ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення ризиків використання віртуальної валюти під час виконання транзакцій»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Асман Олександр

Виконав: здобувач вищої освіти групи БСДМ-61
Асман О. Я.
(ПРІЗВИЩЕ, Ім'я)

Керівник: Кожухівський А. Д.
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Асману Олександру Ярославовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія виявлення ризиків використання віртуальної валюти під час виконання транзакцій»
керівник магістерської роботи д.т.н., професор Кожухівский А. Д.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «19» жовтня 2023 року № 145.

2. Строк подання студентом магістерської роботи 15.12.2023 р.

3. Вихідні дані до магістерської роботи
корпоративна інформаційна система;
Аналіз основних ризиків, пов'язаних з транзакціями віртуальних валют
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи.
2. Аналіз існуючих технологій та засобів для виявлення ризиків у використанні віртуальних валют.
3. Результати аналізу методів та засобів захисту кінцевих точок на прикладі Syxsense.
4. Інноваційні підходи до виявлення та управління ризиками віртуальної валюти

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу проблеми забезпечення кібербезпеки віртуальної валюти під час виконання транзакцій.

4. Аналіз стану та перспективи технологій виявлення ризиків в віртуальній фінансовій сфері

5. Результати аналізу існуючих методів та засобів захисту кібербезпеки віртуальної валюти під час виконання транзакцій.

6. Інноваційні підходи до виявлення та управління ризиками віртуальної валюти

7. Розроблення рекомендацій щодо застосування методів та засобів захисту віртуальної валюти під час виконання транзакцій.

8. Висновки за результатами роботи.

6. Дата видачі завдання 26.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми забезпечення захисту використання віртуальної валюти під час виконання транзакцій.	27.09.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	15.10.2023 р.	
3.	Аналіз ризиків та проблем забезпечення кібербезпеки віртуальної валюти під час виконання транзакцій.	04.11.2023 р.	
4.	Аналіз існуючих методів та засобів захисту віртуальної валюти під час виконання транзакцій.	23.11.2023 р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту віртуальної валюти під час виконання транзакцій.	09.12.2023 р.	
6.	Оформлення результатів дослідження.	13.12.2023 р.	
7.	Підготовка доповіді до захисту.	15.12.2023 р.	

Студент Асман О.Я

(підпис) прізвище та ініціали

Керівник магістерської роботи Кожухівський А. Д.

(підпис) прізвище та ініціали

РЕФЕРАТ

Текстова частина магістерської роботи: 56 сторінок, 6 рисунків, 12 джерел, 2 таблиці.

Об'єкт дослідження – транзакції віртуальної валюти, які є потенційними цілями кібератак.

Предмет дослідження – технологія виявлення ризиків використання віртуальної валюти під час виконання транзакцій.

Мета роботи – є дослідження та аналіз сучасних технологій виявлення ризиків використання віртуальної валюти під час виконання транзакцій.

Методи дослідження – аналіз джерел інформації за темою роботи, вивчення документації, відтворення процесу захисту транзакцій віртуальної валюти.

В сучасному світі віртуальні валюти, такі як біткоїн, ефіріум та інші, набувають все більшого поширення в сфері фінансів. Зростання популярності криптовалют веде до збільшення ризиків, пов'язаних з їх використанням у незаконних або неетичних цілях. Одним із важливих аспектів управління цими ризиками є розробка та впровадження технологій виявлення небезпеки під час виконання транзакцій з віртуальною валютою.

Вивчення цієї теми дозволить виявити перспективи та можливості вдосконалення систем безпеки в криптовалютному середовищі, сприяючи подальшому розвитку цього виду фінансових інструментів. В роботі проаналізовано поняття кібербезпеки у віртуальній валюті та досліджено сучасні технології виявлення ризиків у віртуальній валюті під час виконання транзакцій.

Результати дослідження можуть бути використані в практичній діяльності для підвищення ефективності захисту віртуальних операцій і в організацій від загрозливої діяльності і поведінки.

ВІРТУАЛЬНА ВАЛЮТА, РИЗИКИ, ТРАНЗАКЦІЇ, БЛОКЧЕЙН, КРИПТОГРАФІЯ, ВІДМИВАННЯ ГРОШЕЙ, ФІНАНСУВАННЯ ТЕРОРИЗМУ, СМАРТ-КОНТРАКТИ, ТЕХНОЛОГІЇ ВИЯВЛЕННЯ РИЗИКІВ, НЕНОРМАЛЬНА АКТИВНІСТЬ, ШАХРАЙСТВО, ПЕРСПЕКТИВИ, МАЙБУТНІ НАПРЯМКИ.

ABSTRACT

Master`s thesis: 56 pages, 6 figures, 12 sources, 2 tables.

Object of research - virtual currency transactions, which are potential targets of cyberattacks.

Subject of research - technology for detecting the risks of using virtual currency during transactions.

Purpose - there is research and analysis of modern technologies for identifying the risks of using virtual currency during transactions.

Research methods - analysis of sources of information on the topic of work, study of documentation, reproduction of the process of protection of virtual currency transactions.

In today's world, virtual currencies such as bitcoin, ethereum and others are becoming more and more widespread in the field of finance. The growing popularity of cryptocurrencies leads to an increase in the risks associated with their use for illegal or unethical purposes. One of the important aspects of managing these risks is the development and implementation of technologies to detect the dangers when performing virtual currency transactions.

The study of this topic will reveal prospects and opportunities for improving security systems in the cryptocurrency environment, contributing to the further development of this type of financial instruments. The paper analyzes the concept of cyber security in virtual currency and investigates modern technologies for detecting risks in virtual currency during transactions.

The results of the study can be used in practical activities to increase the effectiveness of protecting virtual operations and organizations from threatening activities and behavior.

VIRTUAL CURRENCY, RISKS, TRANSACTIONS, BLOCKCHAIN, CRYPTOGRAPHY, MONEY LAUNDERING, TERRORISM FINANCING, SMART CONTRACTS, RISK DETECTION TECHNOLOGIES, ABNORMAL ACTIVITY, FRAUD, OUTLOOK, FUTURE DIRECTIONS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DeFi – децентралізовані фінансові платформи

DApps – децентралізовані програми

NFT – незамінні токени

ICO – Initial Coin Offering

KYC – Know Your Client

AML – Anti Money Laundering

DDoS – Distributed Denial of Service

PoW – Proof of Work

PoS – Proof of Stake

DPoS – Delegated Proof of Stake

RSA – Rivest, Shamir та Adleman

API – Application programming interface

SSO – Single Sign-On

LDAP – Lightweight Directory Access Protocol

FATF – Financial Action Task Force

ERC – Enhanced Resource Company

ML – Machine learning

ВСТУП

Сучасний етап розвитку фінансової системи світу супроводжується активним використанням віртуальних валют, які набувають все більшого значення в економіці. Поширення криптовалют, таких як Bitcoin, Ethereum, та інші, викликає рост інтересу до технологічних аспектів їхнього використання та можливих ризиків.

Однією з ключових проблем використання віртуальних валют є необхідність забезпечення безпеки та виявлення можливих ризиків під час здійснення транзакцій. Технологічні інновації в цьому напрямку є критичним елементом для забезпечення стійкості та надійності фінансових операцій у віртуальному середовищі.

Мета даної магістерської роботи полягає в дослідженні та аналізі сучасних технологій виявлення ризиків використання віртуальної валюти під час виконання транзакцій. Вивчення цієї теми дозволить виявити перспективи та можливості вдосконалення систем безпеки в криптовалютному середовищі, сприяючи подальшому розвитку цього виду фінансових інструментів.

Робота передбачає детальний розгляд сучасних методів та інструментів виявлення ризиків, а також їхню ефективність та застосування у віртуальних фінансових системах. Окрім того, планується розгляд можливих викликів та проблем, що виникають при використанні цих технологій, та пошук шляхів їх вирішення.

Дослідження вказаної теми в контексті технологій виявлення ризиків використання віртуальної валюти виявиться важливим внеском у розуміння сучасних викликів та перспектив цього новаторського сегменту фінансового ринку.

Розділ 1. 1 АНАЛІЗ РИЗИКІВ ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ВАЛЮТИ

1.1 Роль віртуальної валюти в сучасному світі

Початок цифрової ери приніс із собою безліч інновацій, змінивши спосіб нашого життя, роботи та транзакцій. Серед цих інновацій віртуальні валюти стали революційною силою, кинувши виклик традиційним фінансовим парадигмам і проклавши шлях до нової ери цифрових транзакцій.

Віртуальна валюта — це тип цифрових активів, призначених для роботи як засіб обміну. Ці валюти використовують криптографію для захисту транзакцій, контролю створення додаткових одиниць і перевірки передачі активів. Віртуальні валюти існують переважно в цифровій сфері, без фізичних аналогів, таких як монети чи купюри.

Однією з ключових рис віртуальних валют є децентралізація. Вони працюють на основі технології блокчейн, що робить їх стійкими до зовнішніх втручань та забезпечує безпеку та прозорість фінансових операцій. Крім того, вони відкривають нові можливості для глобальних та міжнародних фінансових транзакцій, знижуючи витрати та сприяючи ефективності.

Технологія блокчейн ще не досягла своєї остаточної форми — вона постійно розвивається. Поряд із цим можна відзначити п'ять найбільш значущих відкритих інновацій та особливостей, що характеризують блокчейн сьогодні. Першою відкритою інновацією, заснованою на технології блокчейн, стала поява у 2008 році Біткойна — першої криптовалютної однорангової мережі та внутрішньої цифрової валюти. Ця мережа являла собою комп'ютерну систему, в якій кожна одиниця мережі виконувала ту саму функцію. Кожен учасник системи був одночасно клієнтом та сервером [1].

Беручи до уваги ці передумови, використання стали криптовалюти та технології блокчейн - одна з відповідей на можливості та виклики розвитку світового господарства, в т.ч. пов'язані з недосконалістю державного та ринкового регулювання: криптовалюта є продуктом цифрової економіки; при створенні

криптовалюти, алгоритми, засновані на об’єктивних математичних використовуються закони; контроль за обігом криптовалют здійснюється самою системою, що робить її більш стабільною щодо дій третіх осіб; криптовалюти можуть зменшити транзакційні витрати; криптовалюти є міжнародним продуктом, створений в інтересах і для обслуговування всіх учасників. Незважаючи на технічні обмеження та труднощі пов'язані з майнінгом і обігом криптовалют (низька швидкість обробки транзакцій, ризик [2] системи стабільність тощо), окремі держави вже експериментують цифрові гроші, а також технологія блокчейн [3]. однак, значення перспектив використання криптовалют для громадян, уряду і бізнесу різні.

Приклади віртуальних валют

Віртуальні валюти рясні та різноманітні, кожна зі своїми унікальними властивостями, сценаріями використання та базовими технологіями.

- Bitcoin - Першою і найбільш загальновизнаною віртуальною валютою є біткойн, концептуалізований невідомою особою або групою людей під ім’ям Сатоші Накамото. Створення біткойна започаткувало еру децентралізованих віртуальних валют, надихнувши безліч інших проектів.

- Ethereum, інший приклад, розширює концепцію віртуальних валют для створення повноцінної платформи на основі блокчейну. Ефір, рідна валюта Ethereum, живить мережу та створює світ децентралізованих програм.

- Ripple або XRP — це віртуальна валюта, призначена для ефективних міжнародних грошових переказів, спрямована на полегшення недорогих платежів у реальному часі між фінансовими установами по всьому світу.

Криптовалюти — це підмножина віртуальних валют. Хоча всі криптовалюти є віртуальними валютами, не всі віртуальні валюти є криптовалютами. Криптовалюти використовують технологію блокчейн, яка характеризується децентралізацією, прозорістю та незмінністю. Деякі віртуальні валюти, наприклад ті, що використовуються в онлайн-іграх, можуть не використовувати технологію блокчейн і не бути децентралізованими.

Переваги віртуальних валют

Переваги віртуальних валют полягають у наступному:

- Технологічні рейки віртуальних валют можуть усунути географічні кордони.
- Децентралізовані віртуальні валюти можуть усунути посередників під час грошових операцій і встановити прямий зв’язок між двома сторонами транзакції.
- Віртуальні валюти можна запрограмувати для здійснення автоматичних транзакцій. Наприклад, смарт-контракти на блокчейні Ethereum можуть утримувати та вивільняти гроші на депозитних рахунках без втручання людини.
- Віртуальні валюти є цифровими сховищами цінностей і можуть призначати цінність різнорідним наборам об’єктів, від ігрових токенів до творів мистецтва.

Недоліки віртуальних валют

До недоліків віртуальних валют можна віднести наступне:

- Віртуальні валюти є привабливою мішенню для хакерів. Було кілька випадків крадіжки криптовалюти хакерами.
- Віртуальні валюти можуть стати об’єктом шахрайства. Кілька початкових пропозицій монет (ICO), які стали популярними після різкого зростання цін

на криптовалюту, були шахрайством, у якому приватні розробники продавали нікчемні токени для гіпотетичних мереж. Жетони не можна було конвертувати в інші валюти.

- Нерегульовані віртуальні валюти не пропонують інвесторам юридичних засобів, оскільки вони випускаються приватними особами і, здебільшого, не регулюються фінансовими органами.
- Віртуальні валюти можуть бути схильні до різких коливань цін.

Віртуальні валюти можуть бути використані будь-де в світі, де є Інтернет. Це особливо корисно для міжнародних транзакцій, оскільки вони не обмежені територіальними межами чи валютними обмеженнями. Це зменшує необхідність проводити операції через інтермедіарів і може пришвидшити та здешевити глобальні фінансові операції.

Реакція регуляторів на віртуальну валюту в різних країнах різниться. Деякі країни визнають криптовалюту як легітимний засіб платежу чи інвестиції, і розробляють відповідні нормативи, тоді як інші виражають серйозні обурення та виражають сумніви у її легітимності.

У багатьох юрисдикціях проводяться роботи над встановленням стандартів безпеки для обмінників криптовалют, криптовалютних гаманців і торгових платформ. Також розглядаються питання страхування та захисту інвесторів для зменшення ризиків.

Багато країн вимагають від платіжних платформ та обмінників віртуальних валют виконувати процедури «Знай свого клієнта» (KYC) та протидії відмиванню грошей (AML). Це спрямовано на забезпечення безпеки та виключення використання криптовалют для незаконних цілей.

Деякі країни розглядають випуск власних цифрових валют центральних банків. Це може стати альтернативою криптовалютам та дозволить урядам більше контролю над цифровими фінансами.

Деякі юрисдикції впроваджують регуляторні "пісочниці" для інноваційних фінтех-проектів, що дозволяє їм експериментувати в обмеженому регуляторному середовищі без швидкого впровадження жорстких правил.

Оскільки віртуальна валюта перетинає межі багатьох країн, регуляція є досить складною задачею. Відсутність єдиних стандартів часто призводить до неоднакових підходів та може ускладнити взаємодію між різними ринками.

Питання оподаткування криптовалют також залежить від конкретних правил кожної країни. Деякі країни визначають криптовалюту як майно, тоді як інші розглядають її як форму грошей чи товару, що може впливати на спосіб оподаткування.

Відзначається, що регуляція в цій галузі швидко змінюється, і різні країни виробляють власні стратегії, спрямовані на баланс між стимулюванням інновацій та забезпеченням фінансової стабільності та безпеки.

Іноді криптовалюту можна заробити безкоштовно: це невеликий подарунок, який приваблює людей у всьому світі. Все що вам потрібно - це ввести captcha або переглянути рекламу, і за це вам буде нараховано, наприклад, Сатоші (одна сота мільйонів біткойнів). Але це не нормальний спосіб заробітку грошей, тому що у випадку блокування сайту, то криптовалюта зникає. Можливі подарунки від великих сервісів, наприклад, хорошого посту чи статті, зображення, яке користується попитом серед інших користувачів [4].

Купити криптовалюту в Україні можна на різних обмінниках. Обмінники не завжди вигідні, тому що вони заробляють на різниці вартості, найкращі варіанти з обміном або пряма покупка від продавця з хорошою репутацією [7]. Важливо, пам'ятати про безпеку угоди; багато практиків [6] рекомендують купувати криптовалюту від продавців свого міста.

Віртуальні валюти стали об'єктом інвестицій, використовуються для торгівлі на криптовалютних біржах та стають складовою фінансового портфеля для багатьох інвесторів. З'явилися нові фінансові інструменти, такі як Initial Coin Offerings (ICO) та децентралізовані фінансові платформи (DeFi), які змінюють традиційний підхід до фінансів.

Поки ми переходимо в епоху цифрової трансформації, віртуальні валюти продовжують руйнувати традиційний фінансовий ландшафт. Завдяки потенціалу революції в глобальних платежах віртуальні валюти створюють як значні можливості, так і проблеми. Користувачам і зацікавленим сторонам цього нового фінансового світу дуже важливо розуміти динаміку віртуальних валют, щоб використовувати їх переваги та зменшити ризики.

1.2 Структура та функції віртуальних валют

Віртуальні валюти – це цифрові або криптографічні представники вартості, які існують в електронній формі і не мають фізичного аналогу. Серед найвідоміших віртуальних валют можна виділити біткоїн та інші криптовалюти. Це платіжна система, в якій існує логічний зв’язок між двома сторонами транзакції peer-to-peer. Це надихнуло на багато додаткових ідей, концепцій і розробок. Головним підходом у всіх цих нових ініціативах є пропозиція використовувати прямі стосунки «peer-to-peer». Між двома сторонами транзакції без будь-якої третьої сторони, такі транзакції дуже ефективні, але без забезпечення їх перевірки, безпеки та конфіденційності та без участі будь-якої третьої сторони дуже важко.

Нижче наведено загальну структуру та функції віртуальних валют:

- Блокчейн:
    - *Структура блокчейну:* Віртуальні валюти використовують технологію блокчейн – децентралізовану базу даних, яка зберігається на різних комп'ютерах, називаних вузлами.
    - *Блоки:* Інформація про транзакції зберігається у блоках, які зв'язані між собою.

- Криптографія:

- *Ключі:* Віртуальні валюти використовують криптографію для забезпечення безпеки. Кожен користувач має публічний та приватний ключі.
- *Цифровий підпис:* Кожна транзакція підписується приватним ключем, що дозволяє перевірити автентичність транзакції.

- Децентралізація:

  - *Відсутність центрального контролю:* Віртуальні валюти, особливо криптовалюти, прагнуть уникнути централізованого контролю, який зазвичай здійснюється банками чи іншими фінансовими установами.
  - *Мережеві вузли:* Транзакції обробляються мережею розподіленого вузлів, і кожен вузол має копію блокчейну.

- Добування (майнінг):
  - *Процес майнінгу:* Деякі віртуальні валюти, зокрема біткоїн, використовують процес майнінгу, де комп'ютери розв'язують складні математичні завдання для підтвердження транзакцій та створення нових блоків.

- Децентралізовані програми (DApps):
  - *Смарт-контракти:* Деякі віртуальні валюти, як Ethereum, дозволяють розробляти децентралізовані програми (DApps) за допомогою смарт-контрактів – програм, які автоматизують виконання угод.

- Вартість та обмін:

- *Обмін:* Віртуальні валюти можна обмінювати на інші валюти чи товари через криптовалютні біржі.
- *Вартість:* Вартість віртуальних валют може коливатися в залежності від попиту та пропозиції на ринку.

- Анонімність та приватність:
  - *Анонімні транзакції:* Деякі віртуальні валюти, наприклад, Monero, пропонують більш високий рівень анонімності та приватності у порівнянні з біткоїном.

- Регулювання та легальність:
  - *Правовий статус:* Регулювання віртуальних валют різниться в різних країнах, і вони можуть бути суб'єктом різних правових статусів.
- Інновації та розвиток:
  Технологічний прогрес: Віртуальні валюти стають основою для нових технологічних інновацій, таких як блокчейн та розумні контракти.

Блокчейн є розподіленою базою даних, яка зберігається на різних комп'ютерах (вузлах) у мережі. Тут кожен блок містить інформацію про групу транзакцій, і вони послідовно додаються до ланцюжка блоків.

Криптографічні принципи грають важливу роль у забезпеченні безпеки віртуальних валют. Кожен користувач отримує пару ключів: публічний та приватний. Публічний ключ використовується для створення унікальної адреси, на яку можна надсилати валюту. Приватний ключ використовується для підпису транзакцій та забезпечення доступу до власного гаманця.

Децентралізація є ключовим аспектом віртуальних валют. Вони не залежать від центральних установ, таких як банки, і опираються на роботу розподілених вузлів для перевірки та обробки транзакцій. Різні алгоритми консенсусу, такі як Proof of

Work (доказ роботи) або Proof of Stake (доказ власності), використовуються для підтвердження правильності та надійності транзакцій.

Вартість віртуальних валют визначається ринковою попитом і пропозицією. Вони можуть бути обмінювані на традиційні валюти чи інші криптовалюти через спеціалізовані біржі. Крім того, віртуальні валюти використовуються для реалізації смарт-контрактів — програм, які автоматизують та виконують угоди без посередництва.

Загалом, віртуальні валюти виконують роль цифрового середовища для обміну значенням, спираючись на технології блокчейн та криптографії для забезпечення безпеки та децентралізації. Функції та характеристики можуть варіюватися в залежності від конкретної віртуальної валюти.

1.3 Аналіз ризиків при використанні віртуальної валюти

Незважаючи на всі переваги, віртуальні валюти також стикаються з викликами та ризиками, такими як високі коливання вартості, недостатня регуляція, можливості для кібератак і використання для нелегальних дій.

Криптовалюти суттєво впливають на технологічний світ фіатних грошей, якому принаймні 800 років. Криптовалюта — це цифровий актив, який використовує технологію розподіленої книги або блокчейн для здійснення транзакцій. Цифрова валюта, з іншого боку, є різновидом валюти в цифровому світі у вигляді цифрових форм електронного обладнання. Синонімом цифрових грошей, цифрових грошей, електронних грошей і кібергрошей є терміни. Незамінні токени (NFT), токени Defi та криптовалюти є прикладами видів у індустрії блокчейнів. У статті аналізуються двадцять наукових статей за допомогою PRISMA. В результаті дослідження ризик цифрових транзакцій зростає, а довіри немає. Крім того, електронна економіка нестабільна. І поводитися з ним потрібно дуже обережно, щоб уникнути або звести до мінімуму проблеми, які можуть виникнути. Незабаром приватні криптовалюти піддадуться шаленій реконфігурації, а впровадження

блокчейнів поширюватиметься з помітною швидкістю, доки будуть здійснюватися платежі за цифрові інновації. Знову ж таки, дослідження шахрайства з біткойнами швидко розширюються за обсягом і широтою, але все ще знаходяться на ранній стадії.

Отже, поділимо основні ризики використання віртуальних валют на два підрозділи: системні та технічні

Системні ризики використання віртуальної валюти:

- Блокчейн-мережі: Пошкодження або зупинка роботи блокчейн-мережі може призвести до затримок у виконанні транзакцій та порушення їх консистентності.

- Хакерські атаки: Зловмисники можуть атакувати обмінники чи гаманці, що призведе до втрати активів та порушення конфіденційності користувачів.

- Забуття паролю: Втрата пароля або доступу до гаманця може призвести до невідновлення втрачених коштів, особливо в тих випадках, де відсутня процедура відновлення.

- Баги у коді: Недоліки або помилки в смарт-контрактах можуть викликати фінансові втрати та непередбачувані наслідки для користувачів.

- Обмежена пропускна спроможність: Деякі блокчейн-мережі мають обмежену пропускну спроможність, що може призвести до затримок у виконанні транзакцій у разі великого попиту.

- Ризик деанонімізації: Деякі криптовалюти, як Monero або Zcash, надають високий рівень анонімності, але можуть потрапити під небажаний контроль правоохоронних органів.

- Хардфорки та софтфорки: Зміни в протоколах блокчейну через хардфорки чи софтфорки можуть викликати розбрат у спільноті та призвести до виникнення конкуруючих версій блокчейну.

- Енергозатратні алгоритми: Деякі консенсус-алгоритми, такі як Proof-of-Work, вимагають великої кількості енергії, що може впливати на довкілля.

- Споживачі та транзакції: В деяких випадках, використання криптовалют може викликати ризик втрати приватності користувачів через можливість відстеження транзакцій.

- Суперечки у спільноті: Розвиток криптовалют часто супроводжується розбратами та суперечками у спільноті, що може впливати на прийняття рішень та розвиток проекту.

Технічні ризики використання віртуальної валюти:

- Хакерські атаки: Криптовалютні обмінники, гаманці та блокчейн-мережі можуть бути об'єктом хакерських атак, що може призвести до втрати коштів та порушення конфіденційності.

- Баги в коді: Недоліки у смарт-контрактах можуть викликати фінансові втрати та непередбачувані наслідки, адже вони виконуються автоматично без можливості втручання.

- Обмежена пропускна спроможність: Зростаючий обсяг транзакцій може викликати затримки та перевантаження в блокчейн-мережах, обмежуючи їх масштабність.

- Час підтвердження: Швидкість підтвердження транзакцій у блокчейн-мережі може залежати від вибору конкретної криптовалюти та її алгоритму консенсусу.

- Ризик деанонімізації: Деякі криптовалюти, які претендують на високий рівень анонімності, можуть виявитися менш приватними, ніж очікувалося.

- Забуття паролю чи втрата ключів: Втрата доступу до гаманця може призвести до втрати коштів, і відновлення може бути неможливим без відповідних заходів безпеки.

- Конфлікти між розробниками: Технічні обмеження в блокчейн-мережах можуть викликати розбрат та конфлікти між розробниками щодо вдосконалення.

- Хардфорки та софтфорки: Зміни в протоколах, такі як хардфорки, можуть викликати поділ у спільноті та виникнення конфліктів.

- Виток інформації: Непередбачувані витоки конфіденційної інформації можуть виникнути через помилки в програмному забезпеченні або через хакерські атаки.

- Велика енергоспоживання: Алгоритми консенсусу, особливо Proof-of-Work, можуть вимагати значної кількості енергії, що породжує занепокій стосовно екологічних наслідків.

Аналіз ризиків при використанні віртуальної валюти дозволяє глибше розуміти сутність цього фінансового інструменту та підготуватися до ефективного використання його переваг. Технічні аспекти, такі як кібербезпека та проблеми масштабування, потребують постійної уваги для забезпечення безпеки та ефективності транзакцій. Спрощення та прискорення фінансових операцій та смарт-контрактів супроводжується технічними викликами та невизначеністю в регулюванні.

Необхідною є постійна увага до ризиків та взаємодія всіх зацікавлених сторін - користувачів, розробників, регуляторів та громадськості. Тільки враховуючи ці ризики та працюючи над їхнім усуненням, можна забезпечити стійкий та безпечний розвиток віртуальних валют у сучасному фінансовому середовищі.

1.4 Аналіз існуючих рішень з кібербезпеки при використанні віртуальної валюти

Аналіз існуючих рішень з кібербезпеки в контексті віртуальної валюти є важливим завданням, оскільки криптовалюти, такі як Bitcoin, Ethereum, і інші, стали об'єктом зростаючої уваги як серед користувачів, так і серед кіберзлочинців. Нижче наведено деякі ключові аспекти та рішення, які використовуються для забезпечення кібербезпеки в контексті віртуальних валют:

Таблиця 1.1.

Заходи з кібербезпеки при використанні віртуальної валюти

Аспект	Рішення та Заходи безпеки
Зберігання ключових пар	- Використання холодних гаманців або апаратних гаманців - Захист приватних ключів від доступу через Інтернет

Мультипідписні гаманці	- Використання гаманців із можливістю мультипідпису - Збільшення рівня безпеки авторизації транзакцій
Двофакторна автентифікація	- Застосування 2FA для доступу до гаманця та платформ - Збільшення захисту від несанкціонованого доступу
Шифрування	- Використання шифрування для конфіденційної інформації - Захист даних про транзакції від несанкціонованого доступу
Безпека мережі	- Заходи безпеки для запобігання атакам на протоколи - Захист від атак типу 51% та інших атак на консенсус
Регулювання та дотримання	- Дотримання відповідного законодавства та регулювань - Зменшення юридичних ризиків та захист користувачів
Аудит безпеки	- Регулярні аудити для виявлення та усунення вразливостей - Забезпечення сталого вдосконалення системи безпеки
Експертиза безпеки	- Залучення експертів для оцінки та удосконалення заходів - Забезпечення високого рівня експертизи у кібербезпеці
Публічна інформація та освіта	- Інформаційні кампанії для свідомості користувачів

	- Збільшення рівня освіти щодо безпеки віртуальних валют
IDS та IPS	- Використання систем виявлення та запобігання вторгнень - Захист мережевих та системних ресурсів від атак

Одним з основних аспектів забезпечення кібербезпеки віртуальних валют є використання криптографії. Багато віртуальних валют базуються на технології блокчейн, яка використовує складні математичні алгоритми для забезпечення безпеки транзакцій.

Безпека гаманців, де користувачі зберігають свої віртуальні валюти, грає важливу роль. Використання холодних гаманців (offline зберігання ключів) та двофакторної аутентифікації може додатково захистити користувачів від крадіжок і хакерських атак.

Мережеві атаки, такі як DDoS (розподілені атаки з відмовою в обслуговуванні), можуть призвести до збоїв в мережі віртуальної валюти. Для захисту від таких атак, розробники повинні вдосконалювати мережеві та безпекові протоколи.

Регулювання віртуальних валют може відігравати важливу роль у забезпеченні кібербезпеки. Створення стандартів безпеки та їх дотримання може допомогти запобігти багатьом видам атак та зловживань.

Постійне вдосконалення програмного забезпечення для виправлення виявлених уразливостей є критичним елементом кібербезпеки віртуальних валют. Часті оновлення та вчасне встановлення патчів дозволяють уникнути експлуатації нових загроз.

Аналіз існуючих рішень з кібербезпеки віртуальних валют показує, що це складне завдання, яке вимагає інтеграції різноманітних технологій та стратегій. Забезпечення безпеки віртуальних валют потребує співпраці між розробниками, регуляторами та користувачами для створення надійного та стійкого кібербезпечного середовища. Нижчі транзакційні витрати

Для підприємств, яким часто потрібно здійснити кілька великих міжнародних транзакцій, комісія, що стягується традиційними банками, може легко збільшитися. У деяких випадках комісія за транзакцію може становити навіть відсоток від суми, що надсилається.

З криптовалютою комісії або відсутні, або дуже номінальні. На відміну від банків, які стягують комісію заради прибутку, ці комісії призначені лише для компенсації обчислювальної потужності, яка використовується для здійснення транзакції. Завдяки цьому комісії залишаються набагато нижчими, ніж стандартні банківські платежі.

Для великих транзакцій традиційні банки можуть вимагати кілька днів обробки та численні форми, які часто можна заповнити лише особисто. Хоча транзакції з криптовалютою часто тривають кілька годин, процес набагато швидший і повністю виконується онлайн.

Останніми роками низка країн, що розвиваються, зіткнулися з руйнівною інфляцією та різкими коливаннями своєї валюти. Через це компаніям, розташованим за межами цих країн, важко здійснювати операції з постраждалими підприємствами. Якщо валюта надзвичайно девальвована, усі отримують погану угоду.Незважаючи на те, що криптовалюти також зазнають досить значних коливань цін, більша кількість стейблів, таких як біткойн і ефіріум, показали набагато кращі показники, ніж багато офіційних валют. Це стало паличкою-виручалочкою для жителів деяких постраждалих країн і дозволило їм експортувати свої ресурси за справедливою ціною.

Так само, як і традиційні валюти, їхні криптовалюти залежать від мінливості ринку та інших економічних факторів. Однак, оскільки немає уряду, який би наглядав за цими валютами, якщо одна з них падає, немає зовнішнього методу, щоб підтримати її. Крім того, деякі менш відомі монети є просто шахрайством без внутрішньої цінності. Безпечніше використовувати відому криптовалюту, як-от Bitcoin, Ethereum, Litecoin або XRP. Вони відносно стабільні.

Справжній успіх в криптосвіті залежить від здатності галузі адаптуватися до швидко змінюючихся кіберзагроз та впроваджувати інноваційні стратегії

кібербезпеки. Розуміння та впровадження сучасних рішень може зробити віртуальні валюти набагато безпечнішими для користувачів.

Розділ 2. СТАН ТА ПЕРСПЕКТИВИ ТЕХНОЛОГІЙ ВИЯВЛЕННЯ РИЗИКІВ В ВІРТУАЛЬНІЙ ФІНАНСОВІЙ СФЕРІ

2.1 Технологічні засоби виявлення ризиків

Виявлення ризиків віртуальної валюти (криптовалюти) в сучасному світі вимагає використання різноманітних технологічних рішень і засобів.

1. Блокчейн технологія:

Блокчейн технологія є основою для багатьох криптовалют, а також знаходить широке застосування в інших галузях через свої основні принципи: децентралізація, розподіленість та безпека. Наведемо більш детальний аналіз ключових аспектів блокчейн технології:

- Децентралізація:

Без посередника: Блокчейн дозволяє взаємодіяти напряму між учасниками мережі, уникнувши посередників, таких як банки чи фінансові установи. Це зменшує витрати та час, а також збільшує ефективність.

Рівноправність: Учасники мережі мають однакові права, що робить систему більш справедливою і захищеною від владарів одного центру.

- Розподілені реєстри:

Доступ до інформації: Вся історія транзакцій зберігається на кожному вузлі мережі. Це забезпечує розподілену природу і дозволяє учасникам мережі мати доступ до повної інформації.

Захист від атак: Якщо один вузол виявляється компромітованим, інші вузли можуть попередити подальші розповсюдження некоректних даних, зберігши цілісність системи.

- Криптографічна безпека:

Шифрування та підписи: Кожна транзакція в блокчейні захищена криптографічним шифруванням та цифровим підписом. Це забезпечує конфіденційність та автентифікацію учасників.

Приватність: Хоча вся історія транзакцій є відкритою для перегляду, особиста інформація залишається зашифрованою і безпечною.

- Смарт-контракти:

Автоматизація: Смарт-контракти — це програмні коди, які виконуються автоматично при виконанні визначених умов. Вони вбудовані в блокчейн та дозволяють автоматизувати виконання угод.

Прозорість: Логіка смарт-контрактів є відкритою для перегляду, забезпечуючи прозорість між сторонами угоди.

- Консенсус-протоколи:

Гарантована єдність: Визначають правила для підтвердження нових блоків та узгодження всієї мережі. Популярні консенсус-протоколи включають Proof of Work (PoW), Proof of Stake (PoS), і Delegated Proof of Stake (DPoS).

- Масштабованість:

Проблеми масштабованості: Однією з викликів є здатність мережі обробляти великий обсяг транзакцій. Розробники ведуть дослідження та розробляють рішення для покращення масштабованості.

- Токени та ICO:

Емісія власних токенів: Блокчейн технологія дозволяє створювати та розповсюджувати власні токени, що забезпечує механізм краудфандингу через Initial Coin Offerings (ICO).

- Інтероперабельність:

Спільна робота з іншими системами: Розробники працюють над рішеннями для полегшення взаємодії різних блокчейн-мереж та створення спільних стандартів.
Спільна робота з іншими системами: Розробники працюють над рішеннями для полегшення взаємодії різних блокчейн-мереж та створення спільних стандартів.

2. Ключі шифрування:

Ключі шифрування є критичним елементом кібербезпеки, включаючи застосування їх у віртуальних валютах, які базуються на блокчейн технології. Тут детальніше розглянемо ключі шифрування та їх роль у забезпеченні безпеки:

- Пари ключів:

Симетричне та асиметричне шифрування: В системах шифрування використовуються пари ключів. У симетричному шифруванні використовується один ключ для як шифрування, так і розшифрування. У асиметричному шифруванні використовуються два ключі: публічний (для шифрування) та приватний (для розшифрування).

- Приватні ключі:

Ключ конфіденційності: Приватний ключ є конфіденційним інформаційним елементом, який володіє власник криптовалюти. Він використовується для розшифрування інформації та підпису транзакцій.

- Публічні ключі:

Ключі для взаємодії: Публічний ключ використовується для шифрування інформації, яка може бути розшифрована лише приватним ключем. Він служить для визначення власника віртуального гаманця та отримання криптовалюти.

- Криптографічна безпека:

Алгоритми шифрування: Ключі використовуються в криптографічних алгоритмах, таких як RSA, ECC (еліптична крива криптографія), або інших, щоб забезпечити надійне шифрування та захист інформації.

Захист від атак: Довжина ключів грає важливу роль у стійкості до криптографічних атак. Зазвичай використовуються ключі довжиною 128, 256 біт і більше для надійної захисту.

- Управління ключами:

Безпека ключових матеріалів: Ефективне управління ключами включає генерацію, зберігання, використання та видалення ключів. Важливо забезпечити безпеку приватних ключів, щоб уникнути несанкціонованого доступу.

Ротація ключів: Регулярна зміна ключів сприяє збереженню високого рівня безпеки, особливо в разі виявлення порушень чи втрати ключів.

- Холодне та гаряче зберігання ключів:

Гаряче зберігання: Ключі можуть бути збережені в інтернет-з'єднанних пристроях, що полегшує проведення транзакцій, але може становити ризик з віддаленим доступом.

Холодне зберігання: Холодне зберігання відбувається на офлайн-пристроях, таких як апаратні гаманці, що зменшує ризик злому через Інтернет.

- Біометричні ключі:

Інновації в аутентифікації: Розвиток біометричних технологій дозволяє використовувати фізичні параметри (відбитки пальців, розпізнавання обличчя) для забезпечення додаткового рівня безпеки ключів.

Мультифакторна аутентифікація: Використання кількох методів аутентифікації (наприклад, пароля та відбитка пальця) для забезпечення додаткового рівня безпеки.

Збереження та захист ключів шифрування є невід'ємною частиною кібербезпеки в області віртуальних валют та інших криптографічних застосувань. Знання та використання сучасних методів криптографії є критичним для забезпечення безпеки та конфіденційності користувачів.

3. Мультипідписи (Multi-signature):

Мультипідписи (Multi-signature або мультіпідписи) є інноваційною функцією в області криптографії та криптовалют, яка дозволяє створювати адреси, які вимагають підпису від декількох осіб для виконання транзакції. Ось більш детальний розгляд мультипідписів:

- Основна ідея:

Групові підписи: Мультипідписи дозволяють встановлювати вимогу до підпису від групи осіб. Замість того, щоб мати один приватний ключ і відповідний підпис, у мультипідписі є група приватних ключів, і транзакція вимагає підпису від заданої кількості членів групи.

- Кількість підписів:

Множина ключів: Мультипідпис може вимагати будь-яку кількість підписів, визначену при створенні адреси. Наприклад, 2-з 3 мультипідпис вимагає підпису від будь-яких двох з трьох ключів для виконання транзакції.

Кількість може змінюватися: В деяких системах мультипідписів кількість необхідних підписів може бути змінювана під час життєвого циклу адреси.

- Застосування:

Групові рішення: Мультипідписи широко використовуються в групових фінансових операціях, спільних гаманцях, а також в угодах між підприємствами або особами, які вимагають підтвердження декількох сторін.

Безпека та відмовостійкість: Мультипідписи забезпечують вищий рівень безпеки, оскільки для виконання транзакції необхідно скомпрометувати не один, а кілька приватних ключів.

- Більше ніж дві сторони:

Може включати більше двох ключів: Мультипідписи не обмежуються лише двома сторонами, і можуть включати будь-яку кількість ключів.

Розширення: За допомогою мультипідписів можна створити адреси, що вимагають підпису від більшої кількості осіб, що робить їх відмінним інструментом для захисту фінансових активів або розподілення контролю.

- Технічна реалізація:

Скрипти мультипідписів: Для реалізації мультипідписів використовуються спеціальні скрипти, які визначають умови для валідації транзакцій та кількість необхідних підписів.

Стандарти: Існують стандарти мультипідписів, які сприяють сумісності між різними платформами та програмним забезпеченням.

- Приватність та Безпека:

Підвищення приватності: Мультипідписи можуть допомагати зберігати конфіденційні дані, такі як фінансові відомості, в безпеці, оскільки для виконання транзакції потрібно декілька підписів.

Захист від втрати ключа: Якщо один ключ втрачено чи пошкоджено, інші члени групи можуть продовжити використовувати свої ключі безпеки для підпису транзакцій.

Використання мультипідписів сприяє покращенню безпеки та надійності транзакцій в криптовалютних системах, зокрема в умовах спільних власництв, корпоративних рішень та інших випадків, де потрібен консенсус декількох сторін.

4. Системи моніторингу та аналізу транзакцій

Системи моніторингу та аналізу транзакцій грають ключову роль у забезпеченні безпеки та виявленні потенційно небезпечних або зловживаючих операцій в області віртуальних валют і криптовалют. Ось більш детальний огляд таких систем:

- Мета та задачі:

Виявлення шахрайства та відмивання грошей: Основною метою систем моніторингу та аналізу транзакцій є виявлення ненормальної активності, такої як шахрайства, фінансування тероризму, відмивання грошей та інші незаконні операції.

Дотримання вимог законодавства: Велика частина систем моніторингу вивчається для забезпечення дотримання законодавства, зокрема в області боротьби з відмиванням грошей та фінансуванням тероризму (AML/CFT).

- Основні характеристики:

Real-time аналіз: Системи здатні проводити аналіз транзакцій у реальному часі, щоб негайно виявляти незвичайну або підозрілу активність.

Патерни та аномалії: Використання алгоритмів для виявлення звичайних патернів поведінки та аномалій, які можуть свідчити про несанкціоновані дії.

Зв'язки між адресами: Аналіз та виявлення взаємозв'язків між різними адресами гаманців для виявлення групової або координованої активності.

- Методи аналізу:

Кластерний аналіз: Використання методів кластеризації для групування схожих транзакцій та адрес гаманців.

Статистичний аналіз: Використання статистичних методів для визначення аномальних варіацій або відхилень від нормальної активності.

Машинне навчання: Застосування алгоритмів машинного навчання для вдосконалення аналізу та виявлення нових, раніше невідомих шаблонів.

- Взаємодія з регуляторами:

Подання звітності: Багато систем моніторингу транзакцій обладнані функціями подання звітності, щоб відповідати вимогам регуляторів і надавати інформацію про сумнівні операції.

Дотримання стандартів: Забезпечення дотримання стандартів AML/CFT та інших вимог законодавства, які визначають процедури виявлення та заборони незаконних дій.

- Приватність та Конфіденційність:

Анонімізація даних: Забезпечення анонімізації особистих даних для збереження приватності користувачів під час аналізу.

Безпека даних: Захист від несанкціонованого доступу до даних, щоб уникнути ризиків порушення конфіденційності.

- Покращення ефективності:

Оптимізація процесів: Використання алгоритмів та технологій, щоб зменшити кількість ложнопозитивних та ложнонегативних результатів.

Інтеграція з іншими системами: Системи моніторингу можуть інтегруватися з іншими платформами, такими як обмінники криптовалют або електронні гаманці, для збільшення ефективності.

Системи моніторингу та аналізу транзакцій відіграють критичну роль у забезпеченні безпеки та дотриманні вимог законодавства в сфері криптовалют та віртуальних валют, зокрема щодо запобігання фінансовому шахрайству, відмиванню грошей і фінансуванню тероризму.

5. Обмеження доступу до API:

Обмеження доступу до API (інтерфейсу програмування застосунків) є важливою складовою забезпечення безпеки та ефективного використання веб-сервісів та додатків. Тут подано більш детальний огляд основних аспектів обмеження доступу до API:

- Ключі API:

Аутентифікація: Багато API використовують ключі для аутентифікації клієнтів. Це може бути унікальний ідентифікатор, який надається користувачеві для доступу до конкретного API.

Публічні та приватні ключі: Деякі API надають різні рівні доступу, такі як публічні та приватні ключі. Публічні ключі можуть бути відкритими, але приватні ключі використовуються для авторизованого доступу.

- Обмеження швидкості запитів (Rate Limiting):

Контроль частоти: Обмеження кількості запитів, які клієнт може виконати за певний період часу. Це запобігає надмірному використанню ресурсів та можливим атакам.

Оновлення швидкості: Деякі API надають можливість збільшувати або зменшувати ліміти швидкості в залежності від потреб користувача.

- Авторизація та Ролі:

Авторизація на рівні користувача: Деякі API дозволяють визначати ролі та рівні авторизації для кожного користувача або клієнта.

OAuth та інші механізми: Використання протоколів авторизації, таких як OAuth, для забезпечення безпеки при обміні обмеженими правами доступу.

- Обмеження за методами та URL-шляхами:

Доступ лише до певних методів: Контроль доступу до конкретних функцій або методів API, щоб користувачі отримували лише той функціонал, який їм потрібен.

Обмеження за шляхами URL: Визначення обмежень для конкретних URL-шляхів або ендпоінтів, які можна використовувати.

- Моніторинг та Журналювання:

Запис активності: Запис подій та активності, пов'язаної з API, для подальшого аналізу та виявлення незвичайної активності.

Моніторинг швидкості: Системи можуть моніторити швидкість та обсяги запитів для виявлення відхилень від звичайного.

- SSL/TLS та Шифрування:

Безпечний обмін даними: Використання захищеного з'єднання з допомогою протоколів SSL/TLS для зашифрування даних, що передаються між клієнтом і API.

Підписання запитів: Використання методів підпису та шифрування для перевірки цілісності та автентифікації запитів.

- Інтеграція з іншими ідентифікаційними системами:

SSO (Single Sign-On): Інтеграція з системами одноразового входу для спрощення управління правами доступу.

LDAP або інші директорії: Використання ідентифікаційних директорій для управління доступом та ролями користувачів.

Обмеження доступу до API важливе для забезпечення безпеки, конфіденційності та ефективності використання веб-сервісів. Враховуючи ці принципи, розробники можуть створювати надійні та безпечні системи взаємодії між програмами.

Ми розглянули основні технологічні засоби виявлення ризиків, які використовує майже кожен користувач даної сфери. Ці технологічні рішення разом утворюють

комплексний підхід до виявлення та запобігання ризикам в області віртуальної валюти. Однак важливо пам'ятати, що цей ландшафт постійно змінюється, і необхідно постійно вдосконалювати технічні рішення для вирішення нових викликів і загроз.

2.2. Аналіз стану ринку віртуальних валют

Термін «цифрова валюта» є найбільш узагальненим поняттям, що має на увазі особливу нематеріальну форму існування валюти у цифровій (електронній) формі. Оскільки дані про грошові потоки зберігаються на віддалених серверах, для здійснення операцій та взаємодії з цим видом валюти необхідний доступ до Інтернету або іншої мережі, що забезпечує взаємодію електронних гаманців. Цифрові валюти немає внутрішньої вартості — вони лише відбивають еквівалент коштів, депонованих на балансі емітента, чи, інакше, право вимоги проти надання коштів. Однак цей вид валюти часто призначений для оплати товарів та послуг у певних інтернет-магазинах, сайтах та соціальних мережах [3].

Біткойн (Bitcoin):

- Капіталізація та ціна: Біткойн залишався найбільшою криптовалютою за капіталізацією на ринку та ціною. Його популярність як цифрового зберігача вартості і "цифрового золота" збільшувалася.
- Інституційний інтерес: Великі фінансові установи, інвестиційні фонди та корпорації почали виявляти інтерес до біткойну. Деякі з них включали біткойн до своїх інвестиційних портфелів, що дало криптовалюті додаткову легітимність.
- Регулювання: Збільшилася увага до регулювання криптовалют. Різні країни проводили дискусії щодо створення або адаптації регуляторних рамок для криптовалютних операцій та біткойну як активу.

Щоб більш наочно показати коливання ціни біткоіна, графік руху ціни з 2014 року по теперішній час зображено на лінійній діаграмі. Виходячи з мал. 1, ціна біткойна демонструє загальну тенденцію до зростання з 2014 року,
особливо за останні два роки, коли ціна різкіше коливалася. Від таблиці, можна виявити, що є три значні коливання ціни. 1. У третьому кварталі 2017 року він став першим висхідним кульмінаційним моментом і почав знижуватися після досягнення найвищого значення на початку січня 2018 р. 2. На початку листопада 2020 р. це поклало початок стрімкій тенденції зростання з 13 737,11 доларів США 1 листопада 2020 року до 63 503,46 доларів США 13 квітня 2021 року, і швидко впала приблизно до 30 000 доларів США. 3. Після досягнення дна в липні, на новий раунд почалося зростання, яке досягло свого піку 8 листопада 2021 року, а потім стрімко впало до приблизно знову 40 000 доларів із меншою волатильністю цін у першому кварталі 2022 року. Коливання цін на біткойни мають чіткий зв’язок з державними та міжнародними політичні та економічні ситуації та її унікальні атрибути.

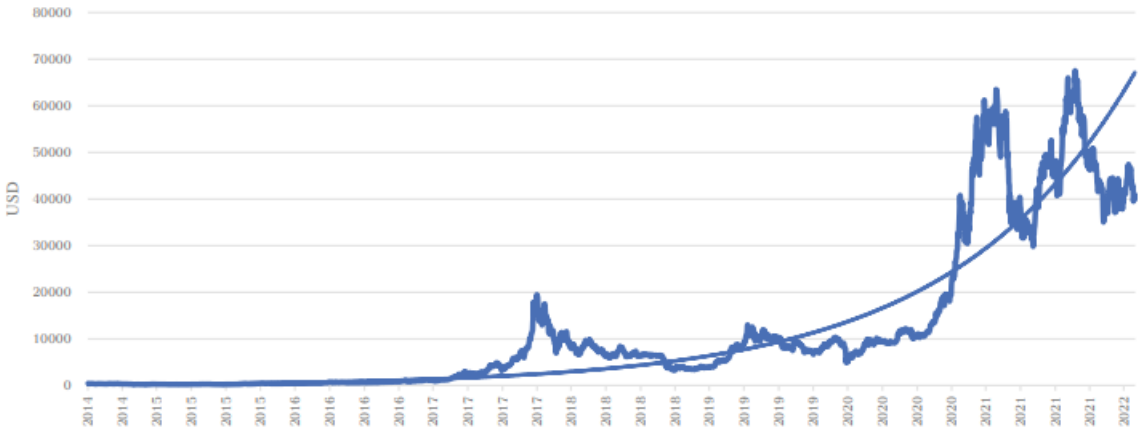

Рис 2.1. Цінова динаміка біткоіна з 2014 по 2022 рік[8]

Ефір (Ethereum):

- Ethereum 2.0: Очікування на ефір було пов'язане з переходом на Ethereum 2.0, що передбачає перехід на Proof-of-Stake. Це мав позитивний вплив на довгострокові перспективи ефіріуму.

- DeFi: Проекти у сфері децентралізованих фінансів (DeFi) на платформі Ethereum зростали. Укладання грамотних угод та розширення фінансових послуг на базі блокчейну призводили до збільшення обсягу замовлень та ліквідності.

Децентралізовані фінанси (DeFi):

- Збільшення обсягу залучених коштів: DeFi ставав все популярнішим, і обсяг залучених коштів у цьому секторі зростав. Проекти, такі як Aave, Compound, і MakerDAO, надавали різноманітні фінансові послуги без потреби в інтермедіарах.
- Ризики та безпека: За зростанням DeFi стояли і ризики, пов'язані з безпекою смарт-контрактів та аспектами управління ризиками.

Невзаємозамінні токени (NFT):

- Мистецькі та культурні застосування: Ринок невзаємозамінних токенів (NFT) зростав завдяки великому інтересу до цифрових мистецьких та культурних активів.
- Ігри та віртуальна власність: NFT також використовувались в галузі віртуальних ігор та віртуальної власності, створюючи нові можливості для творців контенту та гравців.

Регулювання:

- Різноманіття підходів: Різні країни демонстрували різноманітні підходи до регулювання криптовалют. Деякі країни визнавали їх як легальні засоби платежу, тоді як інші встановлювали обмеження або намагалися створити більш прозорі правила.

Технологічні інновації:

- Layer 2 рішення: Виникли різні технологічні інновації, такі як Layer 2 рішення, які спрямовувалися на вирішення проблем масштабованості блокчейнів та зниження вартості транзакцій.
- Розвиток приватних блокчейнів: Деякі підприємства досліджували можливості використання блокчейну для оптимізації своїх процесів, особливо в області логістики та постачання.

Таким чином, стан ринку віртуальних валют відображає велику динаміку та різноманітність подій, які впливали на його розвиток. Ці тенденції можуть змінюватися в залежності від розвитку технологій, змін у регулюванні та глобальних економічних умов.

2.3 Правове регулювання та нормативи

На сьогоднішній день багато країн вивчають та розробляють правове регулювання в галузі використання віртуальних валют, таких як Bitcoin та інші криптовалюти. Технології виявлення ризиків використання віртуальних валют у транзакціях стають важливим елементом регулювання цього сегменту фінансового ринку.

Україна не є «першопрохідцем», а всього лише впроваджує рекомендації FATF, які вже діють у багатьох країнах світу. У зв’язку з цим Україна мала вибір: заборонити криптовалюти або впровадити відповідне регулювання. Україна вибрала другий варіант. Розкриваючи обране для дослідження питання, уважаємо за доцільне зауважити, Юридичний науковий електронний журнал що сьогодні міжнародною спільнотою не винайдено єдиних уніфікованих підходів до регулювання обігу криптовалют. Це зумовлено тим, що нині світові фінансові установи й центральні банки держав не сформували системного підходу до використання віртуальних валют, водночас акцентуючи увагу міжнародної спільноти на тому, що використання віртуальних валют потребує належного моніторингу та осмислення з боку державних регуляторів; окрім того,

Європейський центральний банк у дослідженнях щодо віртуальних цифрових валют «Virtual currency schemes – a further analysis» не висловлює однозначної позиції щодо використання віртуальних валют, застерігаючи про ризики забезпечення безпеки платежів і потенційні загрози в розрахункових операціях [12].

Нижче наведено деякі загальні аспекти правового регулювання та нормативів, які можуть визначати використання віртуальних валют:

AML (Боротьба з відмиванням грошей):

Багато країн включають віртуальні валюти в свої антимонопольні та антитерористичні закони. Обмінники криптовалют, як правило, повинні дотримуватися правил ідентифікації клієнта (KYC) та подавати звіти про транзакції, які можуть бути використані для виявлення потенційно незаконних дій.

Ліцензування обмінників криптовалют:

Деякі країни вимагають, щоб обмінники криптовалют отримували спеціальні ліцензії для своєї діяльності. Це може включати в себе вимоги до капіталу, стандартів безпеки, а також дотримання законів про боротьбу зі злочинністю.

KYC (Знай свого клієнта):

Вимоги до KYC означають, що учасники ринку криптовалют повинні збирати та зберігати інформацію про своїх клієнтів, таку як ім'я, адреса та інші особисті дані. Це допомагає попереджати анонімні транзакції та виявляти небезпечних клієнтів.

ICO (Перший випуск монет):

Деякі країни встановлюють правила для організаторів ICO, такі як обов'язкова реєстрація та дотримання вимог щодо видачі токенів. Це може включати в себе вимоги до розкриття інформації та захисту інвесторів.

Податкове законодавство:

Податкове облік криптовалют може значно відрізнятися в різних країнах. Деякі країни визначають криптовалюти як майно, тоді як інші можуть розглядати їх як валюту. Важливо визначити податковий статус криптовалют у вашій конкретній юрисдикції.

Міжнародне співробітництво:

У зв'язку з глобальним характером криптовалют, міжнародне співробітництво стає ключовим елементом для боротьби зі злочинністю та забезпечення ефективного регулювання.

Загальний тренд полягає в тому, що багато країн поступово пристосовують своє законодавство для врахування впливу криптовалют на фінансову систему та боротьби з можливими ризиками. Однак правове регулювання все ще еволюціонує, і важливо слідкувати за змінами в законодавстві та нормативах у вашій конкретній країні.

Розділ 3. ІННОВАЦІЙНІ ПІДХОДИ ДО ВИЯВЛЕННЯ ТА УПРАВЛІННЯ РИЗИКАМИ ВІРТУАЛЬНОЇ ВАЛЮТИ

3.1 Реалізація методів виявленя шахрайства у віртуальній валюті

Виявлення шахрайства у віртуальній валюті включає в себе використання різних методів і інструментів для виявлення аномалій, несправедливих дій або інших ознак маніпуляцій. Щоб реалізувати методи виявлення шахрайства у віртуальній валюті нам необхідно визначити ситуацію в якій ми знаходимося. Наприклад, ми замовили якусь послугу і маємо її оплати через віруальний гаманець. Адресу гаманця ми отримаємо від виконавця з назвою валюти USDT та мережею TRON(TRC20), як наприклад це буде адреса –

TVfP2yXw9GD8p8vt59CsD5vPm69usuWhT3

Для початку нам необхідно отримати історію транзакцій по даній адресі, це ми можемо зробити через відомі API або використати будь-який сайт, що підтримує змогу пошуку інформації по адресі гаманця або назві аккаунту. Оберемо офіційний tronscan.org в якому вводимо адресу гаманця у пошук і отримуємо всю інформацію про транзакції зв’язані з даним гаманцем, що можемо бачити на малюнку 3.1.

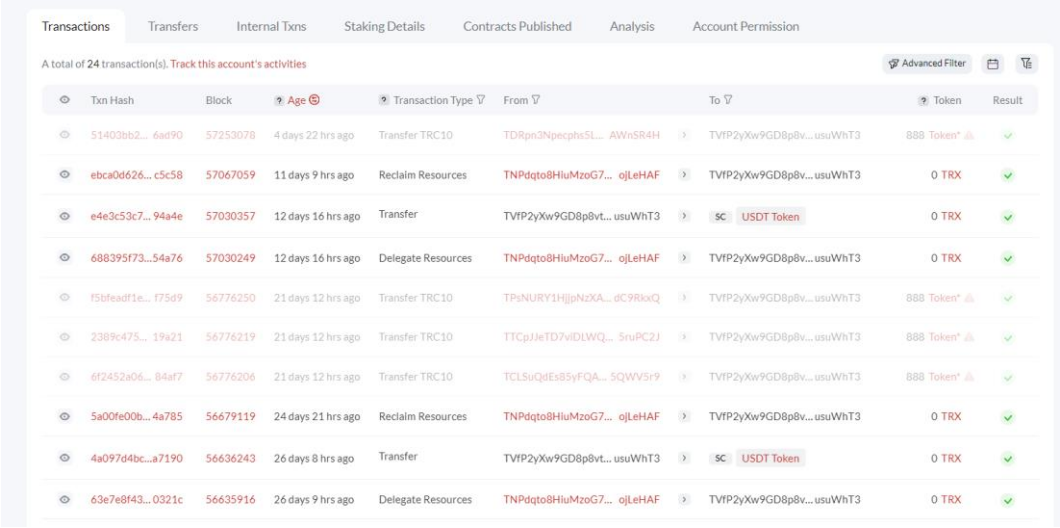

Рис 3.1. Приклад отриманої інформації з ресурсу Tronscan

Далі використовуючи даний ресурс, завантажуємо csv файл з усіма транзакціями гаманця і тепер можемо їх використовувати у виявлені аномалій чи шахрайства. В отриманому csv файлі ми маємо таблицю зі стовбцями: Txn Hash, Block, Time(UTC), From, To, Token, Token Symbol, Amount/TokenID, Result, Status. Інформацію за цими даними ми можемо передивитися в таблиці 3.1.

Таблиця 3.1.

Інформацію про транзакції в блокчейні або системі

Назва	Опис
Txn Hash (Хеш транзакції)	Унікальний ідентифікатор транзакції в блокчейні, який гарантує її унікальність та неперевіреність.
Block (Блок)	Номер блоку, в якому знаходиться транзакція.

Time (UTC) (Час в універсальному часі)	Час виконання транзакції у всесвітньому часі (UTC).
From (Відправник)	Адреса чи ідентифікатор облікового запису, з якого була відправлена транзакція.
To (Отримувач)	Адреса чи ідентифікатор облікового запису, на який була відправлена транзакція.
Token (Токен)	Інформація про токен, який був переданий у цій транзакції.
Token Symbol (Символ токена)	Символ або скорочене позначення токена.
Amount/TokenID (Сума/Ідентифікатор токена)	Кількість токенів, які були передані в цій транзакції, або ідентифікатор токена.
Result (Результат)	Результат виконання транзакції, може бути успішним чи неуспішним.
Status (Статус)	Статус транзакції, який також може вказувати на успішне або неуспішне виконання.

Розглянемо кілька загальних методів виявлення аномалій по отриманим даним:

Виявлення шахрайства в часі транзакції може бути складним завданням і залежить від конкретних особливостей отриманих даних. Однак, ми можемо

поєднати декілька методі, які можуть допомогти нам виявити потенційно шахрайські транзакції.

Почнемо з часу, наведу приклад коду на python з використанням бібліотек: pandas та matplotlib.

```
import pandas as pd
import matplotlib.pyplot as plt

data = pd.read_csv('Transfers_20231217.csv')

# Переформуємо стовбчик з  часом в форматі datetime
data['Time(UTC)'] = pd.to_datetime(data['Time(UTC)'])

# сотруємо
data = data.sort_values(by='Time(UTC)')

# Розрахунок часових інтервалів транзакцій
data['TimeDelta'] = data['Time(UTC)'].diff().dt.total_seconds()

print(data[['Time(UTC)', 'TimeDelta']])

# Построение графика временных интервалов
plt.figure(figsize=(12, 6))
plt.plot(data['Time(UTC)'], data['TimeDelta'], marker='o', linestyle='-', color='b')
plt.title('Часові інтервали між транзакціями')
plt.xlabel('Час транзакцій (UTC)')
plt.ylabel('Інтервал (секунди)')
plt.xticks(rotation=45)
plt.tight_layout()
plt.show()
```

Отриманий результат можемо побачити на малюнку 3.2.

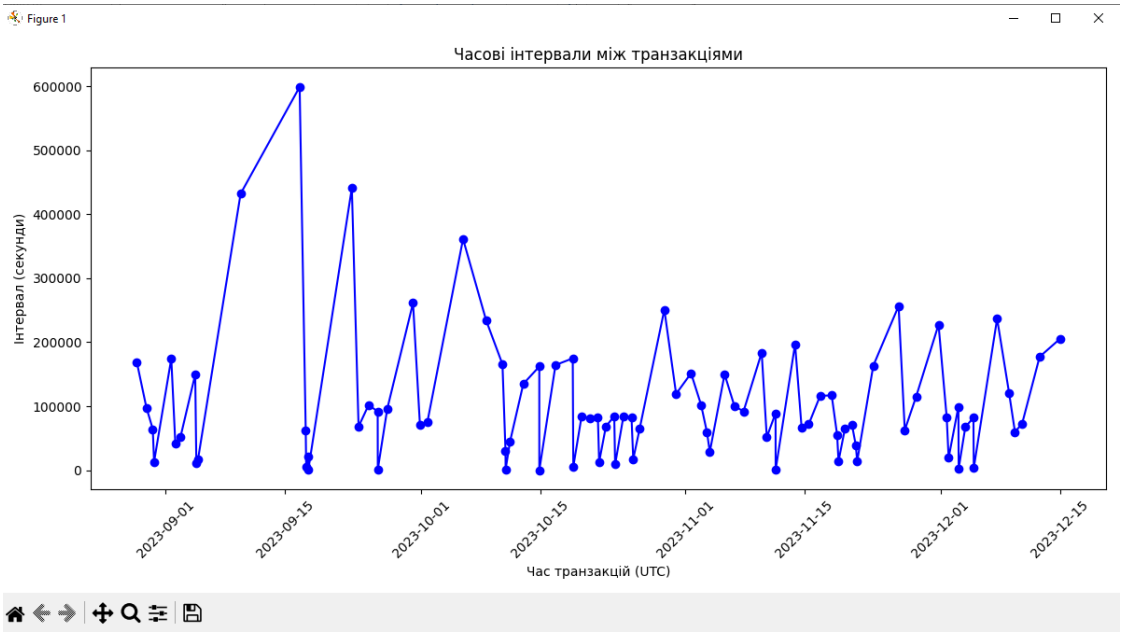

Рис 3.2. Часові інтервали між транзакціями

Графік тимчасових інтервалів між транзакціями може допомогти виявити аномалії у патернах часу між транзакціями. Якщо є великий стрибок на графіку, це може бути ознакою незвичайної події чи шахрайської активності.

Рівномірні інтервали:

Якщо графік показує рівномірні часові інтервали між транзакціями, це може бути ознакою нормальної активності без аномалій.

Великі стрибки:

Великі стрибки у графіку можуть вказувати на незвичайні події чи моменти шахрайства. Наприклад, раптове збільшення часового інтервалу може вказувати на перерву активності або масову зміну образу дій.

Маленькі інтервали:

Маленькі інтервали між транзакціями можуть бути ознакою аномальної активності, якщо вони різко відрізняються від звичайних патернів.

Циклічність або патерни:

Якщо є циклічність або повторювані патерни у графіку, це може бути ознакою регулярної активності або, навпаки, спроб приховування шахрайської діяльності.

Аномальні точки:

Зверніть увагу на точки з аномально більшими інтервалами між транзакціями. Це можуть бути моменти, які потребують додаткової уваги.

Комбінація з іншими ознаками:

Рекомендую аналізувати графік у поєднанні з іншими ознаками, такими як сума транзакцій, тип транзакції та інші. Комбінований аналіз може посилити спроможність виявлення шахрайства.

Далі ми можемо додати в графік суми транзакцій щоб співставити з часовими інтервалами. Додамо наступні рядки у код:

```
ax2 = ax1.twinx()
ax2.plot(data['Time(UTC)'], data['Amount/TokenID'], marker='x', linestyle='-', color='r', label='Amount/TokenID')
ax2.set_ylabel('Сума транзакцій', color='r')
ax2.tick_params('y', colors='r')
```

Як результат ми отримуємо графік порівняння сумм транзакцій, отриманий результат можемо побачити на малюнку 3.3.

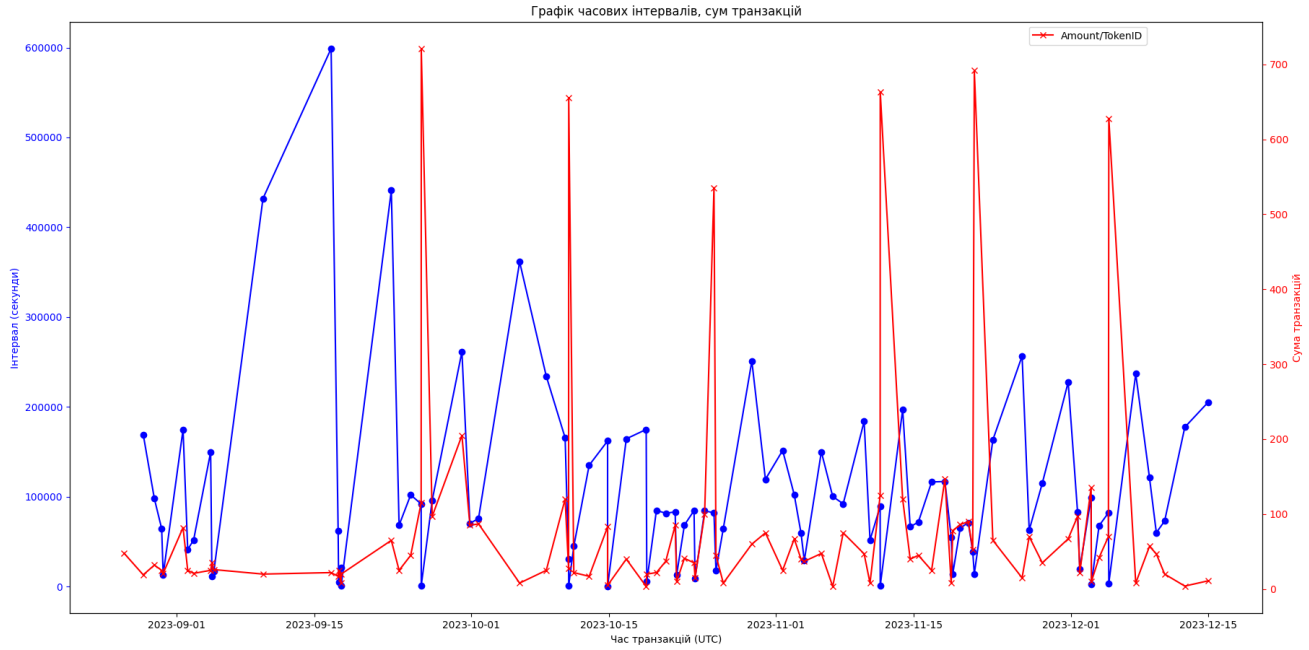

Рис 3.3. Графік співвідношення часу та сум транзакцій

Як результат, бачимо, що великі стрибки в графіку не пересікаються і це каже нам про те що даний гаманець малоймовірно може бути шахрайським. Але для більшої точності слід додати багато аспектів та використання великих ресурсів. Зверніть увагу, що ця ідея є загальним підходом, і ефективність може залежати від специфіки даних і конкретних характеристик вашої програми. Можливо, також буде корисним використання алгоритмів машинного навчання для виявлення аномалій або моделей часових рядів, особливо якщо у вас є великий обсяг даних та складні патерни шахрайства.

Вірогідний результат програми на шахрайство може бути приклад, який вказаний на малюнку 3.4.

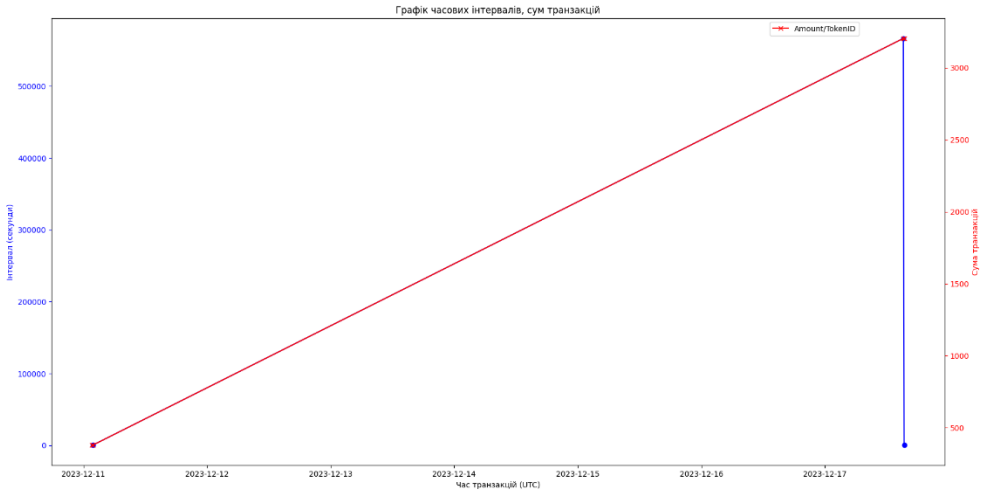

Рис 3.4. Можливий результат шахрайства

По графіку на малюнку 3.4. ми можемо побачити, що транзакції які приходили на даний гаманець одразу ж відправлялись в інше місце, тобто проходив можливий процес відмивання грошей.

Плюси:

Безпека:

- Захист від шахрайства: Виявлення аномалій дозволяє вчасно виявляти та запобігати шахрайським транзакціям.

Проактивність:

- Швидке реагування: Автоматичне виявлення аномалій дозволяє операторам систем швидко реагувати на можливі загрози.

Вдосконалення безпеки:

- Навчання систем: Використання алгоритмів машинного навчання дозволяє системі адаптуватися до нових видів атак та вдосконалювати ефективність виявлення.

Зменшення втрат:

- Мінімізація ризиків: Вчасне виявлення аномалій може допомогти зменшити втрати, пов'язані з шахрайством та іншими кримінальними діями.

Мінуси:

Ложні сигнали:

- Недостатність точності: Алгоритми можуть породжувати ложні сигнали, що призводить до неправильних санкцій або витрат ресурсів на перевірку невинних транзакцій.

Складність реалізації:

- Потреба в експертних знаннях: Виявлення аномалій вимагає розуміння як алгоритмів, так і сутностей, що працюють з віртуальною валютою.

Обмежена ефективність в анонімних мережах:

- Втручання в приватність: В анонімних криптовалютних мережах виявлення аномалій може порушити приватність користувачів.

Адаптація зловмисників:

- Зловмисники можуть адаптуватися: Криміналісти в постійній грі зі зловмисниками, які можуть шукати нові способи обійти системи виявлення аномалій.

Вартість розробки та підтримки:

- Витрати на технічну підтримку: Виявлення аномалій може вимагати значних витрат на розробку та підтримку адекватної інфраструктури та алгоритмів.

Всі ці аспекти повинні бути узгоджені для того, щоб ефективно використовувати системи виявлення аномалій в транзакціях віртуальної валюти.

3.2 Рекомендації запровадження мультипідписів та смарт контрактів для захисту транзакцій криптовалюти

Гаманці з розумними контрактами прокладають шлях до масового впровадження web3 — розблоковують нові потужні функції, які значно покращують роботу гаманця web3 як для існуючих учасників, так і для новачків. Сьогодні ні для кого не секрет, що прості гаманці ненадійні — більшість традиційних гаманців web3 (наприклад, MetaMask, Coinbase Wallet і Rainbow Wallet) є складними та ризикованими у використанні. Але завдяки тому, що

«розумні облікові записи» стали можливими, завдяки представленню Ethereum ERC-4337 (або абстракції облікового запису)[11], набагато більше людей вирішують надати своїм користувачам кращий досвід використання гаманців — звертаючись до різних типів гаманців із смарт-контрактами для різних випадків використання. Одним із тих типів гаманців web3, які набувають значної популярності, є гаманці Multisig (він же Multi-signature).

Впровадження мультипідписів (multisig) у сфері криптовалюти забезпечує додатковий рівень безпеки, що вимагає кількох ключів або підписів для підтвердження транзакції. Це запобігає втраті коштів у разі компрометації одного ключа чи пристрою. Важливо визначитися з типом мультипідписів, який найкраще відповідає вашим потребам. Наприклад, M-of-N мультипідписи дозволяють встановлювати, скільки N ключів необхідно для підтвердження транзакції.

M з N стосується розподілу ризику та згоди на використання ключа

По-перше: N означає кількість частин, а M — мінімальну кількість тих частин, які вам потрібні, щоб цей процес працював. Цифри можуть бути три з чотирьох. Або п’ять із 50. Ви можете розглядати це як частку або відсоток — незалежачи ні від чого. M з N — досить проста концепція. Ви берете щось, що має значну цінність — у цьому випадку це приватний ключ у парі відкритий-приватний ключ, і ви змушуєте групу людей брати участь у його використанні, а не лише одного.

Відповідно до компанії Thales (яка продає апаратні модулі безпеки), M of N також називають «контролем кількох осіб» або «автентифікацією на основі кворуму». Отже, двома ключовими елементами, властивими іменам, є більше ніж один (особа, як власник ключа) і «посередники». Ключові моменти тут полягають у тому, що у вас є набір ключів, і вам потрібно досягти узгодженого рішення людей, які тримають ключі, для доступу.

Розглянемо приклад створення 2-of-3 мультипідпису з використанням біткоін-гаманця Electrum:

Установка Electrum:

Завантажуємо та встановлюємо Electrum з офіційного сайту. Переконуємося, що завантажуємо програмне забезпечення лише з офіційного джерела, щоб уникнути підроблених версій.

Запускаємо Electrum та створюєм новий гаманець. Вибераєм "Create a new wallet" та дотримуємось інструкцій. Далі у меню обираємо "Wallet" -> "Multisig Wallet" -> "Create" та обираємо потрібний тип мультипідпису (наприклад, 2-of-3).

Electrum надасть нам опцію для створення ключів мультипідпису. Можемо використовувати інтегрований генератор ключів або ввести свої попередньо згенеровані ключі. Маємо змогу обрати до 15 частин ключів і такої самої кількості необхідних ключів для підтвердження, що можемо бачити на малюнку 3.5.

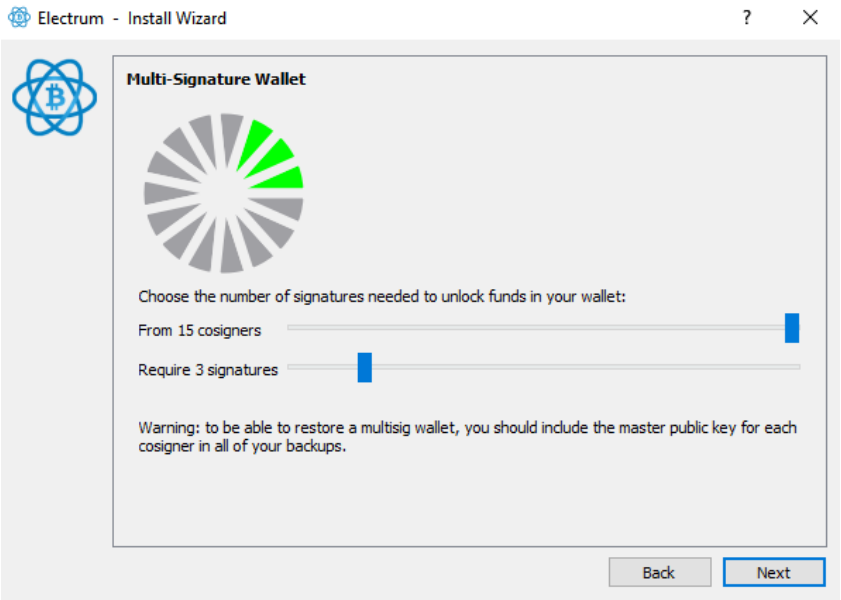

Рис 3.5. Налаштування мультипідписів у біткоін-гаманці Electrum

Отримані ключі розподіляємо на вимогу нашої безпеки. Обов'язково треба зберігати резервні копії ключів у безпечних місцях. Коли готові надіслати транзакцію, вибераємо "Send" і заповнюємо деталі транзакції. Підписуємо транзакцію за допомогою 3 із 15 ключів. Уважно моніторимо наш мультипідписний гаманець. У разі втрати одного з ключів негайно оновлюємо налаштування мультипідпису.

Обов’язково перед використанням на реальних сумах треба провести кілька тестових транзакцій, щоб упевнитися у правильності налаштувань.

Багатопідписний гаманець працює, використовуючи комбінацію криптографічних підписів і логіки смарт-контракту. Коли пропонується транзакція, вона зберігається в розумному контракті гаманця разом із необхідною кількістю підписів. Коли підписанти надають свої підписи, смарт-контракт перевіряє їх на відповідність відкритим ключам уповноважених сторін.

Коли транзакція ініціюється, вона транслюється підписантам, які потім підписують її за допомогою своїх особистих ключів. Потім смарт-контракт перевіряє, чи зібрано необхідну кількість підписів. Якщо умова виконується, транзакція вважається дійсною і може бути виконана в блокчейні. В іншому випадку він залишається на розгляді, доки не будуть зібрані необхідні погодження.

Після збору та перевірки необхідних підписів смарт-контракт виконує транзакцію. Якщо транзакція передбачає передачу активів, вона відповідно оновлює баланс гаманця. У разі виклику функції до іншого смарт-контракту смарт-контракт гаманця з кількома підписами перенаправляє виклик до цільового контракту.

Цей механізм у гаманцях з кількома підписами забезпечує ефективні варіанти використання, які зазвичай неможливі в традиційних гаманцях web3.

Розумні контракти

Розумні контракти – це програмні коди, які автоматизують, контролюють та виконують умови угоди в рамках блокчейн-мережі. Вони часто використовуються в криптовалютних системах, таких як Ethereum для виконання складних смарт-контрактів. Ось детальніший розгляд розумних контрактів:

1. Вибір Платформи:

Визначтеся з блокчейн-платформою для розгортання розумних контрактів. Ethereum є однією з найпопулярніших платформ для розумних контрактів, але також існують інші, такі як Binance Smart Chain, Solana та інші.

2. Розробка Контракту:

Використовуйте мову програмування, яку підтримує обрана платформа (наприклад, Solidity для Ethereum), для написання коду розумного контракту. Контракт може визначати правила та умови угоди, включаючи транзакції та взаємодію з іншими контрактами.

3. Аудит Коду:

Проведіть аудит коду розумного контракту, щоб виявити потенційні вразливості та помилки. Це важливо, оскільки помилки у розумних контрактах можуть призвести до серйозних наслідків, включаючи втрату коштів.

4. Розгортання в Тестовій Мережі:

Перед розгортанням розумного контракту в основній мережі блокчейна проведіть тестування в тестовій мережі. Це дозволяє уникнути проблем, пов'язаних із несподіваною поведінкою контракту у бойових умовах.

5. Управління Угодою:

Переконайтеся, що контракт включає всі необхідні умови угоди, і передбачте механізми зміни цих умов у майбутньому, якщо це необхідно.

6. Безпека та Захист:

Уважно слідкуйте за безпекою розумного договору. Використовуйте стандарти безпеки (наприклад, ERC-20 для токенів), запобігайте можливим атакам (наприклад, рекентрантні атаки), та забезпечуйте безпеку даних користувача.

7. Резервні Копії та Відновлення:

Регулярно створюйте резервні копії розумних контрактів та передбачте механізми відновлення у разі невдачі чи критичної помилки.

8. Оновлення Контрактів:

Якщо виникає потреба у оновленні контракту, передбачте механізми оновлення з урахуванням безпеки та узгодження з учасниками контракту.

9. Моніторинг та Журналування:

Введіть систему моніторингу для відстеження активності розумних контрактів та журналування для реєстрації важливих подій.

10. Освіта Користувачів:

Навчіть користувачів та інші зацікавлені сторони, як взаємодіяти з розумними контрактами, щоб уникнути помилок і дотримуватися безпеки.

11. Розробка Фронтенду:

Якщо ваш розумний контракт призначений для взаємодії з користувачем, розробіть відповідний інтерфейс (фронтенд), який забезпечує зручність використання.

12. Дотримання Законодавства:

Переконайтеся, що ваш розумний контракт та його використання відповідають законодавству країн, де він буде використовуватися.

Приклад розумного договору (на Solidity, для Ethereum):

ERC-20 (стандарт токена Ethereum)

```
pragma solidity ^0.8.0;
contract SimpleToken {
    string public name = "SimpleToken";
    string public symbol = "ST";
    uint256 public totalSupply = 1000000;
    mapping(address => uint256) public balanceOf;
    constructor() {
        balanceOf[msg.sender] = totalSupply;
    }
    function transfer(address to, uint256 amount) external {
        require(balanceOf[msg.sender] >= amount, "Insufficient balance");
        balanceOf[msg.sender] -= amount;
        balanceOf[to] += amount;
    }
}
```

Це простий приклад контракту, який є простим токеном ERC-20. Цей договір містить базову логіку передачі токенів між адресами. Перед використанням подібних контрактів у реальних умовах необхідно провести ретельне тестування та аудит для забезпечення безпеки та коректності роботи.

Плюси:

Безпека:

- Мультипідписи: Забезпечують додатковий рівень безпеки, оскільки потрібні підписи від кількох ключів для підтвердження транзакції.
- Смарт-контракти: Вони можуть використовувати умови та логіку, щоб автоматично виконувати або блокувати транзакції в залежності від певних умов.

Керованість:

- Мультипідписи: Дозволяють розділити керованість між кількома особами або організаціями.
- Смарт-контракти: Можуть автоматизувати різні аспекти угоди без потреби в посередниках.

Захист від шахрайства:

- Мультипідписи: Ускладнюють спроби шахрайства та недозволеного доступу до коштів.
- Смарт-контракти: Зменшують ризик обману, оскільки їх виконання автоматизоване та безпосереднє.

Мінуси:

Складність реалізації:

- Мультипідписи: Вимагають співпраці всіх сторін для встановлення і використання.
- Смарт-контракти: Вимагають високого рівня програмування та аудиту для уникнення помилок та безпекових порушень.

Вартість транзакцій:

- Мультипідписи: Зазвичай збільшують вартість транзакцій через додаткові обчислення та зберігання ключів.
- Смарт-контракти: Викликають витрати на обчислення та газ (для платформ, які використовують концепцію газу).

Небезпека помилок:

- Мультипідписи: Існує ризик втрати доступу до коштів у випадку втрати одного чи декількох ключів.
- Смарт-контракти: Неправильне програмування може призвести до втрати коштів через помилкове виконання умов.

Залежність від технічних знань:

- Мультипідписи: Вимагають від користувачів розуміння процесу підпису та безпеки ключів.
- Смарт-контракти: Потрібно розуміти програмування та криптографію для безпечного використання.

Впровадження цих технологій вимагає уважного аналізу конкретних вимог та умов і може бути корисним засобом для забезпечення безпеки та контролю в області криптовалютних транзакцій.

3.3 Рекомендації щодо впровадження машинного навчання для захисту транзакцій віртуальної валюти

Впровадження машинного навчання (ML) для захисту транзакцій віртуальної валюти є критично важливим у сучасному цифровому середовищі, де кіберзлочинці намагаються використовувати різноманітні технології для несанкціонованого доступу та шахрайства.

Машинне навчання — це підгалузь штучного інтелекту, яка широко визначається як здатність машини імітувати інтелектуальну поведінку людини. Системи штучного інтелекту використовуються для виконання складних завдань у спосіб, подібний до того, як люди вирішують проблеми. Мета штучного інтелекту полягає в тому, щоб створити комп’ютерні моделі, які демонструють «розумну поведінку», як люди. Це означає машини, які можуть розпізнавати візуальну сцену, розуміти текст, написаний природною мовою, або виконувати дію у фізичному світі. Машинне навчання є одним із способів використання ІІ. Але в деяких випадках написання програми, якою слідує машина, займає багато часу або є неможливим, наприклад, навчити комп’ютер розпізнавати зображення різних

людей. Хоча люди можуть легко виконати це завдання, важко вказати комп'ютеру, як це зробити. Машинне навчання використовує підхід, який дозволяє комп'ютерам навчитися самостійно програмувати через досвід.

Комп'ютерам більше не потрібно покладатися на мільярди рядків коду для виконання обчислень. Машинне навчання дає комп'ютерам силу неявних знань, які дозволяють цим машинам встановлювати зв'язки, виявляти закономірності та робити прогнози на основі того, що вони навчилися в минулому. Використання неявних знань у машинному навчанні зробило його популярною технологією майже для всіх галузей, від фінтех до погоди та державного управління.[10]

Машинне навчання починається з даних — чисел, фотографій або тексту, наприклад банківських транзакцій, фотографій людей або навіть будь-яких виробів, записів про ремонт, даних часових рядів із датчиків або звітів про продажі. Дані збираються та готуються для використання як навчальні дані або інформація, на основі якої навчатиметься модель машинного навчання. Чим більше даних, тим краще програма. Звідти програмісти вибирають модель машинного навчання для використання, надають дані та дозволяють комп'ютерній моделі навчитися знаходити закономірності чи робити прогнози. Згодом програміст також може налаштувати модель, зокрема змінити її параметри, щоб підштовхнути її до більш точних результатів. Деякі дані витягуються з навчальних даних, які використовуються як дані оцінки, які перевіряють, наскільки точна модель машинного навчання, коли їй показуються нові дані. Результатом є модель, яку можна використовувати в майбутньому з різними наборами даних.

Типи Машинного Навчання:

- Наглядоване навчання (Supervised Learning): Використовується для навчання моделі на основі маркованих даних, де кожна транзакція має відомий вихід. Це дозволяє системі визначати стандартні та аномальні патерни.
- Ненаглядоване навчання (Unsupervised Learning): Використовується для виявлення аномалій без попереднього маркування даних. Модель навчається визначати відмінності та виявляти непередбачувані зразки.

Методи Виявлення Аномалій:

- Статистичні методи: Використовуються для порівняння активності зі статистичною моделлю нормальної поведінки.
- Методи кластеризації: Групують схожі транзакції та виявляють аномалії в транзакціях, які відрізняються від інших груп.
- Методи глибинного навчання: Використовують нейронні мережі для виявлення складних патернів, що можуть вказувати на аномалії.

Застосування Машинного Навчання в Кібербезпеці:

- Автоматизоване виявлення загроз: Машинне навчання може автоматично реагувати на нові види атак, не вимагаючи ручного втручання.
- Прогнозування ризиків: Аналізуючи різні фактори транзакцій, система може прогнозувати рівень ризику для кожної операції.

Виклики та Переваги:

- Необхідність великої кількості даних: Ефективне навчання моделей вимагає значної кількості маркованих або немаркованих даних.
- Збалансованість між точністю та ложнопозитивними результатами: Важливо збалансувати модель так, щоб вона ефективно реагувала на аномалії, не ведучи при цьому до надмірної кількості ложнопозитивних випадків.

Врахування цих аспектів допоможе створити дієву систему захисту транзакцій віртуальної валюти, забезпечуючи високий рівень кібербезпеки у цьому сфері.

Машинне навчання збирає вхідні дані, які можуть бути даними, зібраними під час тренінгів або з інших джерел, таких як пошукові системи наборів даних, веб-сайти .gov і реєстри відкритих даних, як-от Amazon Web Services. Ці дані виконують ту саму функцію, що й попередній досвід для людей, надаючи моделям машинного навчання історичну інформацію, з якою можна працювати під час прийняття майбутніх рішень. Потім алгоритми аналізують ці дані, шукаючи

закономірності та тенденції, які дозволяють робити точні прогнози. Таким чином, машинне навчання може отримати інформацію з минулого, щоб передбачити майбутні події. Як правило, чим більший набір даних може надати команда програмному забезпеченню машинного навчання, тим точніші прогнози. Ідея полягає в тому, що алгоритми машинного навчання повинні мати можливість виконувати ці завдання самостійно, вимагаючи мінімального втручання людини. Це прискорює різні процеси, оскільки машинне навчання автоматизує багато аспектів різних галузей.

Розглянемо прикладну модель машинного навчання для виявлення шахрайських транзакцій у мережі Ethereum.

Кроки:

1. Збір даних:

Зберемо дані про транзакції Ethereum, включаючи інформацію про суму, відправника, одержувача, газ та інші характеристики транзакцій. Важливо мати дані про транзакції, що включають як легітимні, так і шахрайські операції.

2. Підготовка даних:

Проведемо попередню обробку даних, включаючи масштабування, заповнення пропущених значень, перетворення категоріальних ознак, якщо є.

3. Поділ на Навчальний та Тестовий Набори:

Розділимо дані на навчальний та тестовий набори для навчання та валідації моделі.

4. Вибір Моделі:

Виберемо модель машинного навчання. Можливі варіанти включають логістичну регресію, випадковий ліс, градієнтний бустинг та нейронні мережі. Ми можемо почати, наприклад, з використанням випадкового лісу.

5. Навчання Моделі:

Навчимо модель на навчальному наборі, використовуючи розмічені дані. Мітки вказуватимуть на легітимні та шахрайські транзакції.

6. Оцінка Моделі:

Оцінимо продуктивність моделі на тестовому наборі, використовуючи метрики, такі як точність, повнота, F1 міра. Ми також можемо використати матрицю помилок для більш детального аналізу продуктивності.

7. Налаштування Гіперпараметрів:

Якщо необхідно, проведемо налаштування гіперпараметрів моделі для покращення її продуктивності.

8. Розвиток системи відстеження:

Розгорнемо систему відстеження транзакцій у реальному часі, де нові транзакції будуть аналізуватись моделлю машинного навчання. У разі виявлення шахрайської транзакції система може спрацьовувати сигнал тривоги або автоматично блокувати транзакцію.

9. Регулярне Оновлення Моделі:

Регулярно оновлюємо модель з урахуванням нових даних та змін у патернах шахрайства.

10. Впровадження Додаткових методів захисту:

Крім моделі машинного навчання, впровадимо додаткові методи захисту, такі як двофакторна автентифікація, багаторівневі перевірки та білі/чорні списки адрес.

11. Навчання на реальних даних:

Навчимо модель на реальних даних транзакцій та регулярно оновлюємо її з урахуванням змін у криптовалютному середовищі.

12. Регулярні Аудити та Моніторинг:
Проводимо регулярні аудити моделі, моніторимо її продуктивність та вживаємо заходів щодо покращення при необхідності.

Цей підхід до використання машинного навчання для захисту транзакцій криптовалюти передбачає створення ефективної моделі, безперервне навчання, адаптацію нових видів шахрайства та комбінацію з іншими методами безпеки для створення комплексної системи захисту.

Припустимо, у нас є набір даних transactions.csv з такими стовпцями: amount, frequency, та label (1 - нормально, -1 - аномально).

```
# Імпортуємо необхідні бібліотеки
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import IsolationForest
from sklearn.metrics import classification_report, confusion_matrix

# Завантажимо дані
data = pd.read_csv('transactions.csv')

# Розділімо дані на тренувальний та тестовий набори
X_train, X_test, y_train, y_test = train_test_split(data[['amount', 'frequency']], data['label'], test_size=0.2, random_state=42)

# Створимо та навчимо модель Isolation Forest
model = IsolationForest(contamination=0.01, random_state=42)  # contamination - частка аномальних спостережень
model.fit(X_train)
```

```
# Проведемо прогнози для тестового набору
predictions = model.predict(X_test)

# Оцінимо результати
print(confusion_matrix(y_test, predictions))
print(classification_report(y_test, predictions))
```

Цей код робить наступне:

1. Завантажує дані: Вам слід мати файл transactions.csv з відомостями про транзакції.
2. Розділяє дані: Тренувальний та тестовий набори даних розділяються для тренування та оцінки моделі.
3. Створює та навчає модель Isolation Forest: Модель Isolation Forest є однією з алгоритмів для виявлення аномалій у наборі даних.
4. Проводить прогнози та оцінює результати: Модель використовується для прогнозування аномалій у тестовому наборі, а результати оцінюються за допомогою матриці плутанини та звіту про класифікацію.

Цей код можна розширити, додавши додаткові функції та оптимізації в залежності від конкретних вимог та характеристик ваших даних.

ВИСНОВКИ

Магістерська робота висвітлює важливість розвитку технологій виявлення ризиків використання віртуальної валюти для забезпечення безпеки та легальності фінансових транзакцій. Результати досліджень можуть бути корисні для розробників фінтех-продуктів, регуляторів та інших учасників фінансового ринку у покращенні систем безпеки та виявлення незаконних дій у сегменті віртуальних валют. Отримані результати дозволяють визначити ключові аспекти, які можуть впливати на виявлення ризиків використання віртуальної валюти. Методи машинного навчання виявилися ефективними у виявленні аномальної поведінки, а аналіз блокчейн-даних надав можливість відстежувати та аналізувати транзакційні патерни.

Технології виявлення ризиків виявилися критичним елементом для забезпечення стійкості та надійності фінансових систем у контексті віртуальних валют. Швидкість зростання криптовалютного ринку робить їх важливим об'єктом дослідження та розробки ефективних заходів безпеки. Застосування методів машинного навчання, зокрема алгоритмів Isolation Forest, дозволяє ефективно виявляти аномалії у фінансових транзакціях з використанням віртуальних валют. Це розв'язання виявилося дуже ефективним у визначенні невиправданих ризиків та ідентифікації підозрілих патернів. Використання технології аналізу блокчейн-даних виявилося важливим для відстеження та аналізу транзакцій. Блокчейн надає прозору та невід'ємну історію транзакцій, що полегшує виявлення незвичайних патернів та здійснення ретроспективного аналізу. Використання контекстуального аналізу дозволяє персоналізувати систему виявлення ризиків відповідно до конкретного користувача чи групи користувачів. Це сприяє точнішому виявленню аномалій та зменшує кількість помилкових сигналів.

Ефективна система виявлення ризиків повинна включати в себе механізми співпраці з фінансовими регуляторами та іншими учасниками галузі. Це дозволяє швидко реагувати на нові тренди та зміни в сфері криптовалют.

Вивчення впливу смарт-контрактів на технологію виявлення ризиків вказує на необхідність адаптації аналітичних інструментів для урахування особливостей цих контрактів. Смарт-контракти можуть викликати непередбачувані аномалії, ідентифікація яких вимагає глибокого розуміння логіки їхньої роботи та структури даних.

Використання мультипідписів в системах віртуальних валют впливає на процес виявлення ризиків, оскільки може ускладнити аналіз транзакцій та вимагати додаткових алгоритмів для визначення легітимності підписів. Технології виявлення ризиків повинні бути гнучкими та адаптованими до різних видів криптовалют та їхніх особливостей. Оскільки технології віртуальних валют постійно еволюціонують, системи виявлення ризиків повинні мати можливість динамічного оновлення для врахування нових технологічних вдосконалень та стратегій атак.

Магістерська робота розкрила сутність технологій виявлення ризиків у сфері віртуальних валют, запропонувала ефективний підхід до використання машинного навчання та аналізу блокчейн-даних для досягнення високого рівня безпеки та контролю за транзакціями. Додавання аспектів смарт-контрактів та мультипідписів до технологій виявлення ризиків підкреслює необхідність глибокого розуміння функціоналу віртуальних валют та їхніх технологічних особливостей. Врахування цих аспектів сприяє створенню більш повноцінних та ефективних систем безпеки в криптовалютному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cryptocurrency Market Analysis from the Open Innovation Perspective [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2199853122011726#bb0045

2. Користін, О.Є. та Свиридюк Н.П. (2020), «Методологічні принципи оцінки ризиків в правоохоронній діяльності», «Наука і правоохорона», т. 3, стор. 191-197. [Електронний ресурс] – Режим доступу: https://doi.org/10.36486/np.2020.3(49).19

3. Raihana Syahirah Abdullah, Faizal M.A. (2018), «Блоковий ланцюг: криптографічний метод у четвертому Промислова революція», Міжнародний журнал Безпека комп'ютерних мереж та інформації, вип. 10, № 11, С. 9-17, 2018.

4. Купріяновський В. П. «Економіка Digital» Міжнародний журнал відкритої інформації Технологій, 2017, вип. 5, І. 3, С. 79-99.

5. Journal of Open Innovation: Technology, Market, and Complexity [Електронний ресурс] – Режим доступу: https://www.sciencedirect.com/science/article/pii/S2199853122011726#bb0020

6. Коробейнікова, О.М. Коробейников, Д.А. і Назарбаєв О. (2017), «Інноваційна оплата інструменти в платіжних системах", Актуальні проблеми гуманітарних і соціально-економічних наук, вип. 5, І. 11 (11), С. 102-104.

7. Акін Ойеделе (2017), Заборона біткойнів у Китаї Отримано з Businessinsider, Com. 13.

8. Exploration of the Problems of Virtual Currency and Potential Solutions [Електронний ресурс] – Режим доступу: https://www.atlantis-press.com/article/125980483.pdf

9. Книга «Блокчейн для бізнесу» Вільям Могайар

10. Machine Learning Technology [Електронний ресурс] – Режим доступу: https://builtin.com/machine-learning

11. Blog What is a Multisig Wallet? [Електронний ресурс] – Режим доступу: https://blog.thirdweb.com/multisig-

wallet/#:~:text=A%20multisig%20wallet%20is%20a,the%20assets%20within%20the%20wallet.

12. Про використання в розрахунках віртуальних валют. [Електронний ресурс] - Режим доступу: http://www.bank.gov.ua/control/uk/publish/article?art_id=22249610&cat_id=80928

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)