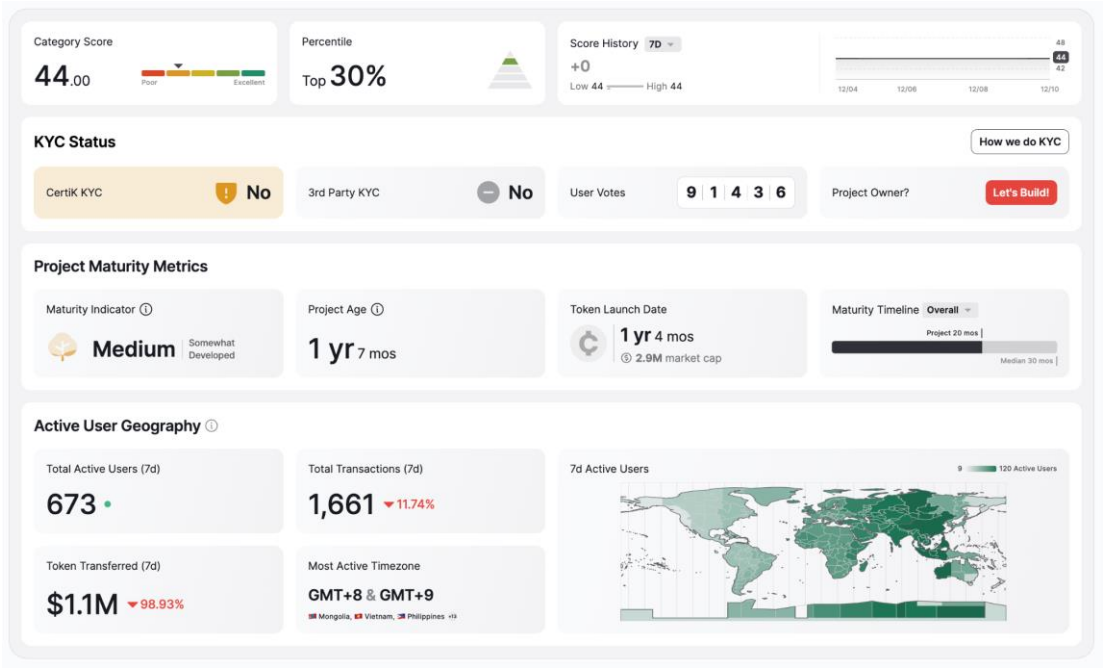

Рис. 2.8. Інтерфейс сервісу Skynet. Фільтрація по геопозиції

Також, потрібно приділити увагу нещодавно випущену Open Source проєкту “ChainAbuse”. Даний сервіс представляє собою загальнодоступну базу даних, яка відстежує біткоїн-адреси, що були використані в шахрайстві та інших незаконних діях (рис. 2.9). Користувачі можуть надсилати звіти до бази даних, які потім перевіряються командою модераторів, у випадку якщо повідомлення підтверджується, криптовалют адреса додається до бази даних та позначається як потенційно небезпечна [31].

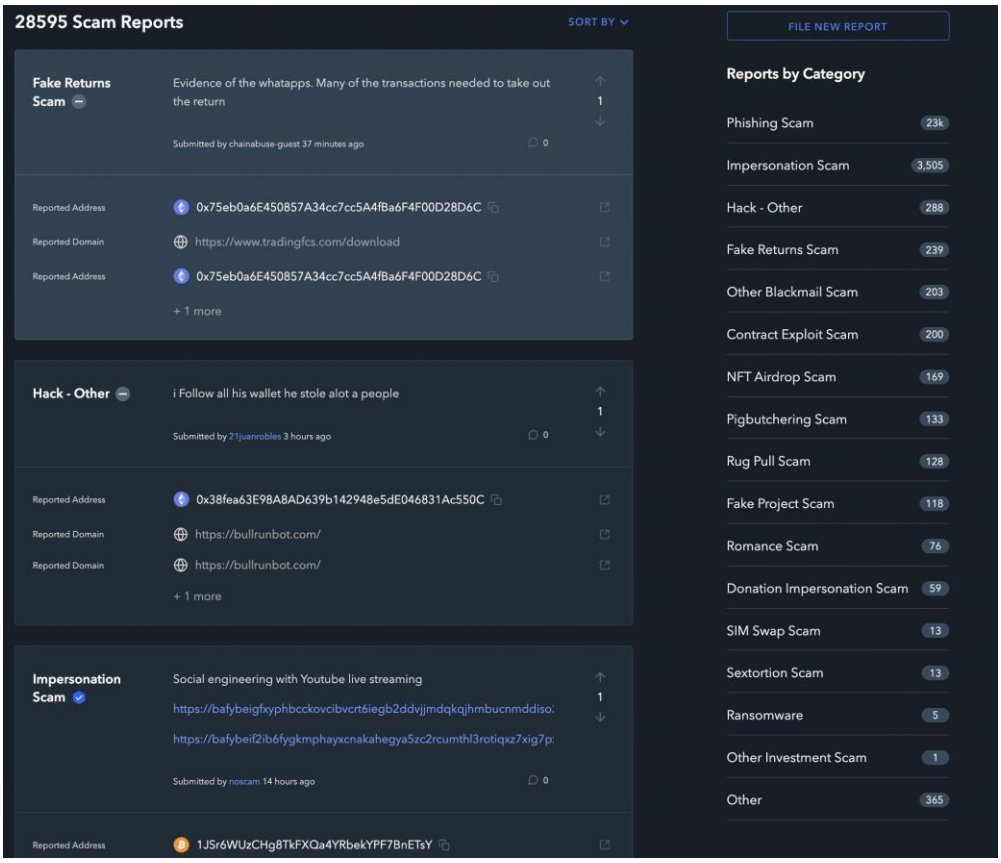

Рис. 2.9. Інтерфейс сервісу ChainAbuse

Користувачі можуть перевірити базу даних, щоб побачити, чи була позначена введена адреса шахрайською, перш ніж відправляти на неї активи.

“Chain Abuse” є цінним ресурсом для крипто-спільноти і допомагає зробити криптовалютні операції безпечнішими та надійними для всіх користувачів.

Веб-сайт “Scam Alert” – також виступає сервісом, для перевірки та валідації адрес на предмет зловживання. Різниця між даними сервісами полягає в тому, що “Scam Alerts” підтримує більшу кількість криптовалютних мереж, цим самим забезпечує повний обсяг необхідної інформації, адже існує безліч комбінованих гаманців, котрі надають змогу маючи одну адресу проводити крипто транзакції в десятках мереж.

Scam Alert збирає інформацію про шахрайство з різних джерел, включаючи новини, повідомлення в соціальних мережах і звіти користувачів (рис. 2.10). Потім ця інформація використовується для створення бази даних відомих

шахрайств і шахрайських веб-сайтів. Користувачі можуть перевірити базу даних Scam Alert, щоб дізнатися, чи пов'язаний криптовалютний веб-сайт або адреса з відомим шахрайством. Вони також можуть повідомляти про нові шахрайства в базу даних [32].

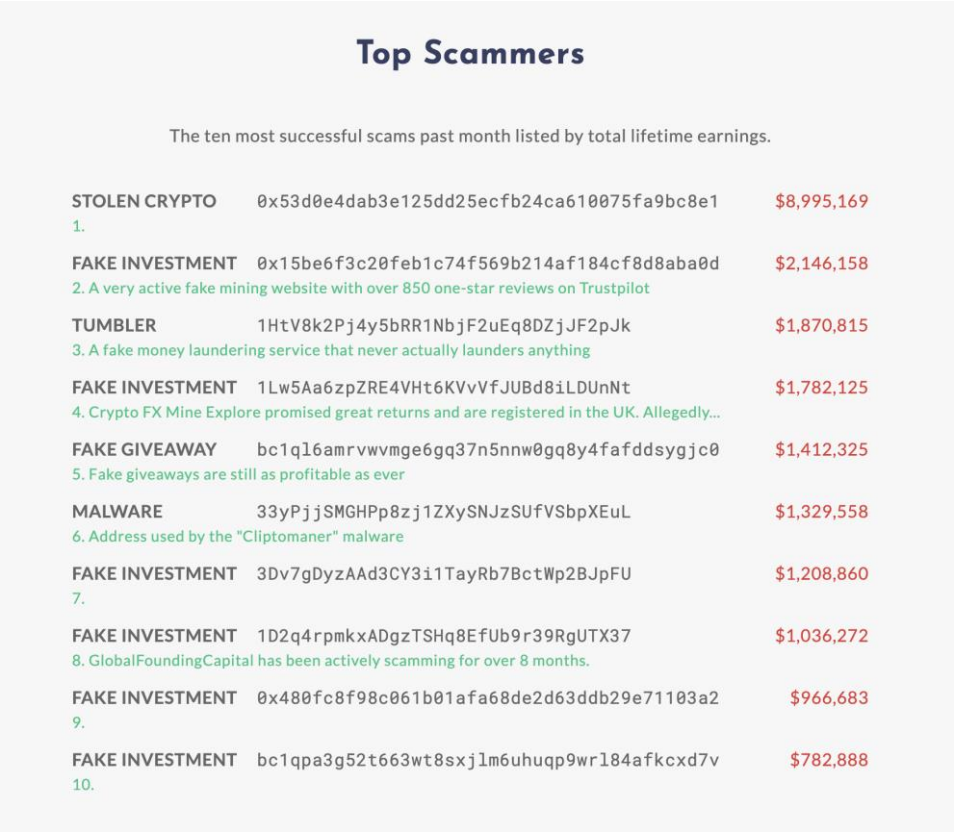

Рис. 2.10. Інтерфейс сервісу ScamAlert

Одним із потужних інструментів аналізу є також платформа Crystal Blockchain, яка дозволяє проводити ризик-аналіз крипто монет (рис. 2.11).

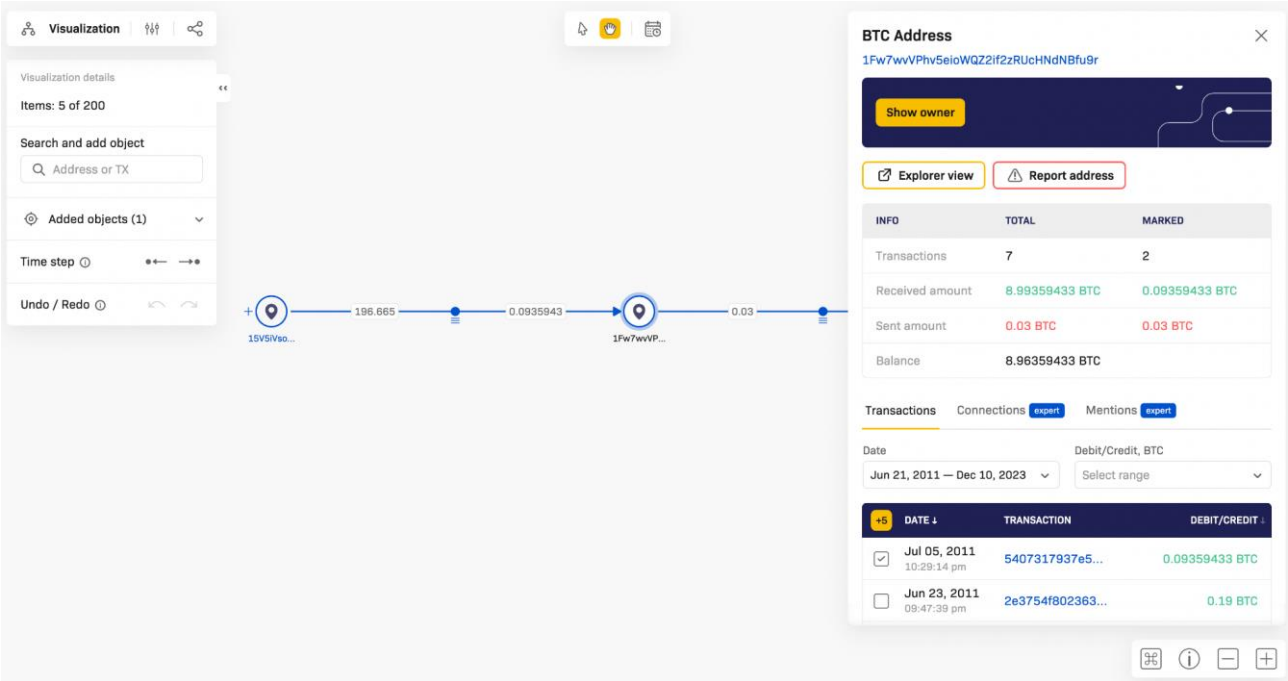

Рис. 2.11. Інтерфейс сервісу Crystal Blockchain

Основною аналітичною цінністю сервісу Crystal Blockchain є база ідентифікаційних та неідентифікованих власників біткоїн адрес, що підтримується в актуальному стані. Адреси розділені на такі типи:

- автоматична покупки/продажу криптоактивів;
- кримінальні торгові майданчики в TOR мережі;
- суб'єкти надання нелегальних послуг за криптовалюту через TOR мережу;
- криптовалютні біржі з градацією ризику відмивання грошей;
- шахрайські обмінники криптовалют;
- сайти азартних ігор;
- сервіси змішування;
- системи обробки криптовалютних платежів;
- шахрайські ресурси, пов'язані з криптовалютами;
- адреси, на які виводились вкрадені монети.

Для кожного власника блокчейн-адреси чи крипто гаманця визначається ризикова оцінка, яка базується на ймовірності його участі в незаконних діях та

законності походження коштів. Crystal Blockchain включає п'ять основних та два додаткових інструменти для проведення розслідувань.

Інструмент “Справи” дозволяє керувати розслідуваннями, створювати та переглядати справи, які включають деталі, адреси, візуалізації та відстеження [35]. “Дослідник” використовується для аналізу транзакцій, блоків та адрес, відображаючи інформацію про власників біткоїн-адрес, їх типи, основні майнери та курс біткоїна.

“Відстеження” служить для моніторингу руху коштів у часі по конкретних транзакціях чи групах транзакцій, що може допомогти ідентифікувати власників біткоїн-адрес через відповідні правові процедури (рис. 2.12).

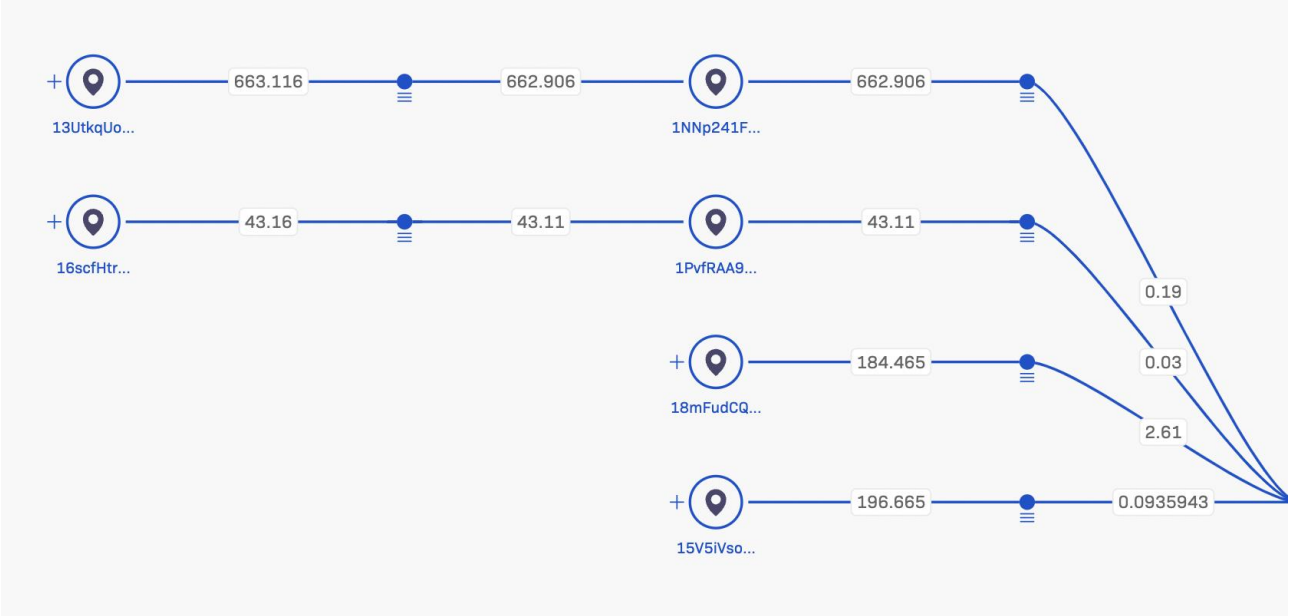

Рис. 2.12. Відображення сервісу Відстеження

“Монітор” призначений для комплаєнс-офіцерів, дозволяє оцінювати ризикованість транзакцій.

“Інформаційна панель” надає користувачам інформацію про створенні та збереженні справи, візуалізації, списки відстеження, закладки аналізу адрес, блоків, транзакцій та власників адрес. При дослідженні біткоїн-адреси за допомогою “Дослідника”, Crystal надає інформацію про категорію власника адреси, поточний баланс, кількість транзакцій, статус, дати активності та оцінку ризику [35].

За допомогою інструменту “Візуалізація” транзакції з конкретною біткоїн-адресою можуть бути представлені у вигляді графіка, що дозволяє керувати відображенням вузлів. Цей інструмент демонструє якісно-кількісну діаграму взаємодії власника біткоїн-адреси з іншими ідентифікованими власниками [35]. Враховуючи ці функції, платформа Crystal Blockchain здатна ефективно сприяти розслідуванню кримінальних порушень, пов'язаних з криптовалютами.

Кожен із перелічених сервісів має свої переваги та недоліки. Проте все ж доволі складно визначити, сервіс котрий би мав зрозумілий веб інтерфейс та надавав можливість проведення аналізу за короткий період часу.

2.4 Визначення ключових критеріїв і метрик для виявлення шахрайських транзакцій в блокчейні

У пошуках виявлення шахрайських транзакцій у технології блокчейн критичним аспектом є встановлення конкретних критеріїв і показників, тригерів для автоматизованої системи. Цей підхід є невід’ємною частиною розробки програмного модуля для моніторингу підозрілих на шахрайство операцій в блокчейні.

Одним з яких може слугувати перевищена кількість розміру активів в одній операції. Транзакції, які значно перевищують середні значення, можуть свідчити про шахрайську діяльність, особливо якщо вони не відповідають типовим моделям залученого користувача чи організації. Наприклад, користувач, історія якого характеризується невеликими послідовними транзакціями, але раптово бере участь у транзакції значного масштабу, може свідчити про спробу переміщення незаконних коштів. Подібні аномалії є потенційними тривожними ознаками, і їх слід піддати подальшому дослідженню.

Іншим важливим критерієм може слугувати частота операцій. Незвично велика кількість транзакцій протягом короткого періоду часу, особливо якщо вона відхиляється від норми для певного криптовалютного гаманця, може свідчити про потенційне шахрайство. Цей шаблон може представляти техніку, відому як міксинг, коли великі суми грошей розбиваються на менші, менш підозрілі суми. Система моніторингу повинна бути відкалібрована, щоб позначати такі аномалії, беручи до уваги звичайну частоту транзакцій для кожного користувача чи облікового запису.

Вивчення моделей транзакцій відіграє важливу роль у виявленні шахрайства. Операції, які відбуваються за нерегулярними або незвичайними шаблонами, особливо якщо порівнювати їх із усталеною поведінкою криптовалютного гаманця, можуть бути признаком шахрайських операцій. Патерни можуть включати час транзакцій або характер учасників транзакцій. Наприклад, серія транзакцій, що відбуваються в надзвичайний час, для попередніх та транзакції між гаманцями, котрі не мали попередньої історії взаємодії, можуть свідчити про потенційні шахрайські дії.

Крім цього в майбутньому програмний модуль можна покращити імплементувавши новітні технології машинного навчання. Застосування прогнозних моделей у машинному навчанні може бути ефективним в області відслідковування потенційно шахрайських операцій в криптовалюті. Ці моделі навчаються на історичних даних транзакцій, що дозволяє їм отримувати та розпізнавати типові шаблони транзакцій і поведінку крипто гаманців. Після навчання ці моделі можуть передбачити ймовірність шахрайства транзакції на основі її характеристик. Порівнюючи аспекти з відомими моделями шахрайських транзакцій, модель може призначити оцінку ризику кожній транзакції, вказуючи на ймовірність того, що вона є шахрайською.

Методи виявлення аномалій у машинному навчанні також відіграють важливу роль. Ці методи призначені для виявлення транзакцій, які суттєво відрізняються від встановлених шаблонів. Технологія виявлення аномалій полягає в здатності модулі адаптуватися та ідентифікувати нові види операцій.

За допомогою таких методів, як кластерний аналіз, аналіз даних може виявити приховані шаблони та кореляції в даних транзакцій, які можуть бути не очевидними.

Інтеграція машинного навчання та аналізу даних у процес виявлення шахрайських операцій у блокчейні кардинально змінює ситуацію. Перераховані технології дозволяють ідентифікувати відомі моделі шахрайства та нададуть системі можливість навчатися та адаптуватися до нових їх типів, адже кіберзлочинність постійно розвивається.

Іншим важливим аспектом створення моделі моніторингу шахрайських операцій в блокчейні є впровадження автоматичних сповіщень. Програмний модуль, виявивши транзакцію, яка відповідає критеріям потенційного шахрайства, може автоматично ініціювати сповіщення для зацікавлених сторін. Дані сповіщення можна налаштувати, для представлення детальної інформації про транзакцію, що дозволяє швидко та обґрунтовано приймати рішення.

Дані показники можуть слугувати невід’ємною частиною аналізу, забезпечуючи кількісну основу для оцінки транзакцій. Встановлення порогових значень для суми операції і частоти допомагає систематично виявляти потенційно шахрайські наміри. Крім того, метрики мережевого аналізу, такі як дослідження зав’язків між сторонами транзакції, можуть надати більш глибоке розуміння. При комплексному застосуванні ці показники дозволяють системі моніторингу з більшою точністю розрізняти законні та потенційно шахрайські операції в блокчейнах.

Проте, важливо також зазначити, що перераховані тригери слід постійно вдосконалювати й оновлювати, щоб адаптуватися до мінливих моделей шахрайської діяльності для того щоб зменшити ймовірність помилкових спрацювань та мати актуальну систему моніторингу і протидії.

2.5 Висновки до другого розділу

У другому розділі, було проведено аналіз роботи криптовалютний операцій на прикладі одного з найпопулярніших блокчейнів сьогодення Ethereum. Розглянути математичні представлення роботи транзакцій та нарахування комісії за кожну операцію, також розглянуто вигляд розумного контракту та його місці, як програмі реалізованій в блокчейн інфраструктурі.

Було проведено аналіз проблематики відслідковування потенційно шахрайських транзакцій в криптовалюті. Не зважаючи на те, що блокчейн виступає відкритою книгою та кожен учасник криптовалютної мережі, має змогу переглянути історію всіх операцій, на даний момент існує незліченна кількість способів маскування свої дій задля уникнення ідентифікації. До прикладу було представлено та розглянути сервіси міксування, котрі дозволяє створити велику кількість транзакцій для маскування сліду надходження коштів та ускладнення їх легітимації. Також з ростом популярності криптовалюти, як однієї з варіацій проведення фінансових операцій та інвестування, виник попит на створення анонімних монет та блокчейнів, які не виступають відкритою книгою з доступом до історії операцій, проте навпаки маскують її та надають псевдо анонімність своїм користувачам. Гарним прикладом виступає блокчейн Monero, який не зважаючи на останні події на криптовалютному ринку, лише має приріст в кількості операцій та нових гаманців.

В розділі, було розглянуто існуючі моделі та методи ідентифікації та відслідковування потенційно шахрайських транзакцій, що є ключовими для забезпечення безпеки та прозорості в системі блокчейн. На основі проаналізованих аналогів, можна дійти до висновку, що кожен із перелічених сервісів має свої переваги та недоліки. Проте все ж доволі складно визначити, сервіс котрий би мав зрозумілий веб інтерфейс та надавав можливість проведення аналізу за короткий період часу.

Було проведено аналіз ключових критеріїв та метрик, необхідних для виявлення шахрайських операцій в рамках блокчейн транзакцій, що буде

використано при розробці програмного модуля моніторингу та ідентифікації потенційно шахрайських транзакцій на основі технології блокчейн.

РОЗДІЛ 3. РОЗРОБКА ПРОГРАМНОГО МОДУЛЯ ВИЯВЛЕННЯ ПІДОЗРІЛИХ НА ШАХРАЙСТВО ОПЕРАЦІЙ В БЛОКЧЕЙНІ ТА ЙОГО ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

3.1 Розробка програмного модуля виявлення підозрілих на шахрайство операцій в блокчейні та побудова інфраструктурного рішення

Вибираючи мову програмної реалізації модуля виявлення підозрілих на шахрайство транзакцій в блокчейні, було звернено увагу на адаптивність даної мови до різних задач, простота та ефективність у роботі з API запитами і можливість використання даної мови для автоматизації задач. Виходячи з поставлених задач, для програмної реалізації було обрану Python.

Python – це мова програмування, яка є одним із найкращих виборів, коли йдеться мова про створення програмного забезпечення, автоматизації завдань, аналізу даних та машинного навчання. Ця універсальність разом із зручністю у використанні зробили її однією з найпопулярніших та затребуваних мов сьогодення (рис. 3.1).

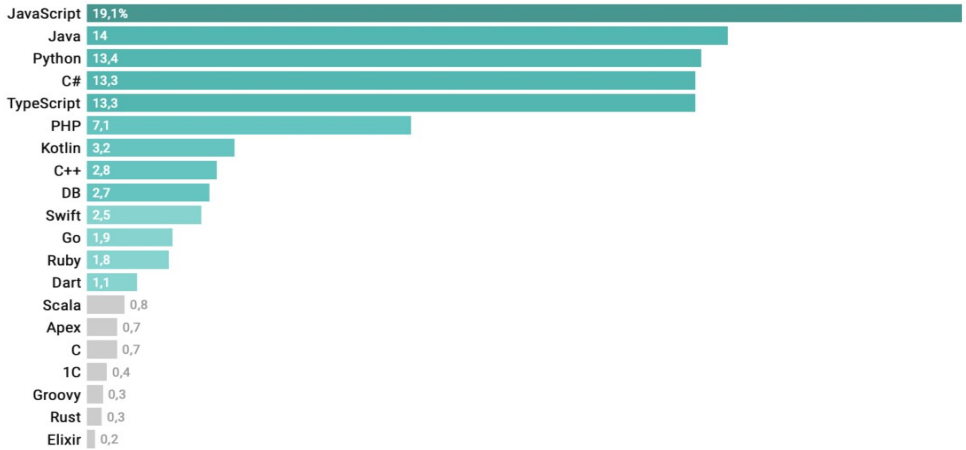

Рис. 3.1. Найбільш затребувані мови програмування 2023

Одні з найвідоміших компаній світового рівня сьогодення використовують Python для реалізації свого функціоналу, до прикладу Google використовує її для

перегляду сторінок, Spotify та Netflix для свого рекомендаційного алгоритму, який надає користувачам знаходити найкращі пропозиції побудовані на їх попередньо збудованим смакам.

Професіонали часто використовують Python для ефективного виконання різноманітних завдань у різних дисциплінах. Більш високої продуктивності можна досягти, серед іншого, за допомогою автоматизації [28]. Фінанси, страхування, маркетинг та навіть великі IT гіганти – усі ці сфери стикаються з проблемою автоматизації, де людям є необхідністю виконувати повторювані та виснажливі завдання. Замість виконання всіх цих рутинних задач кожного разу, працівник може реалізувати програмний компонент, задля спрощення та автоматизацій рутинної роботи, необхідністю є лише знаходження патерну по якому вона відбувається.

Базуючись на прийнятому рішенні стосовно мови програмної реалізації та бачені програми, було створено блок схемне представлення майбутньої програми (рис. 3.2):

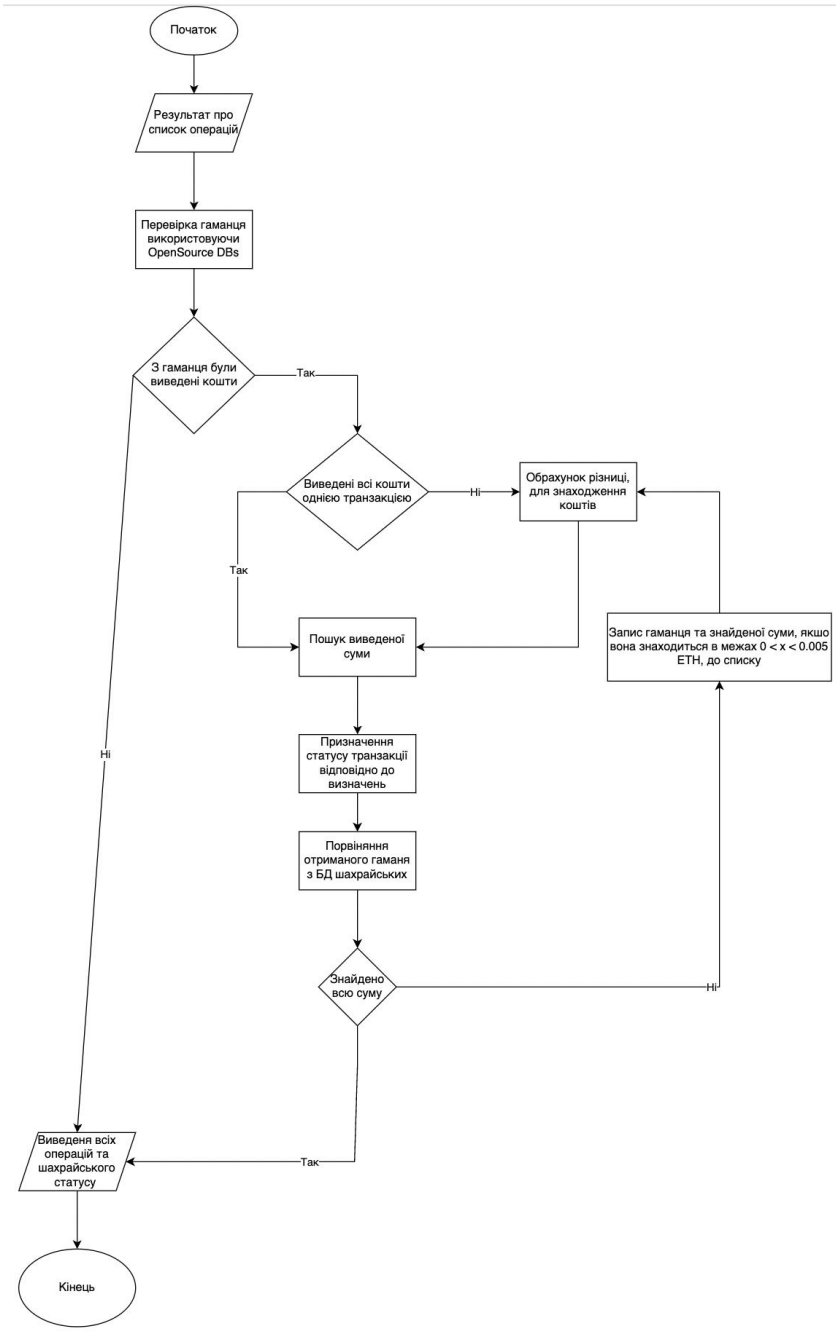

Рис. 3.2. Блок схема програмного модуля

У цій програмі початковий крок полягає в імпорті модуля requests, цей процес реалізується через використання команди import. Ця команда дозволяє інтегрувати модуль в програму, перетворюючи його назву на змінну, що надає доступ до різних функцій та атрибутів модуля.

Модуль requests використовується для здійснення HTTP запитів в мові програмування Python. Він забезпечує зворотний зв'язок у формі масиву, що містить всю інформацію відповіді, включаючи вміст, статус та інші дані.

У цьому дослідженні, за допомогою API та методу запиту GET, було здійснено підключення до Etherscan для збору даних про статус блокчейна, гаманців та транзакцій.

Для отримання власного ключа до API необхідно здійснити реєстрацію користувача на сервісі блокчейн дослідника Etherscan, безкоштовна версія API надає можливість відправляти до 5 запитів за секунду. Отримавши ключ, відбувається його підключення до програми, для безпечної передачі значення ключа було передано використовуючи AWS Secrets Manager, котрий зашифровує та зберігає облікові дані (рис. 3.3).

```python
## Використання Boto3 бібліотеки для отримання EtherscanAPI Key від AWS SecretsManager
def get_secret(secret_name):
    session = boto3.session.Session()
    client = session.client(service_name='secretsmanager')

    try:
        get_secret_value_response = client.get_secret_value(SecretId=secret_name)
    except Exception as e:
        print(f"Error retrieving secret: {e}")
        return None

    if 'SecretString' in get_secret_value_response:
        secret = get_secret_value_response['SecretString']
    else:
        secret = get_secret_value_response['SecretBinary']

    return secret

API_KEY_TOKEN = get_secret("/monitoring_phishing_operation/eth_api_key")
```

Рис. 3.3. Підключення Etherscan API до програми

Адреса початкового гаманця та першої транзакції береться з введення через інтерфейс програмного рядка. В майбутньому покращенням може бути інтеграція та реалізація веб інтерфейсу користувача, для покращення та залучення нових користувачів до даної програми.

```python
def main():
    account_address = input("Account address: ")
    transaction_hash_test = input("Interested TransactionID: ")
```

Рис. 3.4. Рядки для вводу адреси гаманця та хешу першої транзакції

За допомогою функції send_request відправляється API запит до кінцевої точки блокчейн дослідника Etherscan та форматується відповідь. В даному

випадку повернеою буде інформація про транзакції, їх суму та гаманці на які кошти були отримані (рис. 3.5).

```
def send_request(url_params):
    try:
        response = requests.get(BASE_URL + url_params, headers=HEADERS)
        response.raise_for_status()
        return response.json()['result']
    except requests.RequestException as e:
        print(f"Request error: {e}")
        return None
    except KeyError:
        print("Error parsing JSON response.")
        return None
```

Рис. 3.5. Реалізація функції send_request

Після отримання даних виконується функція get_all_transactions, яка отримує транзакції, запит на які відправився в попередньому фрагменті коду. Після цього, створюється масив з ними, а далі і видозміна результату відповідно до заданих параметрів (Рис. 3.6).

```
def get_all_transactions(address, start_time=0):
    params = f"?module=account&action=txlist&address={address}&startblock=0&endblock=99999999&sort=asc&apikey={API_KEY_TOKEN}"
    result = send_request(params)
    if result:
        return [tx for tx in result if int(tx["timeStamp"]) > start_time]
    return []
```

Рис. 3.6. Виконання функції get_all_transactions

Функції get_specific_trans_info та get_wallet_balance повертає інформацію про хеш отриманої транзакції. Далі виконується цикл, який перевіряє кожну та нумерує їх за допомогою ітератора enumerate (рис. 3.7).

```
def get_specific_trans_info(transactions, transaction_hash):
    return next((tx for tx in transactions if tx['hash'] == transaction_hash), None)

def get_wallet_balance(address):
    params = f"?module=account&action=balance&address={address}&tag=latest&apikey={API_KEY_TOKEN}"
    result = send_request(params)
    return int(result) if result else None
```

Рис. 3.7. Функція get_specific_trans_info

Функція track_transaction_chain знаходить транзакції та гаманці з отриманими коштами, до останнього отримувача. Спочатку визначається, який

баланс рахунку був на момент останньої транзакції та визначається сума переведених коштів.

Також, в даній функції реалізований функціонал та визначення пріорітетності повідомлень (рис. 3.8), котрі будуть помічати старі та нові операції проведені з даного гаманця відповідно до визначених у другому розділі умов:

- якщо транзакція була надіслана з більшою сумою ніж зазвичай;
- якщо було помічено більше ніж 3 операцій в мережі від початкової;
- збільшена кількість активності по операціям з гаманця ніж зазвичай;
- сума активів на балансі стала нульовою після останньої операції
- повторювані операції з однаковою кількість криптовалютних активів, проте на різні адреси.

```python
def track_transaction_chain(transactions, stolen_amount):
    thief_wallets = {}
    wallet_chain_length = 0
    amount_frequencies = {}
    time_stamps = []

    for tx in transactions:
        value = int(tx['value'])
        if value >= stolen_amount:
            thief_wallets[tx["to"]] = value
            wallet_chain_length += 1
            amount_frequencies[value] = amount_frequencies.get(value, 0) + 1
            time_stamps.append(int(tx["timeStamp"]))

    triggers = []
    if any(value > ETH_THRESHOLD for value in thief_wallets.values()):
        triggers.append("P1: Transaction amount exceeded the threshold")
    if wallet_chain_length > 3:
        triggers.append("P2: Possible mixing services")
    if len(time_stamps) >= FREQUENCY_THRESHOLD and max(time_stamps) - min(time_stamps) < 3600:
        triggers.append("P3: High frequency of transactions within a short time frame")
    if any(count >= SAME_AMOUNT_THRESHOLD for count in amount_frequencies.values()):
        triggers.append("P2: Repeated transactions of the same amount to different addresses")
    for tx in transactions:
        if get_wallet_balance(tx["to"]) == 0:
            triggers.append("P3: Wallet's balance dropped to zero after transaction")
            break

    return thief_wallets, triggers
```

Рис. 3.8. Функція визначення порогових значень та пріорітетності

Дані порогові значення були налаштовані на початку запуску програми, та передані як закодовані значення (рис. 3.9), проте їх можна змінити відповідно до потреб користувача та для того щоб система сповіщення була точнішою.

```
ETH_THRESHOLD = 2 * 10**18  # 2 ETH в Wei
FREQUENCY_THRESHOLD = 10  # Кількість операцій
SAME_AMOUNT_THRESHOLD = 3  # Кількість одинакових транзакцій підряд
```

Рис. 3.9. Закодовані порогові значення в моніторинговій системі

Також потрібно зазначити, що гаманці котрі були проаналізовані відповідно до баз даних, також мають свою пріоритетність. Було визначено, що якщо адресу гаманця було помічено в одній з БД повідомленню назначається найвища серйозні або ж пріоритет, для подальшого перегляду та поглибленого аналізу (рис. 3.10).

```
for address, balance in thief_wallets.items():
    print(f"Address: {address}, Balance: {balance / 10**18} ETH")
    check_wallet_security(address)

    for site, wallets in phishing_data.items():
        if address in wallets:
            print(f"P0: Wallet address {address} is found in IllegalActivityDB, as {site}")
            wallet_found_in_phishing_db = True

    if address in ofac_data:
        print(f"P0: Wallet address {address} is found in OFAC Sanction DB")
        wallet_found_in_ofac_db = True

if account_address in ofac_data:
    print(f"P0: Initial account address {account_address} is found in OFAC Sanction DB")
for site, wallets in phishing_data.items():
    if account_address in wallets:
        print(f"P0: Initial account address {account_address} is found in IllegalActivityDB, as {site}")
check_wallet_security(account_address)
```

Рис. 3.10. Визначення пріорітетності для гаманців ідентифікованих як зловмисні

В програмний модуль було інтегровано зв’язок з програмним забезпеченням з відкритим початковим кодом GoPlusLabs. Дана інтеграція, надає змогу отримувати інформацію про стан гаманця та чи був він зафіксований в протиправних діях. Також дане ПЗ, ідентифікує види злочинної діяльності, в яких було помічено надану адресу криптовалютного гаманця (рис. 3.11).

```python
def check_wallet_security(address):
    response = Address(access_token=None).address_security(address=address)

    try:
        data = response.to_dict()
    except AttributeError:
        print("Cannot convert response to dictionary.")
        return

    if data['code'] == 1:
        result = data.get('result', {})
        flagged_issues = [key for key, value in result.items() if value == "1"]

        if flagged_issues:
            print(f"P0: Wallet {address} is flagged in 'data_source': {result.get('data_source', 'Unknown')}")
            for issue in flagged_issues:
                print(f"    Flagged Issue: {issue}")
```

Рис. 3.11. Використання GoPlusLabs ПЗ

Потрібно зазначити, що до об’єкта ResponseWrapperAddressContract, який повертає GoPlusLabs, неможливо отримати доступ, як до стандартного словника Python. Саме тому у даній функції ми перетворюємо об’єкт відповіді від ПЗ у словник.

Також для забезпечення максимальної точності та обширності результатів, було імплементовано інтеграції такими сервісами, як санкційний лист Управління контролю за іноземними активами, котрий повертає список криптовалютних адрес, які знаходяться під санкціями і адрес, що використовувались для відмивання коштів та відритою базою даних від ScamSniffer котра містить інформацію про злочинні крипто-проєкти.

Для їх інтеграції необхідно написати реалізувати додатковий програмний компонент, який виконуватиме обробку даних та їх збереження у зрозумілому форматі. В якості рішення для зберігання даних було обрано сервіс AWS DynamoDB, оскільки він дозволяє зберігати результати у форматі json.

AWS Lambda функції було використано для запиту даних з кінцевих точок, їх подальша обробка, відправлення та зберігання в AWS DynamoDB. Цей вибір зумовлений кількома причинами: по-перше, AWS Lambda дозволяє автоматично масштабувати обробку відповідно до потреб, по-друге, вона інтегрується з AWS DynamoDB, забезпечуючи ефективний обмін даними. Крім того, Lambda є

вартісно-ефективним рішенням, оскільки користувачі платять лише за час виконання коду, що знижує витрати на інфраструктуру.

Для отримання даних з AWS DynamoDB таблиць, для подальшої обробки та використання в програмному модулі була використана бібліотека boto3, котра надає змогу зручно налаштовувати запити до таблиць в сервісі (рис. 3.12).

```
def get_ofac_wallets_list():
    dynamodb = boto3.resource('dynamodb')

    table = dynamodb.Table('ofac_eth_list')

    try:
        response = table.get_item(Key={'source': 'ofac_eth'})
    except Exception as e:
        print(f"Error accessing DynamoDB: {e}")
        return []

    return response.get('Item', {}).get('wallets_list', [])

def get_illegal_ops_wallets_list():
    dynamodb = boto3.resource('dynamodb')

    table = dynamodb.Table('wallets_illegal_ops_open_source')

    try:
        response = table.get_item(Key={'source': 'wallets_illegal_ops'})
    except Exception as e:
        print(f"Error accessing DynamoDB: {e}")
        return {}

    return response.get('Item', {}).get('project_list', {})
```

Рис. 3.12. Отримання даних з таблиць AWS DynamoDB

В програмний модуль, також було імплментовано режим моніторингу, в якому ми надсилаємо запити до Etherscan API, на нові транзакції від отриманих в ході виконання програми гаманців. На даний момент, було запрограмовано відправляти лише один запит в хвилину, для того щоб не навантажувати мережу, проте дане значення можна з легкістю під корегувати для адаптації під потреби користувача (рис. 3.13).

```python
def ask_to_continue():
    response = input("Do you want to continue monitoring the wallet? Enter Yes/No (Y/N): ").lower()
    return response in ['yes', 'y']

def monitor_wallet(account_address, last_check_timestamp):
    print("Program in the monitoring mode, waiting for the new transactions in the wallet.....")
    time.sleep(3600)
    print("Checking for new transactions...")
    new_transactions = get_all_transactions(account_address, last_check_timestamp)
    if new_transactions:
        print("\nNew transactions found:")
        for tx in new_transactions:
            print(f"Transaction Hash: {tx['hash']}, Value: {int(tx['value']) / 10**18} ETH")
    else:
        print("No new transactions found.")
    return int(time.time())
```

Рис. 3.13. Імплементація режиму моніторингу

Також, для кращого досвіду майбутніх користувачів було продумано та реалізовано інфраструктурне рішення на базі хмарного провайдеру AWS (рис. 3.14). Програма буде запакована Docker образ для подальшого перенесення в AWS ECR сервіс котрий надає змогу зберігати образи застосунків в приватних та публічних репозиторіях.

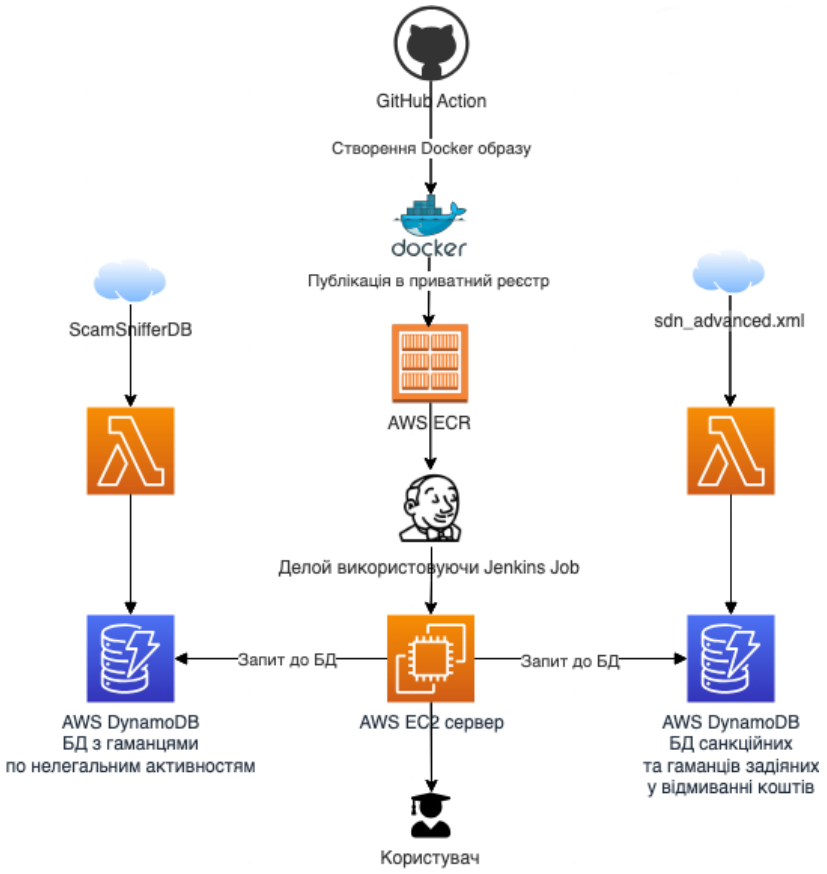

Рис. 3.14. Блок схема інфраструктурного рішення

Для автоматизації процесу будування та відправки Docker образу до AWS ECR сервісу найкращим рішенням, на мою думку, є використання GitHub Action, правильна побудова команд дадуть змогу автоматично відправляти побудований образ до сервісу зберігання за лічені хвилини, без необхідності ручного втручання.

Наступним кроком є налаштування та реліз програмного модуля на серверній інфраструктурі, це може бути виконано за допомогою Jenkins сервісу, котрий автоматично при зберіганні нової версії в AWS ECR нашого застосунку буде розгортати її на сервері EC2.

Також, важливим кроком є отримання та правильне опрацювання інформації з джерел даних. Для цього було імплементовано AWS Lambda функцію, котра з мінімальним часом обробки матиме змогу автоматично оновлювати та обробляти результати з відкритих джерел та імплементовувати їх в AWS DynamoDB сервіс, котрий слугує не реляційною базою даних та надає змогу отримувати представлення таблиць у вигляді json.

Описаний програмний модуль для моніторингу та ідентифікації підозрілих на шахрайство транзакцій в блокчейні необхідно піддати тестуванню, що буде зроблену у наступному підрозділі.

3.2 Експериментальне дослідження розробленого програмного методу

Перед тим як розпочати експериментальне дослідження, потрібно було здійснити створення криптовалютного гаманця. У рамках цього тесту було обрано MetaMask. MetaMask представляє собою криптовалютний гаманець з відкритим кодом, який активно використовується як розробниками, так і звичайними користувачами криптовалют.

Особливістю цього гаманця є його використання в якості браузерного розширення, що дозволяє легко інтегруватися з різними веб-сайтами. У порівнянні з іншими аналогами, де користувачам необхідно сканувати QR-код з мобільного телефону або вводити адресу гаманця в спеціальне поле, розширення MetaMask дозволяє веб-сайтам автоматично відправляти запити до гаманця, який вже відкритий у браузері. Таким чином, користувачеві пропонується прийняти або відхилити запит на здійснення транзакції або підключення до смарт-контракту (рис. 3.15).

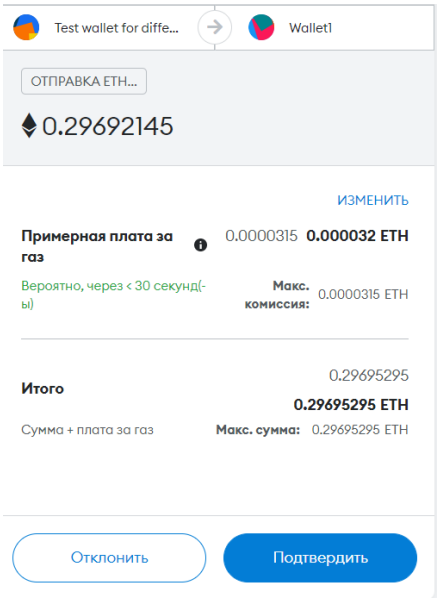

Рис. 3.15. Приклад підтвердження операції

Також для проведення експериментального дослідження програмного модуля необхідно використовувати блокчейн дослідник Etherscan оскільки він допоможе нам вручну перевірити правильність виконання програми.

Як було зазначено в попередньому розділі, програма використовує кілька джерел даних, включно з деякими власними рішеннями по ідентифікації криптовалютного гаманця чи транзакції на підозрілі шахрайські дії.

Для проведення першого тестування, було використано сервіс Scam Alert оскільки він надає у відкритому доступі список найактивніших гаманців зловмисників, які були категоризовані відповідно до їх шахрайських дій (рис. 3.16).

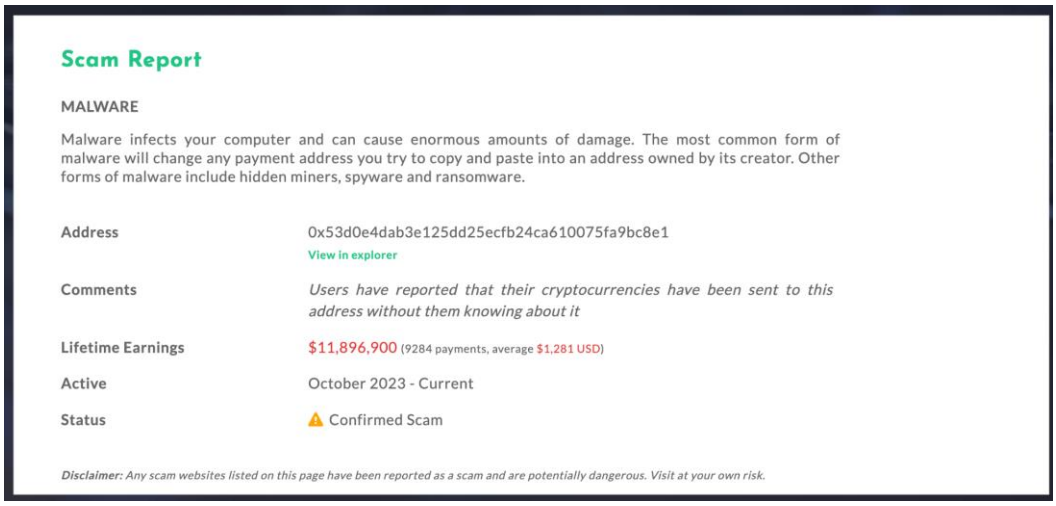

Рис. 3.16. Приклад адреси криптовалютного гаманця зловмисника

Для проведення наступних дій за допомогою блокчейн дослідника Etherscan, було знайдено транзакцію по надсиланню коштів до даного гаманця, та вставлено у програмний модуль разом з самою адресою зазначеною в документі від Scam Alert сервісу (рис. 3.17).

```
[root@m-sudnitsyn Diploma # python3 monitoring_phishing_operation.py
Account address: 0xce5445314fc86584Fd75645211e62C962763F19E
Interested TransactionID: 0xab5f72710df2e23e641eb6f44021a52209fa44b859ff403966bb611726646dea
Tracking fraudulent transactions...

Wallets with stolen money:
Address: 0xce5445314fc86584fd75645211e62c962763f19e, Balance: 385.0 ETH
Address: 0x53d0e4dab3e125dd25ecfb24ca610075fa9bc8e1, Balance: 384.9993745111714 ETH
P0: Wallet 0x53d0e4dab3e125dd25ecfb24ca610075fa9bc8e1 is flagged in 'data_source': SlowMist
    Flagged Issue: phishing_activities
Do you want to continue monitoring the wallet? Enter Yes/No (Y/N): no

Notifications:
P1: Transaction amount exceeded the threshold
INFO: No wallets are found in the IllegalActivityDB.
INFO: No wallets are found in the OFAC Sanction DB.
```

Рис. 3.17. Приклад виконання програмного модулю

Як можна побачити з результату виконання даної програми, було знайдено адресу в базі даних , та визначено відповідний статус, оскільки вона зафіксована в шахрайських операціях.

Також з відповіді програми ми бачимо, які саме тригери були присвоєні даній операції, а саме дані адреси не було знайдено в базі даних нелегальних активностей та в базі даних Управління контролю за іноземними активами.

Проте варто зазначити, що була присвоєна перша пріоритетність даній операції, оскільки сума виведеної транзакції перевищує визначену в програмі порохову для моніторинга – 2 ETH.

Наступним кроком для перевірки коректності програмного модулю по моніторингу є ідентифікація адрес котрі могли б бути зафіксовані в базі даних нелегальних активностей. Як вже було зазначено, адреси гаманців з якої надаються через повідомлення користувачів крипто мережі та ретельно піддаються аналізу іншими користувачами та розробниками відкритого проєкту Scam Sniffer перш ніж потрапити в офіційну версію.

Також варто зазначити, що дане джерело інформації містить також й адреси розумних контрактів, котрі були помічені за злочинними операціями та містили шкідливий код.

Для даної перевірки було знайдено адресу гаманця котра була зафіксована, як основна в більше ніж 30 злочинних операціях з криптовалютними активами (рис. 3.18).

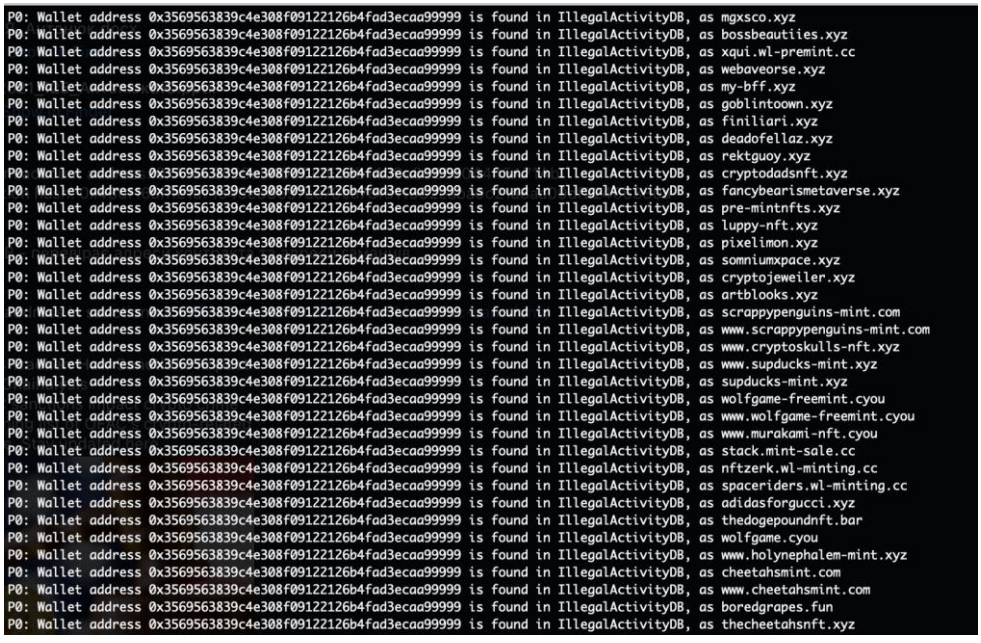

Рис. 3.18. Список криптовалтних зловмисник проєктів, в яких визначена адреса є основною

Як можемо бачити з виконання програмного модуля, було успішно ідентифіковано криптовалютну адресу, котра була задіяна в злочинних діях та визначено проєкти в котрих вона була основною для проведення операцій.

Для перевірки наступного кроку виконання програмного модуля, було обрано спробу ідентифікації сервісів міксування, котрі можуть використовуватись зловмисниками, для протиправних дій та відмивання коштів (рис. 3.19).

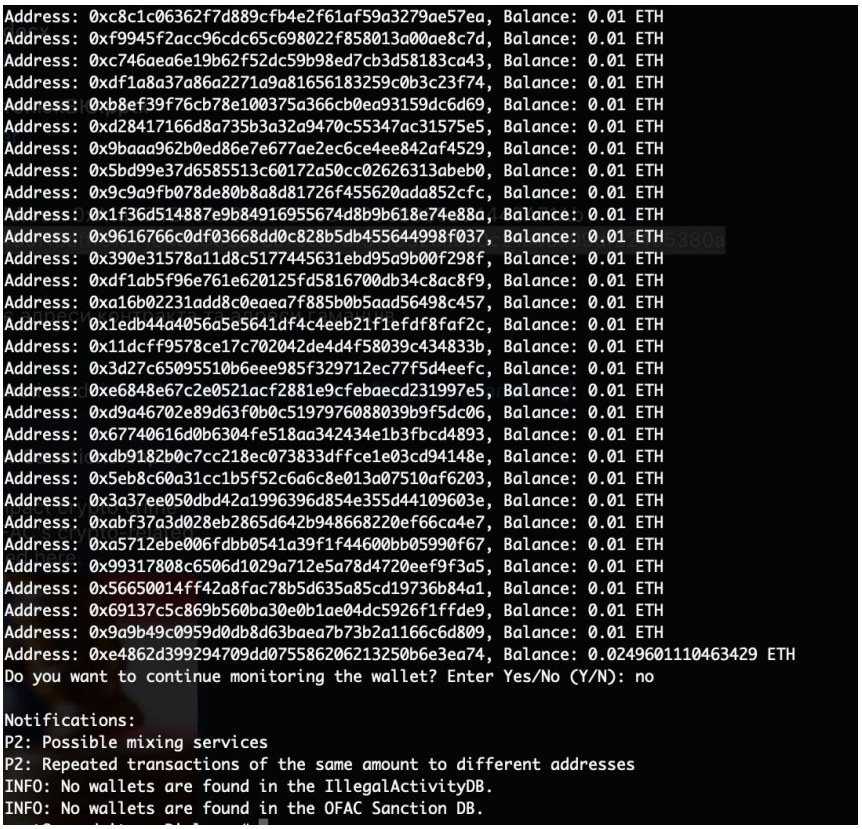

Рис. 3.19. Виявлення сервісів міксування криптовалюти

Відповідно до отриманих результатів, можна прийти до висновку, що програмний модуль успішно справляється з ідентифікацією сервісів міксування та назначає даним операціям визначену пріоритетність для подальшого розгляду. Крім того, варто зазначити, що під час перевірки даного гаманця та транзакції, серед гаманців одноденок, було виявлено одну з адрес котра ідентифікована базою даних SlowMist, як така котра проводить шахрайські операції (рис. 3.20).

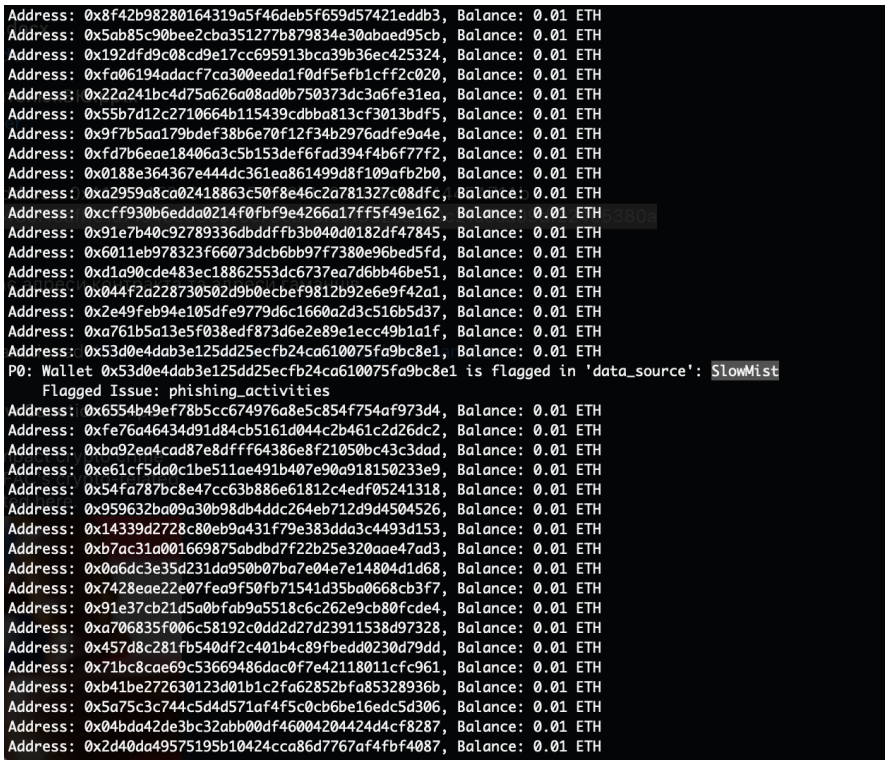

Рис. 3.20. Ідентифікація шахрайської адреси

Рахую важливим також удостовіритись в правильності ідентифікації адрес котрі були зафіксовані Управлінням контролю за іноземними активами, як криптовалютні гаманці, що використовувались в операціях по відмиванню коштів або додані до санкційного списку. Для перевірки таких, було знайдено останній xml звід установи котрий містить адреси ETH криптовалюних гаманців та запущено програму з однією з них для перевірки (рис. 3.21).

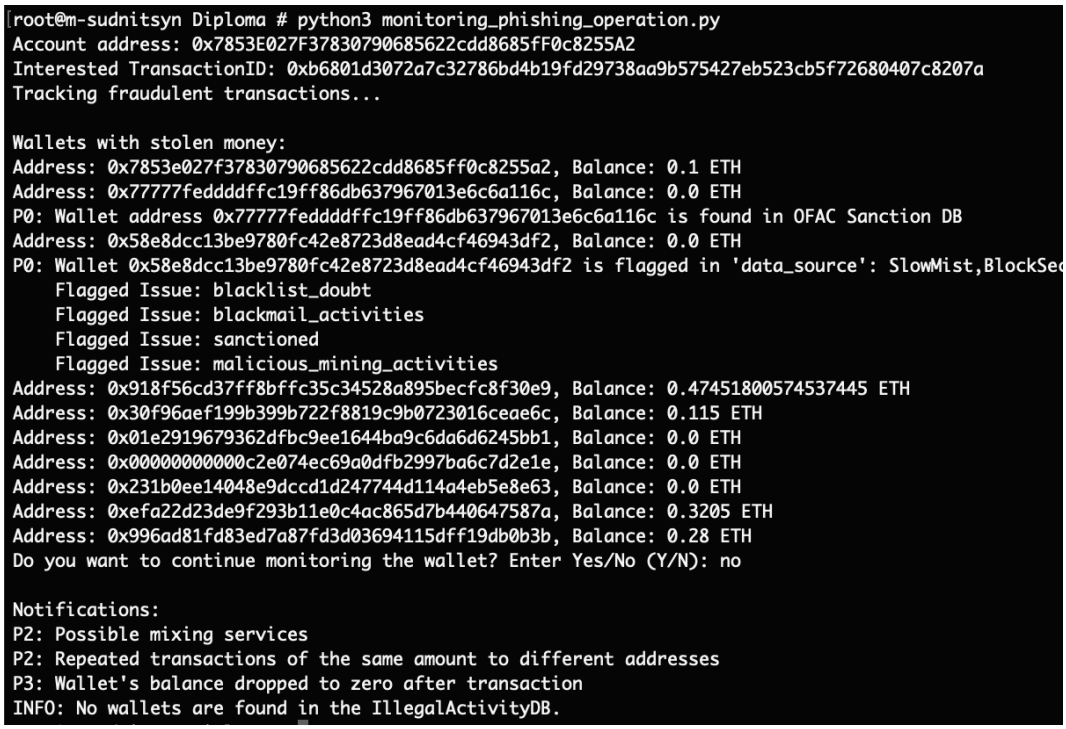

Рис. 3.21. Ідентифікація гаманця, який використовувався в операціях по відмиванню коштів або знаходиться під санкціями

З результатів виконання програми ми можемо побачити, що гаманець було успішно ідентифіковано, як такий, що використовувався в злочинних операціях по відмиванню коштів. Також один із гаманців в ланцюзі було ідентифіковано багатьма джерелами, як такий, що використовувався в операціях з шантажу та розповсюдження шкідливого програмного забезпечення, в даному випадку майнінгового ПЗ.

3.4 Висновки до третього розділу

У даному розділі ми розглянули ключові аспекти розробки програмного модуля для виявлення підозрілих операцій в блокчейні. Значна увага була приділена створенню ефективної та надійної системи, що включає в себе аналіз на реалізацію тригерів котрі могли б ідентифікувати та повідомити про

потенційно шахрайські операції або гаманець котрий вже був ідентифікований як такий раніше.

Інтеграція ключових критеріїв і показників у програмний модуль для моніторингу транзакцій в блокчейні є значним прогресом у сфері виявлення шахрайства. Ця імплементація дозволяє не тільки аналізувати транзакції в режимі реального часу, але й гарантує швидке та ефективне реагування на потенційну шахрайство забезпечуючи при цьому високий рівень безпеки та прозорості в блокчейн-мережах.

Далі, у розділі було представлено експериментальне дослідження розробленого програмного методу, фрагмент вихідного коду якого, надано у додатку А. В ході якого було продемонстровано, що розроблена система ефективно виявляє підозрілі транзакції, при цьому мінімізуючи помилкові позитивні сигнали. Експериментальні результати підтверджують високу точність та надійність методу, що робить його корисним інструментом у боротьбі з фінансовими шахрайствами в блокчейні.

Отже, враховуючи результати роботи програмного модуля моніторингу потенційно шахрайських операцій, можна зробити висновок, що програмний модуль функціонує і здатний знаходити та ідентифіковувати такі транзакції та гаманці користувачів.

РОЗДІЛ 4. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

4.1 Екологічна культура

Людське існування тісно пов'язане зі станом довкілля, і зростаюча загроза самознищення через нераціональне використання природних ресурсів вимагає термінового переосмислення відносин людини з природою. Розвиток екологічної культури, яка є фактично кодексом поведінки для екологічної діяльності та ставлення до природи, є ключовим елементом у вирішенні цієї проблеми.

В Україні особливу увагу приділяють формуванню екологічної культури, яка включає в себе знання, цінності, навички, поведінку та світогляд, спрямовані на гармонійне співіснування людини з природним середовищем. Вона охоплює різноманітні аспекти людської діяльності, від особистої відповідальності та етики до колективних зусиль у сфері охорони довкілля та сталого розвитку. Екологічна культура не лише визначає спосіб, яким суспільство взаємодіє з природним середовищем, але й впливає на прийняття рішень у сфері екології на різних рівнях.

Розвиток екологічної культури як цілісної системи починається з давніх часів, коли люди вперше усвідомили необхідність бережливого ставлення до природи для власного виживання. Історично це поняття зазнало значних змін, від традиційних світоглядів, заснованих на повазі до природи у різних культурах, до сучасного розуміння екологічної кризи та необхідності глобальної екологічної відповідальності [57].

В різні епохи існували різні підходи до взаємодії з природою, які формували фундамент для сучасної екологічної культури. Зокрема, у XX столітті відбулося значне зростання усвідомлення екологічних проблем, що призвело до розвитку різноманітних екологічних рухів та ініціатив. Серед ключових

проблем, які вплинули на глобальну екологічну свідомість, можна виділити наступні [57]:

- Індустріалізація та зростання міських агломерацій призвели до значного збільшення забруднення повітря, води та ґрунту;
- Інтенсивне використання природних ресурсів, включаючи ліси, мінеральні ресурси, корисні копалини, призвело до їх значного виснаження;
- Руйнування природних середовищ існування, неконтрольоване полювання, розорювання лісів та інші антропогенні фактори призвели до масового вимирання видів, що ставить під загрозу екологічну рівновагу;
- Викиди парникових газів від фосильних палив та інших джерел значно підвищили глобальну середню температуру, призводячи до зміни клімату з усіма його негативними наслідками, включаючи підвищення рівня моря, екстремальні погодні умови та вплив на сільське господарство.

У відповідь на ці виклики з'явилися різноманітні екологічні ініціативи та рухи, серед яких можна виділити найголовніші:

- Створення природоохоронних організацій;
- Значні зусилля були спрямовані на розвиток міжнародного екологічного права, укладення угод та проведення конференцій, таких як Ріо-92, Кіотський протокол, Паризька угода по клімату, які встановлюють глобальні рамки для охорони довкілля;
- Процвітання та створення нових освітніх програм та популяризація просвітницької діяльності діяльність;
- Створення громадських організацій, що відіграє ключову роль у підвищенні, адже вони діють як міст між громадськістю, урядами та приватним сектором;
- Екологічні ініціативи та проекти також є важливою частиною практичних зусиль щодо підвищення екологічної культури. Ці

проекти можуть включати локальні, національні та міжнародні ініціативи, наприклад, програми з переробки відходів, збереження водних ресурсів, посадка дерев та створення зелених зон у міських просторах.

Сьогодні екологічна культура є важливим елементом у боротьбі з екологічними викликами, такими як зміна клімату, втрата біорізноманіття, забруднення та виснаження природних ресурсів. Вона включає не тільки знання про екологічні проблеми, але й активне залучення громадськості до процесу їх вирішення через освіту, просвітницьку діяльність та участь у різноманітних екологічних проектах. Основою екологічної культури є розуміння того, що здоров'я людини тісно пов'язане зі станом навколишнього середовища, а також усвідомлення того, що кожна дія чи бездіяльність індивіда може мати далекосяжні екологічні наслідки.

Ефективне використання екологічних культурних практик можна спостерігати у багатьох аспектах сучасного життя. Наприклад, збільшення популярності використання відновлюваних джерел енергії, таких як сонячні панелі та вітряки, значно зменшує залежність від викопного палива та вплив на зміну клімату. Іншим прикладом є розвиток концепцій зеленого будівництва та енергоефективності у міському плануванні, що сприяє зниженню вуглецевого сліду міст.

Проте, існують також проблеми та виклики, які пов'язані з екологічною культурою. Однією з основних проблем є недостатня обізнаність та залученість широкої громадськості. Незважаючи на зростаючу увагу до екологічних питань, все ще багато людей не мають достатньої інформації або не розуміють повної серйозності екологічних викликів. Це може призводити до недостатньої підтримки екологічних ініціатив або небажання змінювати особисті звички та спосіб життя. Відповідно до соціологічного опитування в близько 72% студентської молоді рівень екологічної культури насправді є низьким. Це небезпечна тенденція, адже складна екологічна ситуація сьогодення вимагає висококваліфікованих фахівців з належним рівнем екологічної культури не лише

в галузі екологічної безпеки, а й в інших, де працівники мають вміти будувати свою діяльність відповідно до засад екологічної культури.

Сьогоднішнє молоде покоління стикається з ерою, яка включає не тільки стрімкий прогрес науки та технологій, але й включає в себе наслідки науково-технічного прориву та демографічного сплеску. Підвищення рівня забруднення повітря, води та землі, а також накопичення величезної кількості відходів від людської активності, паралельно з виснаженням більшості природних ресурсів, спричинили екологічну кризу. Також на жаль потрібно зазначити [56].

4.2 Висновки до четвертого розділу

У даному розділі ми розглянули теперішній стан екологічної культури в Україні та світі, а також і важливість зародження та розповсюдження її серед молоді та учасників спільнот.

Важливо зазначити, що хоч і були здійснені значні зусилля у сфері освіти та законодавства, все ще існує простір для покращення та поширення екологічної культури. Програми освіти та просвітництва мають бути більш інтегрованими та орієнтованими на практичне застосування знань. Також, необхідно постійне покращення законодавства України, зокрема щодо контролю викидів і їх утилізації та інших екологічних проблем.

Необхідністю, є також залучення молоді через інноваційні освітні підходи, використання цифрових технологій та соціальних медіа, що може значно підвищити інтерес та участь у екологічних ініціативах. Залучення приватного сектору до екологічних ініціатив, через стимулювання зеленого бізнесу та інвестицій у сталий розвиток, є ще одним важливим аспектом. Це може включати податкові пільги для компаній, які впроваджують екологічно сталі практики, а також розвиток ринків екологічних товарів та послуг.

ВИСНОВКИ

У даній роботі було проаналізовано принцип роботи блокчейну та створення блоку, які є його складовими. Кожен блок в блокчейні складається із серії транзакцій. Кожна транзакція публікується у вигляді хеш-значення, а потім усі хеш-значення поєднуються в блок. Заголовок блоку містить власний хеш та хеш попереднього блоку, що робить їх пов’язаними між собою та сам блокчейн неможливим до змін будь якої із його частин.

Також, було представлено аналіз переваг та недоліків криптовалюти. Хоч і можна сказати, що недоліків використання на даний момент більше, це не зупиняє ентузіастів від використання криптовалюти та блокчейну та заохоченню з кожним днем все більшої кількості людей до свого кола.

Проведено аналіз правового регулювання криптовалютних активів в Україні та закордоном. Хоч і світова спільнота поки не дійшла до уніфікованого правового регулювання використання блокчейну, ця технологія вже активно використовується у державному секторі деяких країн. Україна також не відходить від світових тенденцій, та активно намагається запровадити нормативно правові акти по регулюванню використання блокчейну та обігу криптовалютних активів. Нещодавно Верховна Рада України створила проєкт закону про оподаткування доходу від криптовалюти та операцій з нею, що можна вважати великим кроком на зустріч легалізації криптовалютних активів та використання технології блокчейн в Україні.

Після детального вивчення теорії щодо правового регулювання, можна прийти до висновку, що часто саме його відсутність робить сферу криптовалют вразливою перед шахрайством та протиправними діями. Це спонукало до створення програмного рішення для моніторингу блокчейн-транзакцій, яке може допомогти в виявленні та протидії легалізації незаконних дій з допомогою криптовалютних активів.

Важливим аспектом імплементації програмного модуля моніторингу підозрілих на шахрайство транзакцій стало визначення ключових метрик, по

яким можна трактувати та призначати операції даний статус. Саме тому було розроблено список пріоритетності, відповідно до різних критеріїв, таких як, сума коштів надісланих в останній операції, знаходження адреси криптовалютних гаманців в базах даних по нелегальним операціям та інші. Звернувши увагу саме на критичність отриманого повідомлення, користувач зможе прийняти зважене рішення по ідентифікації шахрайських операцій в блокчейні.

Експериментальна перевірка розробленого програмного рішення підтвердила адекватність його роботи. Тестування продемонструвало, що програма відповідає всім вимогам. Також було доведено, що вона адекватно реагує на поставлені завдання і функціонує без збоїв. Це підтверджує належну ефективність програмного засобу для виявлення транзакцій що мають на меті протиправні дії у блокчейні, забезпечуючи високу якість і достовірність результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Свон М. Блокчейн. Схема нової економіки // (онлайн): https://booksonline.com.ua/view.php?book=183306
2. Проект Закону Про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами (№ 7150 від 13.03.2022) // (онлайн): https://itd.rada.gov.ua/billInfo/Bills/Card/39211
3. Світлана Заражевська, Криптозима прийшла й до України. Ринок скорочує видатки та донати і чекає на банкрутства спекулянтів. Хто постраждає найбільше // (онлайн): https://forbes.ua/inside/kriptozima-priyshla-y-do-ukraini-ukrainski-skorochuyut-vidatki-ta-donati-i-chekayut-na-bankrutstva-spekulyantiv-khto-postrazhdae-naybilshe-16062022-6616
4. Рішення Щодо виконання вимог деяких рішень Національної комісії з цінних паперів та фондового ринку у зв'язку з введенням воєнного стану // (онлайн): https://ips.ligazakon.net/document/KL220399
5. Батракова Т.І. Проблеми та перспективи розвитку електронних грошей в Україні / Т.І. Батракова, А.Ю. Грінченко // Мукачівський державний університет. 2016. – № 7. // (онлайн): http://www.economyandsociety.in.ua/journal
6. Сінищ П.М. Світовий досвід та перспективи розвитку електронних грошей в Україні / Національний банк України. Дослідницький центр – 2008 // (онлайн): https://www.bank.gov.ua/doccatalog/document
7. Chaum D. Blind signature for untraceable / D. Chaum, A.T. Sherman, R.L. Ronald // (онлайн): https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18
8. Директива 2009/110/ЄС Європейського парламенту та Ради про діяльність установ, що випускають електронні гроші, та пруденційний нагляд за ними // (онлайн): http://zakon3.rada.gov.ua/laws/show / 994_a18
9. Шишкова Н.Л. Електронні гроші: сутність та проблеми використання в Україні / Н.Л. Шишкова, Є.Ю. Мороз // Національний гірничий

університет. – 2017. // (онлайн): http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/evngu_2017_4_7.pdf

10. Постанова НБУ від 04.11.2010 № 481 «Положення про електронні гроші в Україні» // (онлайн): http://zakon2.rada.gov.ua/laws/show/z1336-10
11. Serhii Hrytsai. Cryptocurrency In The Declarations Of Government Officials: A Toolkit For Money Laundering (Trends And Experience Of Counteraction, By The Example Of Ukraine) // (онлайн): https://ajee-journal.com/upload/attaches/att_1690878898.pdf
12. Закон України від 17.02.2022 № 2074-IX "Про віртуальні активи" // (онлайн): https://zakon.rada.gov.ua/laws/show/2074-20
13. Електронні гроші: що, де, як // (онлайн): http://www.prostobank.ua/internetbanking/stat
14. Ярош В.І. Електронні гроші: переваги та недоліки / В. І. Ярош, Ю. А. Романовська // "Young Scientist" – №5 (45) – 2017 // (онлайн): http://www.irbisnbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/molv_2017_5_178.pdf
15. Що таке Etherscan та як його використовувати? // (онлайн): https://academy.binance.com/uk/articles/what-is-etherscan-and-how-to-use-it
16. Чумаченко О. Г. Передумови виникнення криптовалюти / О. Г. Чумаченко, Л. О. Баластрик // Міжнародна науково-практична конференція "Нові форми грошей та фінансових активів: становлення, перспективи, ризики" – 2017 // (онлайн): http://npndfi.org.ua/docs/NP_17_04_096_uk.pdf
17. Лук'янов В. С. Зародження ринку криптовалюти в інформаційно-мережевій парадигмі / В. С. Лук'янов // Актуальні проблеми економіки. – 2014. – № 8 (158). – С. 436-441.

18. Tapscott A. Технологія блокчейн – те що рухає фінансовою революцією сьогодні // Alex Tapscott, Don Tapscott / Переклад з англійської. К. Шашкова, Є. Ряхіна – 2017. – 448с.
19. Сатоші Накамото Біткоїн: однорангова електронна готівкова система // (онлайн): https://bitcoin.org/bitcoin.pdf
20. Zheng Z. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends / Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang // 2017 IEEE International Congress on Big Data 557–564 p.
21. Бутерін В. Представлення Ripple. Журнал Біткоїн // (онлайн): https://bitcoinmagazine.com/3506/introduction-ripple/
22. Duivestein S. Bitcoin: It's the platform, not the currency! / S. Duivestein, P. Savalle // (онлайн): http://thenextweb.com/insider/2014/02/15/bitcoin-platform-currency/1/
23. Wood G. Ethereum: A secure decentralized generalized Transaction Ledger EIP-150 Revision // (онлайн): https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf
24. Herbert J. A Novel Method for Decentralized Peer-to-Peer Software License Validation Using Cryptocurrency Blockchain Technology / J. Herbert, A. Litchfield // (онлайн): https://www.researchgate.net/publication/283655502_A_Novel_Method_for_Decentralised_Peer-to Peer_Software_License_Validation_Using_Cryptocurrency_Blockchain_Technology
25. What is a Blockchain Explorer? Guide to Block Explorers // (онлайн): https://www.sofi.com/learn/content/blockchain-explorer/
26. Getting Started with Python requests – GET Requests // (онлайн): https://www.digitalocean.com/community/tutorials/getting-started-with-python-requests-get-requests
27. Документація по використанню Etherscan // (онлайн): https://docs.etherscan.io/api-pro/api-pro

28. Регулювання ринку крипто активів. Регламент MiCA 2022 // (онлайн): https://lmfgr.com/tpost/ezucha2ia1-regulyuvannya-rinku-kriptoaktivv-reglame
29. Блокчейн статистика. Швидкість транзакцій в секунду // (онлайн): https://www.blockchain.com/charts/transactions-per-second
30. Visa Fact Sheet. A global payment technology company at glance // (онлайн): https://usa.visa.com/dam/VCOM/global/about-visa/documents/aboutvisafactsheet.pdf
31. Документація по використанню сервіса “Chain Abuse Database” // (онлайн): https://www.chainabuse.com/reports
32. Документація по використанню сервіса “Scam Alert” // (онлайн): https://scam-alert.io/
33. The best programing language to learn in 2022 // (онлайн): https://www.techrepublic.com/article/the-best-programming-languages-to-learn-in-2022/
34. Програмування на Python – стан екосистеми розробників // (онлайн): https://www.jetbrains.com/lp/devecosystem-2021/python/
35. Опис роботи сервісу CrystalBlockchain // (онлайн): https://crystalblockchain.com/
36. Buelta J. Python Automation Cookbook: Explore the world of automation using Python recipes that will enhance your skills // Packt, 2019 – 35-47p.
37. Браян Д. Біткоїн та відмивання коштів: майнинг ефективне рішення // Журнал правознавця 2014 – 89с.
38. Максуров А. А. Блокчейн, криптовалюта, майнинг: поняття і правове регулювання // А. А. Максуров – Видавнича торгова корпорація, 2020 – 198с.
39. Дерев’янко Б. В. Ризики здійснення операцій з криптовалютою (біткоїнами) громадян і суб’єктів господарювання України // Форум права: електрон. наук. фахове вид. 2017. № 3. С. 33–39. // (онлайн): http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_3_8.pdf

40. Петрук О. М. Сучасні міжнародні тенденції в організації обігу електронних грошей / О. М. Петрук, О. В. Мельниченко // Збірник наукових праць. Економічні науки. 2014. № 22. Т. 2. С. 160–165
41. Документація по роботі блокчейн дослідника Etherscan // (онлайн): https://docs.etherscan.io/
42. A Complex Web: Bitcoin Mixing Services // (онлайн): https://blog.checkpoint.com/2016/11/23/complex-web-bitcoin-mixing-services/
43. Chainalysis team. Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies // (онлайн): https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/
44. Документація по роботі блокчейну Ethereum // (онлайн): https://ethereum.org/en/whitepaper/#token-systems
45. Kurt M. Alonso. Zero to Monero: First Edition a technical guide to a private digital currency; for beginners, amateurs, and experts // (онлайн): https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
46. H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for bitcoin," 2017 APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, 2017, pp. 9-16.
47. K. Liao, Z. Zhao, A. Doupe and G. Ahn. “Behind Closed Doors:Measurement and Analysis of CryptoLocker Ransom in Bitcoin.” in Electronic Crime Research, 2016 APWG Symposium on 2016 Jun 1, Toronto, ON. IEEE.
48. G. Ahn, A. Doupe, Z. Zhao and K. Liao. “Ransomware and Cryptocurrency: Partners in Crime” in T. Holt (ed.) Cybercrime Through an Interdisciplinary Lens. New York: Taylor & Francis, 2017, pp. 105- 126.
49. F. Reid and M. Harrigan. “Analysis of anonymity in the Bitcoin System. Security and Privacy Social Networks” New York: Springer, 2013, pp. 197-223.

50. Blockchain Inspector. “What is Blockchain Inspector.” // (онлайн): http://www.blockchaininspector.com
51. M. Moser and R. Bohme. “Trends, Tips, Tolls:A Longitudinal Study of Bitcoin transaction Fees” in International Conference on Financial Cryptography and Data Security, 2015 Jan 30. Springer, Berlin, Heidelberg.
52. M. Lischke and B. Fabian. “Analysing the Bitcoin Network:The First Four Year”. Future Internet, 2016, vol. 8, no. 1.
53. D. Ron, A. Shamir. “Quantitative analysis of the bitcoin transaction graph.” International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013. // (онлайн): https://link.springer.com/chapter/10.1007%2F978-3-642-39884-1_2
54. G. Battista, V. Donato, M. Patrignani, M. Pizzonia, V. Roselli and R. Tamassia. “Bitconeview: Visualisation of Flows in the Bitcoin Transaction Graph” in 2015 IEEE Symposium on Visualization for Cyber Security, VizSec. IEEE Computer Society, 2015, pp. 1-8.
55. C. Kinkeldey, J. Fekete and P. Isenberg. “BitConduite: Visualising and Analysing Activity on the Bitcoin Network” Eurographics Conference on Visualization (EuroVis), Posters Track (2017), 2017, pp. 1–3.
56. Половинко Г. Шляхи підвищення ефективності екологічного виховання школярів / Г. Половинко // Краєзнавство. Географія. Туризм. - 2004. - С. 4-5.
57. Логвиненко В. М. Педагогічні засади формування екологічної культури курсантів і студентів вищих навчальних закладів МНС України / В. М. Логвиненко // Вісник Львівського державного університету безпеки життєдіяльності: Збірник наукових праць. – Львів : ЛДУ БЖД, 2011. – С. 188-193.
58. Єрмоленко А.М. Соціальна етика та екологія. Гідність людини – шанування природи / А.М. Єрмоленко. – 2010. – С. 416.

ДОДАТКИ

Додаток А

Фрагмент вихідного коду програмного забезпечення

```
import requests
import json
import time
import boto3
from goplus.address import Address

## Використання Boto3 бібліотеки для отримання EtherscanAPI Key від AWS SecretsManager
def get_secret(secret_name):
    session = boto3.session.Session()
    client = session.client(service_name='secretsmanager')

    try:
        get_secret_value_response = client.get_secret_value(SecretId=secret_name)
    except Exception as e:
        print(f"Error retrieving secret: {e}")
        return None

    if 'SecretString' in get_secret_value_response:
        secret = get_secret_value_response['SecretString']
    else:
        secret = get_secret_value_response['SecretBinary']
```

```
return secret

## Використання Boto3 бібліотеки для отримання даних з таблиць
def get_ofac_wallets_list():
    dynamodb = boto3.resource('dynamodb')

    table = dynamodb.Table('ofac_eth_list')

    try:
        response = table.get_item(Key={'source': 'ofac_eth'})
    except Exception as e:
        print(f"Error accessing DynamoDB: {e}")
        return []

    return response.get('Item', {}).get('wallets_list', [])

def get_illegal_ops_wallets_list():
    dynamodb = boto3.resource('dynamodb')

    table = dynamodb.Table('wallets_illegal_ops_open_source')

    try:
        response = table.get_item(Key={'source': 'wallets_illegal_ops'})
    except Exception as e:
        print(f"Error accessing DynamoDB: {e}")
        return {}
```

```
  return response.get('Item', {}).get('project_list', {})


API_KEY_TOKEN = get_secret("/monitoring_phishing_operation/eth_api_key")
BASE_URL = "https://api.etherscan.io/api"
HEADERS = {'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
OPR/82.0.4227.50'}


ETH_THRESHOLD = 2 * 10**18  # 2 ETH в Wei
FREQUENCY_THRESHOLD = 10  # Кількість операцій
SAME_AMOUNT_THRESHOLD = 3  # Кількість одинакових транзакцій підряд


def load_json_data(file_path):
    try:
        with open(file_path, 'r') as file:
            return json.load(file)
    except Exception as e:
        print(f"Error loading JSON data: {e}")
        return None


def send_request(url_params):
    try:
        response = requests.get(BASE_URL + url_params, headers=HEADERS)
        response.raise_for_status()
        return response.json()['result']
    except requests.RequestException as e:
        print(f"Request error: {e}")
        return None
```

```
    except KeyError:
        print("Error parsing JSON response.")
        return None

def get_all_transactions(address, start_time=0):
    params = f"?module=account&action=txlist&address={address}&startblock=0&endblock=99999999&sort=asc&apikey={API_KEY_TOKEN}"
    result = send_request(params)
    if result:
        return [tx for tx in result if int(tx["timeStamp"]) > start_time]
    return []

def get_specific_trans_info(transactions, transaction_hash):
    return next((tx for tx in transactions if tx['hash'] == transaction_hash), None)

def get_wallet_balance(address):
    params = f"?module=account&action=balance&address={address}&tag=latest&apikey={API_KEY_TOKEN}"
    result = send_request(params)
    return int(result) if result else None

def check_wallet_security(address):
    response = Address(access_token=None).address_security(address=address)

    try:
        data = response.to_dict()
```

```
    except AttributeError:
        print("Cannot convert response to dictionary.")
        return

    if data['code'] == 1:
        result = data.get('result', {})
        flagged_issues = [key for key, value in result.items() if value == "1"]

        if flagged_issues:
            print(f"P0: Wallet {address} is flagged in 'data_source':
{result.get('data_source', 'Unknown')}")
            for issue in flagged_issues:
                print(f"    Flagged Issue: {issue}")

def ask_to_continue():
    response = input("Do you want to continue monitoring the wallet? Enter Yes/No
(Y/N): ").lower()
    return response in ['yes', 'y']

def monitor_wallet(account_address, last_check_timestamp):
    print("Program in the monitoring mode, waiting for the new transactions in the
wallet.....")
    time.sleep(3600)
    print("Checking for new transactions...")
    new_transactions = get_all_transactions(account_address, last_check_timestamp)
    if new_transactions:
        print("\nNew transactions found:")
        for tx in new_transactions:
```

```
            print(f"Transaction Hash: {tx['hash']}, Value: {int(tx['value']) / 10**18}
ETH")
    else:
        print("No new transactions found.")
    return int(time.time())


def track_transaction_chain(transactions, stolen_amount):
    thief_wallets = {}
    wallet_chain_length = 0
    amount_frequencies = {}
    time_stamps = []

    for tx in transactions:
        value = int(tx['value'])
        if value >= stolen_amount:
            thief_wallets[tx["to"]] = value
            wallet_chain_length += 1
            amount_frequencies[value] = amount_frequencies.get(value, 0) + 1
            time_stamps.append(int(tx["timeStamp"]))

    triggers = []
    if any(value > ETH_THRESHOLD for value in thief_wallets.values()):
        triggers.append("P1: Transaction amount exceeded the threshold")
    if wallet_chain_length > 3:
        triggers.append("P2: Possible mixing services")
    if len(time_stamps) >= FREQUENCY_THRESHOLD and max(time_stamps) -
min(time_stamps) < 3600:
        triggers.append("P3: High frequency of transactions within a short time frame")
```

```
    if any(count >= SAME_AMOUNT_THRESHOLD for count in
amount_frequencies.values()):
        triggers.append("P2: Repeated transactions of the same amount to different
addresses")
    for tx in transactions:
        if get_wallet_balance(tx["to"]) == 0:
            triggers.append("P3: Wallet's balance dropped to zero after transaction")
            break

    return thief_wallets, triggers

def main():
    account_address = input("Account address: ")
    transaction_hash_test = input("Interested TransactionID: ")
    illegal_phishing_data = get_illegal_ops_wallets_list()
    ofac_data = get_ofac_wallets_list()

    print("Tracking fraudulent transactions...")
    all_transactions = get_all_transactions(account_address)
    specific_trans = get_specific_trans_info(all_transactions, transaction_hash_test)

    last_check_timestamp = int(time.time())  # Current timestamp

    wallet_found_in_phishing_db = False
    wallet_found_in_ofac_db = False

    if specific_trans:
        stolen_amount = int(specific_trans['value'])
```

```
    thief_wallets, triggers = track_transaction_chain(all_transactions,
stolen_amount)


    print("\nWallets with stolen money:")
    for address, balance in thief_wallets.items():
        print(f"Address: {address}, Balance: {balance / 10**18} ETH")
        check_wallet_security(address)


        for site, wallets in illegal_phishing_data.items():
            if address in wallets:
                print(f"P0: Wallet address {address} is found in IllegalActivityDB, as
{site}")
                wallet_found_in_phishing_db = True


        if address in ofac_data:
            print(f"P0: Wallet address {address} is found in OFAC Sanction DB")
            wallet_found_in_ofac_db = True


    if account_address in ofac_data:
        print(f"P0: Initial account address {account_address} is found in OFAC
Sanction DB")
    for site, wallets in illegal_phishing_data.items():
        if account_address in wallets:
            print(f"P0: Initial account address {account_address} is found in
IllegalActivityDB, as {site}")
    check_wallet_security(account_address)


    continue_monitoring = ask_to_continue()
```

```
        while continue_monitoring:
            last_check_timestamp = monitor_wallet(account_address,
last_check_timestamp)
            continue_monitoring = ask_to_continue()

        if triggers:
            print("\nNotifications:")
            for trigger in triggers:
                print(trigger)

        if not wallet_found_in_phishing_db:
            print("INFO: No wallets are found in the IllegalActivityDB.")

        if not wallet_found_in_ofac_db:
            print("INFO: No wallets are found in the OFAC Sanction DB.")

    else:
        print("Transaction not found.")

if __name__ == "__main__":
    main()
```