МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

МАКСИМЧУК Роман Олександрович

Алгоритми виявлення незаконних операцій з криптовалютами / Algorithms for Detecting Illegal Transactions with Cryptocurrency

спеціальність: 125 – Кібербезпека

освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
Р.О. Максимчук

Науковий керівник
к.т.н., доцент Т.Г. Цаволик

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Максимчуку Роману Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми виявлення незаконних операцій з криптовалютами / Algorithms for Detecting Illegal Transactions with Cryptocurrency
керівник роботи к.т.н., доцент Т.Г. Цаволик

затверджені наказом по університету від 1 грудня 2022 року № 491

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- проаналізувати існуючі алгоритми виявлення незаконних операцій;
- провести аналіз потенційних загроз;
- розгляд алгоритмів виявлення незаконних операцій з криптовалютою;
- використання штучного інтелекту;
- дослідження ефективності та покращення алгоритмів.

5. Перелік графічного матеріалу у роботі:
- покрокове формування блокчейн транзакції
- моніторинг транзакцій фіатних коштів
- моніторинг криптовалютних транзакцій у блокчейн мережі
- структура Bitcoin мережі на основі дерева Меркла.
- Незаконні операції з криптовалютою в 2022 році

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз алгоритмів виявлення незаконних операцій з криптовалютами	12.2022 р. – 03.2023 р.	
2	Використання штучного інтелекту для виявлення незаконних операцій	03.2023 р. – 05.2023 р.	
3	Дослідження ефективності та покращення алгоритмів	05.2023 р. – 11.2023 р.	

Студент _____ Максимчук Р.О.
(підпис)

Керівник роботи _____ к.т.н., доцент Т.Г. Цаволик

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Алгоритми виявлення незаконних операцій з криптовалютами» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 55 сторінок і містить 5 ілюстрацій, 1 таблицю, 1 додаток та 23 джерела за переліком посилань.

Метою випускної кваліфікаційної роботи є аналіз ефективності алгоритмів для виявлення та запобігання незаконних операцій з криптовалютами, з метою підвищення безпеки та прозорості у сфері цифрових валют.

Методи досліджень. Основними методами є аналіз даних та моделювання, включаючи використання статистичного аналізу, машинного навчання та штучного інтелекту для ідентифікації підозрілих транзакцій.

Результати дослідження: Аналіз взаємодії алгоритмів виявлення незаконних операцій з правовими та регуляторними рамками.

Орієнтовні напрямки розвитку досліджень: сформульовані та обґрунтовані висновки цього дослідження можуть бути базою для подальших наукових пошуків у галузі машинного навчання для виявлення аномальних паттернів у поведінці транзакцій та ідентифікації незаконних операцій.

Ключові слова: АЛГОРИТМ, ШТУЧНИЙ ІНТЕЛЕКТ, КРИПТОВАЛЮТА, ЕФЕКТИВНІСТЬ, ДОСЛІДЖЕННЯ.

ABSTRACT

The final qualification work on the topic "Algorithms for detecting illegal operations with cryptocurrencies" for the educational degree "Master" in the specialty 125 "Cybersecurity" of the educational and professional program "Cybersecurity" is written in the volume of 55 pages and contains 5 illustrations, 1 table, 1 appendix and 23 sources according to the list of references.

The purpose of the graduation qualification work is to analyze the effectiveness of algorithms for detecting and preventing illegal operations with cryptocurrencies in order to increase security and transparency in the field of digital currencies.

Research methods. The main methods are data analysis and modeling, including the use of statistical analysis, machine learning and artificial intelligence to identify suspicious transactions.

Research results: Analysis of the interaction of algorithms for detecting illegal transactions with legal and regulatory frameworks.

Indicative directions for further research: The formulated and substantiated conclusions of this study can be the basis for further research in the field of machine learning to detect abnormal patterns in transaction behavior and identify illegal transactions.

Keywords: ALGORITHM, ARTIFICIAL INTELLIGENCE, CRYPTOCURRENCY, EFFICIENCY, RESEARCH.

ЗМІСТ

ВСТУП

Актуальність теми. Алгоритми виявлення незаконних операцій з криптовалютами є надзвичайно актуальною з кількох причин: зростання популярності криптовалют з останніх років свідчить про значне збільшення використання криптовалют у світовій економіці, яке вимагає розробки ефективних механізмів для виявлення та запобігання незаконним операціям; анонімність та децентралізація, де особливості криптовалют, такі як анонімність користувачів та відсутність централізованого контролю, створюють сприятливе середовище для незаконних дій, включаючи відмивання грошей та фінансування тероризму; потреба у відповідності до регуляторних вимог, де уряди та міжнародні організації активно працюють над створенням правових рамок для регулювання операцій з криптовалютами; технологічний розвиток, таких як штучний інтелект та машинне навчання, відкриває нові можливості для аналізу та виявлення підозрілих транзакцій в режимі реального часу; ефективні алгоритми виявлення незаконних операцій з криптовалютами сприяють захисту прав та інтересів інвесторів і звичайних користувачів, підвищуючи довіру до цієї сфери; міжнародна співпраця та обмін інформацією.

Враховуючи ці аспекти, розробка та вдосконалення алгоритмів для виявлення незаконних операцій з криптовалютами є ключовим кроком для забезпечення безпеки та прозорості в цій швидко розвиваючійся області.

Мета і завдання дослідження. Мета дослідження полягає в аналізі ефективності алгоритму для виявлення та запобігання незаконним операціям з криптовалютами, з метою підвищення безпеки та прозорості у сфері цифрових валют.

Зазначена мета передбачає вирішення таких завдань дослідження:

- аналіз існуючих викликів;
- розробка нових методів;
- оцінка ефективності алгоритмів;
- відповідність регуляторним вимогам;
- захист інтересів користувачів;

Об’єктом дослідження є операції з криптовалютами та механізми їх виявлення. Це включає транзакції з криптовалютами, підозрілі діяльності та шаблони транзакцій, алгоритми та методи виявлення, регуляторні рамки та стандарти.

Предметом дослідження є вивчення та розробка методів аналізу, виявлення та запобігання незаконним операціям у сфері криптовалют, зосереджуючись на алгоритмах штучного інтелекту, машинного навчання та аналітичних підходах.

Методи дослідження. Основними методами є аналіз даних та моделювання, включаючи використання статистичного аналізу, машинного навчання та штучного інтелекту для ідентифікації підозрілих транзакцій.

Наукова новизна отриманих результатів полягає у дослідженні передових алгоритмів на базі штучного інтелекту для більш ефективного виявлення незаконних операцій з криптовалютами.

Практичне значення дослідження полягає у розвитку ефективних алгоритмів для забезпечення безпеки криптовалютних операцій та захисту інтересів інвесторів, сприяючи водночас відповідності регуляторним стандартам та підтримці міжнародної співпраці у протидії фінансовим злочинам.

Публікації та апробація.

1. Максимчук Р.О., Цаволик Т.Г. Налаштування та оцінка поширених програм по збору інформації транзакцій з криптовалютами "Автоматизація та комп’ютерно-інтегровані технології" (АКІТ-2023), Тернопіль, 2023. С. 137 - 138.

2. Максимчук Р.О., Цаволик Т.Г. Технологічні тренди в галузі криптовалют та блокчейну «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. С. 40 – 41.

1.АНАЛІЗ ТА ОЦІНКА ІСНУЮЧИХ АЛГОРИТМІВ ДЛЯ ВИЯВЛЕННЯ НЕЗАКОННИХ ОПЕРАЦІЙ З КРИПТОВАЛЮТОЮ

1.1 Поняття, принципи та види шахрайства з криптовалютою

У зв’язку з низкою прикладів нелегального використання криптовалют, їх часто зображують як ідеальний засіб платіжної системи для злочинців, які прагнуть приховати свої незаконні кошти.

Банківські та фінансові регулятори країн G20 впроваджують низку законів на тему фінансового моніторингу криптовалют та зробили спільну заяву, в якій наголошено на активізації зусиль у боротьбі з фінансуванням тероризму, і закликали інші країни долучитись.

Українське законодавство розвивається повільніше, але не стоїть осторонь світових процесів. «AML/CFT. Фінансовий моніторинг в Україні» – проект, який запроваджено з метою розуміння, що таке фінансовий моніторинг, як відрізнити звичайні операції від операцій з відмивання коштів, які дії повинні виконати фінансові установи, щоб не впустити в фінансову систему «брудні» кошти, не втратити свою репутацію, уникнути застосування до них штрафних санкцій. Головне завдання фінансового моніторингу – це протидія та запобігання відмиванню коштів, розповсюдження зброї масового знищення та фінансуванню тероризму. Ця боротьба сьогодні – одна з головних тем світової фінансової системи.

На сьогоднішній день існує велика кількість криптовалют, кожна з яких має свої унікальні характеристики та функції. У цьому тексті ми розглянемо декілька видів криптовалют, які є найбільш поширеними та відомими.

Bitcoin [1]: Bitcoin - перша і найвідоміша криптовалюта. Вона була створена в 2009 році та відзначається високою капіталізацією, широким використанням та популярністю. Bitcoin має децентралізовану систему управління та забезпечує повну анонімність та приватність користувачів.

Ethereum [2]: Ethereum - друга за популярністю криптовалюта після Bitcoin. Її головна особливість - можливість створення децентралізованих додатків та контрактів, що називається "розумні контракти". Ethereum має власну

криптовалюту - Ether, яка використовується як платіжний засіб в екосистемі Ethereum.

Litecoin [3]: Litecoin була створена в 2011 році як "вдосконалена версія" Bitcoin. Вона має швидший час обробки транзакцій та меншу вартість транзакцій порівняно з Bitcoin. Litecoin також має більшу кількість монет, ніж Bitcoin, що забезпечує більшу доступність для користувачів.

Ripple [4]: Ripple - це криптовалюта, яка використовується в системі глобальних платежів, що базується на технології блокчейн. Основна мета Ripple полягає у спрощенні та зниженні вартості міжнародних грошових переказів. Ripple не є децентралізованою криптовалютою, оскільки управління мережею здійснюється від імен

Купівля криптовалюти може проходити в різних варіантах, але загалом її можна розділити на три основні етапи:

1. Реєстрація на платформі обміну: першим етапом є реєстрація на платформі обміну, де можна купити криптовалюту. Крім того, потрібно забезпечити платіжну інформацію, таку як банківський рахунок або кредитну картку.

2. Придбання криптовалюти: на другому етапі можна придбати криптовалюту, використовуючи розміщені на платформі обміну замовлення на купівлю. Крім того, можна обрати метод оплати, такий як банківський переказ або кредитну картку.

3. Зберігання криптовалюти: після придбання криптовалюти її потрібно зберегти в безпечному місці. Зазвичай, криптовалюти зберігаються в крипто кошельках, що можуть бути онлайн або офлайн. Онлайн-крипто кошельки зберігаються в інтернеті, тоді як офлайн-крипто кошельки зберігаються на жорсткому диску або флеш-накопичувачі.

Після завершення цих етапів, криптовалюта знаходиться у власності користувача і може бути використана для платежів, зберігання вартості, інвестування та інших цілей.

Зберігання криптовалюти є важливою складовою успішного використання цього активу. Оскільки криптовалюта не має фізичної форми, її можна зберігати тільки в електронному вигляді, а саме в:

1. Криптовалютні гаманці: Криптовалютні гаманці є програмними засобами зберігання криптовалюти. Гаманці можуть бути встановлені на комп'ютері, смартфоні або спеціальному пристрої. Криптовалютні гаманці мають різні рівні безпеки, тому перед вибором гаманця варто провести ретельний аналіз. Як правило, криптовалютні гаманці забезпечують приватні ключі, необхідні для доступу до криптовалюти.

2. Апаратні гаманці: Апаратні гаманці є фізичними пристроями зберігання криптовалюти. Вони забезпечують більш високий рівень безпеки, оскільки приватні ключі зберігаються на пристрої, а не на комп'ютері або смартфоні. Апаратні гаманці можуть бути придбані в спеціалізованих магазинах або від виробників криптовалют.

3. Криптовалютні біржі: Криптовалютні біржі забезпечують зберігання криптовалюти на користь користувачів. Криптовалютні біржі зазвичай забезпечують високий рівень безпеки, оскільки вони використовують різні заходи захисту, такі як двофакторна автентифікація та захист від хакерських атак. Проте, перед зберіганням криптовалюти на біржі, необхідно провести докладний аналіз без посередньої безпеки платформи. Деякі аспекти, які важливо врахувати, включають аудит систем безпеки, історію попередніх інцидентів, а також репутацію біржі серед користувачів. Забезпечення надійності та безпеки зберігання криптовалюти на біржі - це важлива передумова для успішної та безпечної участі в криптовалютному просторі.

Хоча криптовалюти стали досить популярними, вони не є повністю безпечними від шахрайства. Шахраї використовують різні методи для обману користувачів та викрадення їх грошей. Криптовалюти працюють на основі технології блокчейн, яка є децентралізованою системою, що дозволяє виконувати операції без прямої участі посередників, таких як банки або інші фінансові установи.

Криптовалюти можуть використовуватися для здійснення платежів, зберігання вартості та інвестування. Деякі з найбільш відомих криптовалют включають Bitcoin, Ethereum, Litecoin та Ripple.

Оскільки криптовалюти не контролюються централізованою владою, вони можуть мати високу ступінь анонімності та конфіденційності. Однак, це також може створити проблеми з підтримкою законності та зловживанням.

Поняття, принципи та види шахрайства з криптовалютою відноситься:

1. Фішинг - це вид атаки, коли зловмисники використовують підроблені веб-сайти та електронні листи для викрадення конфіденційної інформації від користувачів криптовалюти.

2. Розсилка шахрайських повідомлень - це коли шахраї надсилають спам-повідомлення з метою обману користувачів та викрадення їх грошей.

3. Соціальний інжиніринг - це коли шахраї використовують психологічні та маніпулятивні методи для викрадення конфіденційної інформації та грошей.

4. Шахрайство з підробкою - це коли зловмисники підробляють існуючі криптовалюти для того, щоб вкрасти гроші у досвідчених користувачів.

5. Крадіжка особистих даних - це коли зловмисники викрадали особисті дані користувачів, такі як імена, адреси та номери кредитних карток, для того, щоб викрасти їх гроші.

Принципи шахрайства з криптовалютою полягають в тому, щоб обманути користувачів та викрасти їх гроші. Шахраї використовують різні методи для того, щоб переконати користувачів виконати деякі дії, які призводять до викрадення їх грошей.

Для того, щоб уникнути шахрайства з криптовалютою, користувачі повинні бути обережними і підтримувати безпеку.

1.2 Аналіз відкритих джерел та використання спеціальних програм для збору інформації про транзакції з криптовалютами

Використання спеціальних програм для збору інформації про транзакції з криптовалютами може допомогти розкрити злочини, пов'язані з використанням криптовалют. Для збору інформації про транзакції з криптовалютами можна використовувати спеціальні програми, такі як блокчейн-експлорери, які дозволяють переглядати дані про транзакції та адреси гаманців. Наприклад, такі програми, як Blockchair, BlockCypher, Bitaps та інші, дозволяють переглядати дані про транзакції та адреси гаманців для багатьох різних криптовалют. Крім того, можна використовувати різні відкриті джерела, такі як соціальні мережі, форуми та інші ресурси, для збору додаткової інформації про транзакції з криптовалютами. Наприклад, на форумах, таких як Reddit або Bitcointalk, користувачі можуть обговорювати різні транзакції та вказувати на можливі злочинні дії, пов'язані з криптовалютами. Загалом, аналіз відкритих джерел та використання спеціальних програм для збору інформації про транзакції з криптовалютами може бути корисним для правоохоронних органів та інших установ, які займаються виявленням та розслідуванням злочинів, пов'язаних з криптовалютами. Однак, при зборі та використанні цих даних варто дотримуватись принципів конфіденційності та захисту персональних даних.

Блокчейн-експлорер (або блокчейн-оглядач) - це веб-інтерфейс, який дозволяє переглядати дані про транзакції та блоки, які зберігаються в блокчейні криптовалютної мережі. Такі програми дозволяють користувачам швидко та зручно переглядати дані про транзакції, блоки, адреси гаманців, стан мережі та іншу інформацію, яка є доступною в блокчейні. Блокчейн-експлорери доступні для багатьох різних криптовалют, таких як Bitcoin, Ethereum, Litecoin, Ripple та інші. Вони можуть мати різні функції та можливості, такі як пошук транзакцій за певними параметрами, графіки та статистику, можливість переглядати дані про блоки, непідтверджені транзакції та інші дані про мережу. Блокчейн-експлорери можуть бути корисні для користувачів криптовалют, які хочуть перевірити стан своїх транзакцій або отримати інформацію про стан мережі. Також вони можуть

бути корисні для дослідників, які займаються аналізом даних блокчейну, та правоохоронних органів, які розслідують злочини, пов'язані з криптовалютами.

Ethereum Explorer - популярний блокчейн-експлорер для Ethereum, який надає користувачам інформацію про транзакції, блоки, гаманці та контракти.

Blockchair - блокчейн-експлорер, який підтримує багато різних криптовалют, таких як Bitcoin, Ethereum, Litecoin, Bitcoin Cash та інші. Binance

Explorer - блокчейн-експлорер для Binance Smart Chain, який дозволяє переглядати інформацію про транзакції та блоки, а також отримувати інформацію про контракти.

Cardano Explorer - блокчейн-експлорер для Cardano, який надає інформацію про транзакції, блоки, адреси та інші дані про мережу. Ці блокчейн-експлорери не є єдиними доступними, але їх популярність пояснюється їхньою широкою функціональністю, доступністю та зручним інтерфейсом.

Сьогодні, розслідування кіберзлочинності в області криптовалюти неможливо без використання аналітичних інструментів для блокчейн мереж. Компанія CryptoLocker розробила власний спосіб аналізу блокчейн інформації, дослідникам вдалося розробити прототип, що дозволяє ідентифікувати цифрові сліди, які можуть більш детально розкрити інформацію про особистість, що їх залишила. Рід і Гарріган розповіли про труднощі щодо загального питання анонімності у блокчейн мережах та виявлення поведінки реального користувача. Вони розробили Blockchain Inspector – система, що використовує штучний інтелект для ідентифікації та створення профілю користувача блокчейн мережі, та дозволяє відстежувати їх поведінку.

Дослідження економічних аспектів поведінки користувачів блокчейн мереж є також одним із видів блокчейн-аналізу. Мозер і Боме були сконцентровані на розгляді інформації про розподілення комісії від транзакцій. Як відбуваються транзакції зображено на рисунку 1.1.

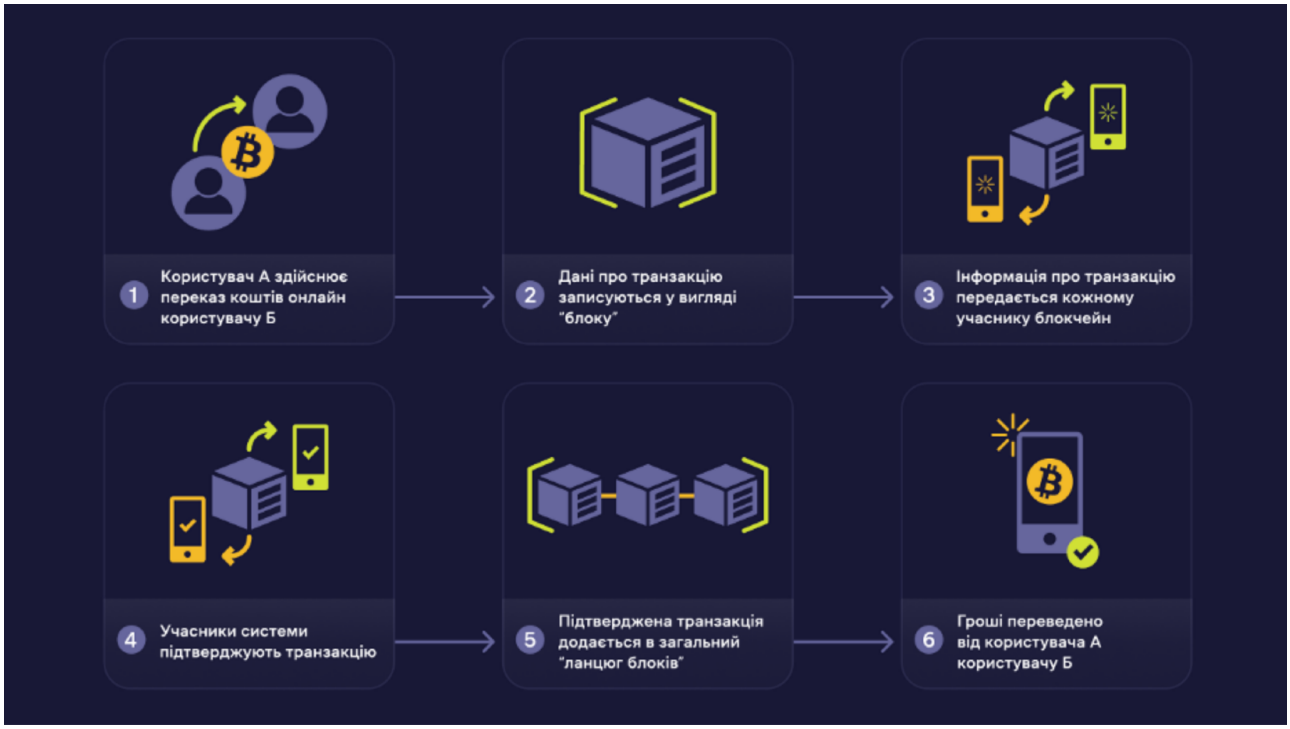

Рисунок 1.1 – Покрокове формування блокчейн транзакцій

Лішке і Фабіан, а також Рон і Шамір провели аналіз ринку за допомогою блокчейну, поєднавши мережеві дані з координатами геолокацій, таким чином вони отримали уявлення про розподіл криптовалютного бізнесу. Обидва дослідження використовують blockexplorer.com – веб-інструмент з відкритим кодом, який дозволяє візуалізувати інформацію щодо блоків та транзакцій у блокчейні. BitConeView [18] – це веб-інструмент, який полегшує дослідження транзакцій у Bitcoin мережі. Інструмент також дозволяє відстежувати витрати, дозволяючи ідентифікувати закономірності та потік грошей. BitIodine – ще один інструмент для аналізу блокчейну. Надає базову інформацію, наприклад баланс гаманця та загальну кількість транзакцій. Обидва інструменти були протестовані користувачами та 22 демонструють ефективний спосіб аналізу та виявлення патернів поведінки всередині Bitcoin блокчейн мережі. Blockchain.info є одним з найпопулярніших сервісів, що вперше з'явився на ринку ще в 2011. Цей інструмент надає швидкі та прості у використанні можливості для відстеження окремих транзакцій, а також надає велику кількість інформації, включаючи базові діаграми та статистику, про всю Bitcoin мережу. Ортега використовував публічну інформацію з blockchain.info деякий проміжок часу, щоб

деанонімізувати адреси мережі Tor та їх проксі сервера. Blockchain.info надає інформацію в зручному вигляді та дозволяє аналітикам переглянути кожну транзакцію. Кінкельдей, Фекете та Ізенберг розробили систему, яка дозволяє розпізнавати об’єкти Bitcoin мережі на основі їх публічної адреси (адреси гаманця). Інструмент називається BitConduite, він використовує топологію мережі (з її мільярдами транзакцій), надаючи оцінку до якої сутності відповідає певна адреса. Bitcoin можна використовувати у різних цілях -– починаючи від інвестицій до здійснення нелегальних платежів. BitConduite може стати корисними для вивчення та виявлення засобів використанням Bitcoin. Аналітики, які працюють з BitConduite можуть групувати та фільтрувати дані на основі різних атрибутів. Дані про торгівлю з криптовалютних бірж можуть надати цікаве розуміння потоку грошей. Веб-сайт bitcoincharts.com надає фінансову та технічну інформацію, що пов’язана з Bitcoin та може бути використана для аналізу щоденних торгових курсів, тенденцій та аномалій ринку. Також на ринку існують комерційні програми. Chainalysis був запропонований як інструмент, що дозволяє оцінити ризики, пов'язані з Bitcoin операціями. На даний час використовується правоохоронними органами під час розслідування кіберзлочинності. Загалом, на ринку не існує ідеального інструменту для блокчейн-аналізу. Кожен із перелічених сервісів має свої переваги та недоліки. Наразі, повний аналіз вимагає 23 поєднання даних як з самого блокчейну, так із зовнішніми даними, отриманими за допомогою блокчейн-аналітики, вікі або публічних форумів.

Аналіз відкритих джерел та використання спеціальних програм для збору інформації про транзакції з криптовалютами може допомогти розкрити різні види злочинів, пов'язаних з використанням криптовалют. Ось кілька прикладів: Біл laundering (відмивання грошей) - злочин, пов'язаний з переведенням грошей, отриманих незаконним шляхом, через кілька рахунків, щоб затруднити відстеження походження цих коштів. Криптовалюти є одним з основних засобів для відмивання грошей, тому аналіз транзакцій може допомогти виявити та викрити такі злочини.

Фінансування тероризму - злочин, пов'язаний з переказом коштів на підтримку терористичних організацій. Криптовалюти можуть бути використані для фінансування тероризму, оскільки їхні транзакції можуть бути анонімними та важко відстежуватись. Аналіз транзакцій може допомогти виявити підозрілі транзакції та встановити зв'язки з терористичними організаціями.

Кіберзлочини [8] - злочини, пов'язані з комп'ютерними мережами, такі як шахрайство, крадіжка ідентифікаційних даних, розповсюдження вірусів та інші. Криптовалюти можуть бути використані для оплати за послуги злочинців, тому аналіз транзакцій може допомогти виявити підозрілі транзакції та встановити зв'язки з кіберзлочинцями.

Щоб боротися з злочинністю, пов'язаною з криптовалютами, необхідно вжити ряд заходів. Ось кілька з них:

– регулювання - держави можуть встановлювати правила та норми, які обмежують використання криптовалют у злочинних цілях, а також встановлюють вимоги до компаній, які працюють з криптовалютами;

– контроль за обміном криптовалют - різні країни можуть встановлювати різні правила для обміну криптовалют. Наприклад, вимоги до реєстрації користувачів, встановлення обмежень на операції та обмін коштів;

– запобігання відмиванню грошей - країни можуть встановлювати закони, що вимагають від провайдерів послуг з криптовалютами вести облік клієнтів та вживати заходів для запобігання відмиванню грошей;

– розширення міжнародної співпраці - злочинні мережі часто працюють на міжнародному рівні, тому необхідно розвивати міжнародну співпрацю в боротьбі з криптовалютними злочинами.

Розробка нових технологій, що дозволяють відстежувати транзакції криптовалют, може допомогти виявляти підозрілі транзакції та зменшувати використання криптовалют у злочинних цілях. Підвищення рівня освітита підвищення інформованості громадськості можуть допомогти зменшити використання криптовалют у злочинних цілях шляхом підвищення рівня свідомості про потенційні негативні наслідки використання криптовалют.

1.3 Оцінка ефективності алгоритмів для виявлення незаконних операцій з криптовалютами

У світі фіатних валют широко використовують рішення для автоматичного моніторингу транзакцій, що базуються на вивченні поведінки клієнтів. Такі методи є ефективним способом задовольнити вимоги щодо відмивання коштів та протидії фінансування тероризму. Незважаючи на поширену теорію того, що транзакції криптовалют неможливо ідентифікувати та відслідкувати, існує можливість створити автоматичне рішення для моніторингу блокчейну, що буде мати змогу ідентифікувати потенційно небезпечні транзакції в мережі, а також перевіряти їх законність за визначеними критеріями. Слід зазначити що моніторинг транзакцій звичайних фіатних валют, та моніторинг криптовалютних транзакцій мають важливі відмінності. На рисунку 1.2 видно, що традиційні методи моніторингу фіатних транзакцій зосереджуються на виявленні аномалій поведінки в момент, коли клієнтські кошти вносяться або вилучаються з фінансової установи:

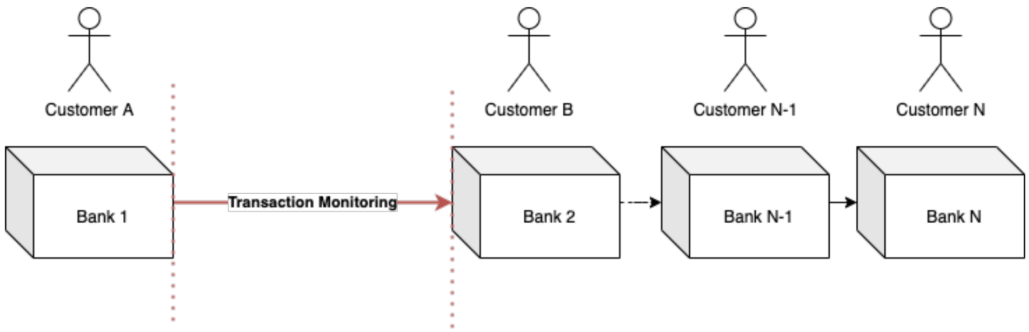

Рисунок 1.2 – Моніторинг транзакцій фіатних коштів

«Bank 1» володіє інформацією про те, що його клієнт переводить кошти іншому клієнту «Bank 2», при цьому банк не володіє інформацією про історію коштів до входження їх до банку та після виведення коштів з цього банку. 12 Розглянемо більш детально ситуацію у світі криптовалют. Як видно з рисунку 1.3, біржа криптовалют не завжди володіє інформацією про фізичну або юридичну особу, яка здійснює транзакцію.

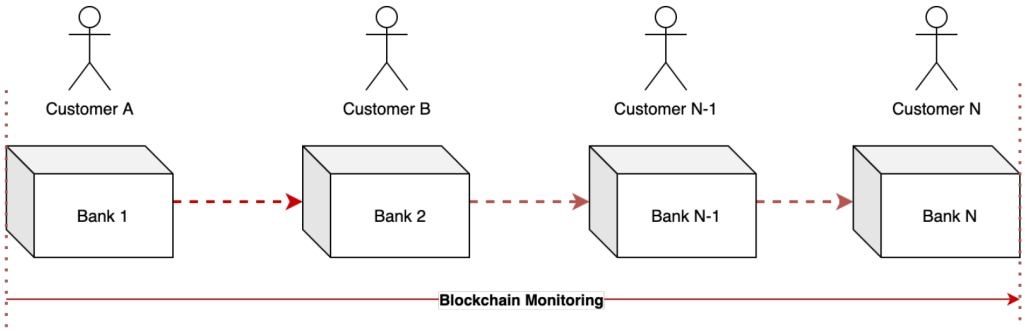

Рисунок 1.3 – Моніторинг криптовалютних транзакцій у блокчейн мережі

Проте прозорість публічних блокчейн мереж надає можливість повністю переглядати історію коштів від початкового до кінцевого джерела виникнення, розкриваючи додаткову інформацію, що може свідчити про ризик транзакції та ймовірність заходжень «брудних» коштів, які були пов’язані з відмиванням коштів, фінансуванням тероризму або іншим показникам AML/CFT регуляторів.

Для ефективного виявлення незаконних операцій з криптовалютами можуть використовуватись різні підходи та технології. Наприклад, одним з підходів є використання технології блокчейн, яка дозволяє забезпечувати безпеку операцій та слідкувати за ними у режимі реального часу. Також можна використовувати машинне навчання для виявлення аномалій у поведінці користувачів та транзакцій. Наприклад, можна навчати моделі на прикладах незаконних операцій та користувачів, щоб вони могли виявляти подібні ситуації у майбутньому. Ще одним підходом є аналіз зв'язків між адресами криптовалют, що дозволяє виявляти підозрілі транзакції та адреси. Наприклад, якщо відомо, що одна адреса належить злочинній групі, то можна аналізувати зв'язки цієї адреси з іншими адресами, щоб виявити можливі спроби переказу коштів з цієї адреси на інші адреси злочинців. Крім того, можна використовувати різні методи аналізу графів транзакцій, які дозволяють виявляти підозрілі схеми переміщення криптовалют між різними адресами. У будь-якому випадку, ефективність алгоритмів для виявлення незаконних операцій з криптовалютами може залежати від ряду факторів, таких як точність, швидкість, вартість розробки та

впровадження, а також потенційні обмеження з точки зору безпеки та конфіденційності даних.

Анонімність [9] – одна з найважливіших особливостей технології блокчейн. Сьогодні кожен може створити власний крипто гаманець та використовувати його для надсилання або отримання коштів, не залишаючи свої персональні дані. Вірогідно ідентифікувати особу за адресою криптовалютного гаманця без проходження KYC процедури неможливо, однак, завдяки аналізу блокчейн мереж, крипто гаманці можуть бути згруповані залежно від їх поведінки. Для того, щоб здійснити транзакцію у Bitcoin мережі, користувач повинен мати крипто гаманець. Найбільш фундаментальним об'єктом в блокчейні є адреса крипто гаманця. Найпоширеніша його форма складається з пари відкритого та приватних ключів. Відкритий ключ використовується для ідентифікації цієї адреси в ланцюзі блоків, наприклад для отримання Bitcoin. У той час як приватний ключ ECDSA, сформований із випадкового числа довжиною 256 біт, використовується для криптографічного підпису транзакції. Другий найпоширеніший тип адреси – P2SH, де ключем для переказу коштів є не геш ключа, а геш сценарію. Це дозволяє проводити більш складні транзакції, де потрібно знати кілька ключів, пароль або що-небудь, щоб задовольнити виконання сценарію. Загальна транзакція складається з чотирьох основних елементів: – геш транзакції; – адреса відправника; – адреса отримувача; – сума. Кожна транзакція в новому блоці обов'язково перевіряється майнерами, щоб переконатися, що жодні монети не витрачаються двічі. Транзакції нового блоку обробляються в єдиний геш, яке є коренем дерева Меркла (рисунок 1.4). Така бінарна деревоподібна структура містить лише транзакції в листках.

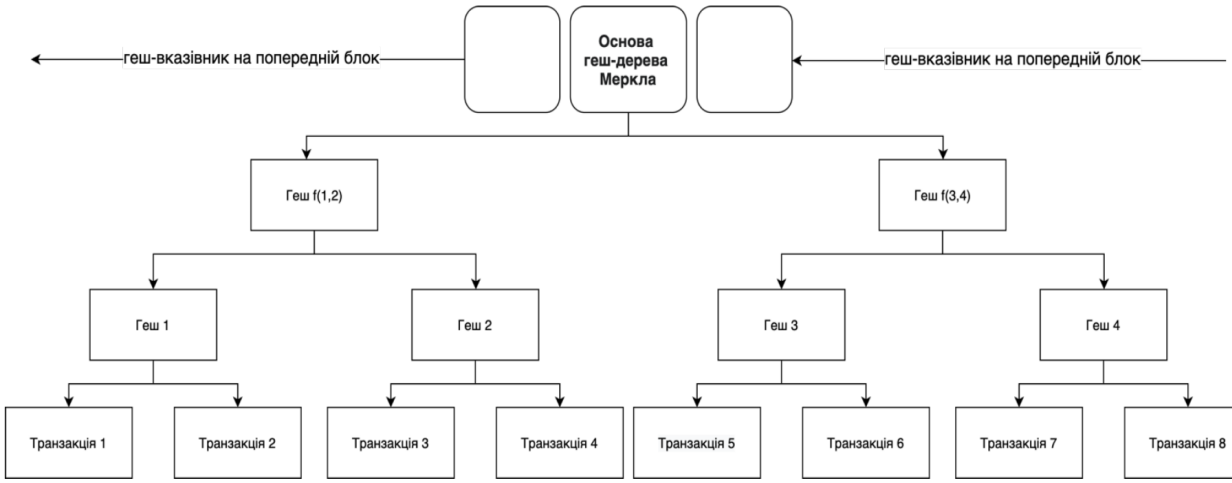

Рисунок 1.4 – Структура Bitcoin мережі на основі дерева Меркла

До кожного нового блоку додається геш попереднього блоку. Узагальнено процес транзакції виглядає наступним чином: – знімається повна сума з гаманця відправника; – кошти відправляються на адресу одержувача; – формується решта (віднімається комісія); – решта відправляється на адресу гаманця відправника; – транзакція відправляється в мережу, де формується в блоки разом з іншими транзакціями мережі; – коли всі вузли мережі підтвердять операцію за алгоритмом консенсусу, транзакція буде публічно доступною. Необхідно зауважити, що відправник може зазначити іншу (відмінну від початкової) адресу для повернення решти, це є один зі способів ще більше анонімізувати транзакцію. Кожна транзакція повинна бути підтверджена відправником з використанням приватного ключа, котрий був згенерований під час створення гаманця. 28 Як наголошувалось раніше, переваги використання блокчейн мереж – анонімність, але особливість архітектури Bitcoin блокчейн мереж полягають у тому, що коли адреса гаманця пов'язується з реальним власником, існує можливість розкрити та ідентифікувати усі операції, здійснені ним, без можливості видалення історії транзакцій.

2. СИСТЕМИ ВИЯВЛЕННЯ НЕЗАКОННИХ ОПЕРАЦІЙ З КРИПТОВАЛЮТОЮ

2.1 Моніторинг поведінки користувачів та виявлення відхилень від звичної поведінки

Збір інформації про користувачів є важливим етапом для реалізації моніторингу та виявлення відхилень в їхній поведінці. У цьому розділі магістерської роботи розглянемо різні методи та техніки, які використовуються для цього, а також їхні особливості.

Збір активності користувачів: Збір журналів логінів: Цей метод передбачає записування подій, пов'язаних з авторизацією та входом користувачів до системи чи платформи. Детально розглядаються способи реєстрації цих подій та їхнє використання для встановлення ідентичності користувачів.

Збір історії дій: Описується метод збору даних про дії користувачів після входу в систему, включаючи їхню взаємодію з веб-сайтом, додатками, перегляд вмісту тощо. Розглядається важливість цієї інформації для аналізу поведінки.

Використання кукісів (cookies): Розглядаються кукіси як інструмент для збору та зберігання інформації про користувачів у веб-середовищі. Описується їхня функція та вплив на стеження за активністю користувачів.

Огляд технологій та інструментів, які сприяють збору і обробці користувальницьких даних для подальшого аналізу. Сучасна обробка та аналіз користувальницьких даних є неможливою без використання різних технологій та інструментів, що допомагають збирати, зберігати, обробляти та аналізувати великі обсяги інформації. Ця область технологічного прогресу стала ключовою для багатьох сфер, включаючи маркетинг, медицину, фінанси, кібербезпеку і багато інших.

Системи збору даних: Датчики і сенсори присутні в сучасні пристрої, такі як мобільні телефони та смарт-годинники, оснащені різними сенсорами, які збирають інформацію про місцезнаходження, температуру, пульс та інші параметри. Ці дані можуть бути використані для створення профілю користувача. Інтернет речей (IoT) це - промислові об'єкти та побутові пристрої,

підключені до Інтернету, генерують велику кількість даних, які можна використовувати для аналізу. Наприклад, смарт-термостати, які збирають дані про споживання енергії в будинку.

Системи зберігання даних [11]: Існують реляційні та нереляційні бази даних, такі як MySQL, PostgreSQL, MongoDB, дозволяють зберігати структуровані та неструктуровані дані. Вони надають можливість ефективного зберігання та організації інформації. Хмарні сервіси, публічні хмарні платформи, такі як Amazon Web Services (AWS), Google Cloud, Microsoft Azure, надають інфраструктуру для зберігання даних в хмарі, що дозволяє масштабувати ресурси відповідно до потреб.

Інструменти обробки та аналізу даних: Мови програмування такі як Python, R, і Java є популярними мовами програмування для обробки та аналізу даних. Вони мають багатий екосистему бібліотек та інструментів для статистичного аналізу та машинного навчання. Інструменти візуалізації даних такі як Matplotlib, Seaborn, Tableau та Power BI, дозволяють створювати інтерактивні графіки та візуалізації для представлення даних користувачам. Бібліотеки для машинного навчання: TensorFlow, PyTorch, Scikit-Learn надають інструменти для розробки та тренування моделей машинного навчання, які можна використовувати для аналізу даних та виявлення патернів.

Методи обробки даних: Обробка текстової інформації використовує застосування методів обробки природної мови (NLP) для аналізу текстових даних, включаючи виявлення сентименту та екстракцію ключових слів. Використання комп'ютерного зору та нейронних мереж для аналізу зображень та виявлення об'єктів на них.

Ці технології та інструменти стали невід'ємною частиною аналізу користувальницьких даних, дозволяючи отримувати цінні інсайти та підтримувати прийняття рішень.

В сучасному цифровому світі, де обмін даними став невід'ємною частиною нашого життя, важливо мати механізми для виявлення відхилень від нормальної поведінки. Це особливо актуально в галузі кібербезпеки, фінансових операцій, медичних досліджень та багатьох інших сферах. Одним із ключових завдань є

розробка та впровадження моделей та алгоритмів, які допомагають виявляти аномалії та потенційні загрози в реальному часі. У цій статті ми розглянемо деякі типові моделі та алгоритми для виявлення відхилень від нормальної поведінки. Машинне навчання використовується для створення моделей, які можуть класифікувати дані на нормальну та аномальну поведінку. Основні підходи включають: Навчання з учителем це - використання алгоритмів, таких як логістична регресія та випадковий ліс, для побудови моделей на основі навчального набору даних, які містять як нормальну, так і аномальну поведінку. Навчання без учителя це - використання алгоритмів кластеризації та зменшення розмірності, таких як метод k-середніх та методи головних компонент, для групування даних та виділення аномалій на основі внутрішньої структури даних.

Методи аналізу часових рядів у великій кількості сценаріїв даних відображаються у вигляді часових рядів. Для виявлення аномалій у часових рядах використовуються такі методи: Експоненційне згладжування, цей метод дозволяє прогнозувати майбутні значення та виявляти аномалії, які відхиляються від очікуваних трендів. Авторегресійні моделі застосовуються для моделювання залежності між поточними та попередніми значеннями та виявлення аномалій на основі резидуальних помилок. Методи глибинного навчання використовують Нейронні мережі це - глибокі нейронні мережі, включаючи рекурентні та згорткові мережі, використовуються для аналізу послідовностей даних та виявлення аномалій в реальному часі.

Статистичні методи: Здвигові статистики це - алгоритми, які визначають статистичні метрики, такі як середнє та стандартне відхилення, для виявлення відхилень від нормальної поведінки. Зовнішні моделі використовуються для порівняння поточних даних з нормативними даними та виявлення аномалій на основі відхилень від цих норм.

Аалгоритми мають свої переваги та обмеження, і їх вибір залежить від конкретного завдання та характеристик даних. Наявність ефективних інструментів для виявлення відхилень від нормальної поведінки є важливою складовою для забезпечення кібербезпеки, збереження фінансової стійкості та підтримки рішень в різних галузях нашого сучасного світу.

Аналіз працездатності, чутливості та точності алгоритмів та моделей для виявлення аномалій є критичним етапом в їхньому впровадженні в різних сценаріях. Враховуючи різноманітність ситуацій та даних, важливо розуміти, як ці аспекти впливають на ефективність системи виявлення аномалій. Нижче розглянемо кожну з цих характеристик. Працездатність алгоритму виявлення аномалій визначає його здатність правильно функціонувати в різних умовах та на різних типах даних. Аналіз працездатності допомагає визначити, наскільки стійкий алгоритм до:

1. Чи може алгоритм адаптуватися до змін у розподілі даних, які можуть виникнути в часі або в різних сценаріях?
2. Як впливають зміни в обсязі даних, їхній складності та характеристиках на ефективність алгоритму?
3. Наскільки добре алгоритм впорається з шумом в даних та іншими артефактами?
4. Які заходи вживаються для захисту від спроб обхіду системи та кібератак?

Чутливість алгоритму виявлення аномалій вказує на його здатність виявляти реальні аномалії та незвичайні події в даних. Це важливо в умовах, де помилкові срабатування можуть призвести до великої кількості фальшивих тривог. Аналіз чутливості включає такі аспекти:

1. Як ефективно алгоритм виявляє реальні аномалії, які представляють ризик чи загрозу?
2. Наскільки алгоритм уникав ситуацій, коли нормальні дані помилково класифікуються як аномальні?
3. Чи дозволяє алгоритм налаштовувати рівень чутливості в залежності від потреби?

Точність алгоритму для виявлення аномалій визначає, наскільки правильно він класифікує дані, тобто наскільки реальні аномалії та нормальні дані відповідають прогнозам. Аналіз точності оцінює:

1. Як точно алгоритм розпізнає та класифікує аномалії та нормальні дані?

2. Яка кількість хибнопозитивних та ложнонегативних срабатувань має алгоритм?

3. Чи може алгоритм бути налаштований для досягнення оптимального балансу між точністю та чутливістю?

У різних сценаріях виявлення аномалій важливо підібрати модель та параметри, які найкраще відповідають конкретному завданню. Наприклад, в бізнес-сфері може бути важливою точність для мінімізації фальшивих тривог, тоді як у кібербезпеці може бути критичною чутливість для виявлення справжніх загроз. Отже, ретельний аналіз та налаштування моделей є ключовими складовими для досягнення ефективної системи виявлення аномалій в різних контекстах.

Визначення ключових параметрів та ознак для виявлення відхилень: підґрунтя аналізу даних.

У цифровій епосі, коли обробка та аналіз даних стають невід'ємною частиною багатьох сфер, важливим завданням є виявлення відхилень від нормальної поведінки. Це має вирішальне значення в таких областях, як кібербезпека, фінансовий моніторинг, медицина та багато інших. В цій статті ми розглянемо ключові параметри та ознаки, які використовуються для ефективного виявлення відхилень від норми в наборах даних.

Системні параметри включають у себе технічні або фізичні характеристики, які можуть бути виміряні або спостережені в реальному часі. Вони можуть бути важливими для виявлення відхилень у випадках, коли незвичайна поведінка може бути визначена за технічними параметрами, такими як:

– загальний обсяг мережевого трафіку, зміни в розподілі портів чи протоколів, затримки пакетів та інші параметри;

– використання центрального процесора (CPU), оперативної пам'яті (RAM) та інших ресурсів системи;

– спроби незвичайного доступу до файлової системи, включаючи зчитування, запис та зміну прав доступу.

Поведінкові ознаки відображають споживання або активність користувачів та об'єктів. Вони включають у себе такі аспекти як:

– часові штампи дата та час подій або транзакцій;

– споживачі ресурсів, ідентифікація користувачів, IP-адреси, акаунти, сесії та інші ідентифікаційні ознаки.

Запити та операції:

– вміст запитів;

– SQL-запити;

– методи HTTP-запитів та інші дії з даними.

Структурні ознаки відображають взаємозв'язки та структуру даних, що аналізуються. Вони важливі для розуміння, як дані взаємодіють та як можуть виникати відхилення від норми. Це може включати:

– взаємозв'язки та залежності між різними полями в даних;

– структури графів або мереж, які можуть відображати взаємозв'язки між об'єктами;

– групи даних, що мають спільні характеристики або розподіли.

Деякі сценарії можуть вимагати спеціалізованих ознак, що відображають конкретні аспекти аналізу. Наприклад:

– дані з сенсорів, що вимірюють фізичні величини, такі як температура, вологість, тиск, рух та інші;

– аналіз текстового вмісту, який може включати ключові слова, синтаксичні структури та сентимент.

Підбір та аналіз правильних ключових параметрів та ознак є критично важливим завданням для розробки систем виявлення відхилень від нормальної поведінки. Від правильно обраного набору ознак залежить ефективність та точність аналізу.

В світі криптовалют важливим завданням є виявлення незаконних операцій та запобігання фінансовим злочинам, таким як відмивання грошей, шахрайство та фінансування тероризму. Для цього використовуються системи виявлення відхилень, які аналізують та моніторять транзакції та поведінку

користувачів у блокчейні. У цій статті ми розглянемо ключові параметри та ознаки, які використовуються для виявлення незаконних операцій з криптовалютою.

Обсяг та суми транзакцій один із перших параметрів, який аналізують, - це обсяг та сума транзакцій. Незвичайно великі або малий обсяги транзакцій можуть вказувати на можливість фінансових аномалій. Наприклад, велика кількість невеликих транзакцій може бути ознакою відмивання грошей.

Ідентифікація Адрес та Користувачів: Важливим аспектом є ідентифікація адрес та користувачів. Користувачі, які відомі своєю поганою репутацією або зв'язками зі злочинною діяльністю, можуть бути виключені з легальних транзакцій.

Час та часові штампи транзакцій грають важливу роль у виявленні аномалій. Наприклад, надзвичайно швидкі послідовні транзакції можуть бути ознакою шахрайства або ботнетів.

Аналіз поведінки користувачів та адрес важливий для виявлення аномальних дій. Це включає в себе звичайну поведінку в адресах, патерни витрат, найбільш часті контрагенти та інші ознаки.

Аналіз графів транзакцій та зв'язків між адресами може виявити складні фінансові схеми та потенційно незаконні операції. Графова база даних може розкривати патерни, які є складні для виявлення в інший спосіб.

Машинне навчання та алгоритми глибинного навчання можуть бути використані для аналізу великих обсягів даних та виявлення аномалій на основі складних залежностей та патернів.

В деяких випадках використовуються спеціалізовані ознаки, такі як параметри транзакцій (наприклад, комісія), інформація про блоки, типи транзакцій та багато інших.

Визначення ключових параметрів та ознак для виявлення незаконних операцій з криптовалютою є складним завданням, і воно зазвичай вимагає комбінації різних методів та підходів. Сучасні технології та аналітичні інструменти стають все більш потужними у виявленні фінансових аномалій та запобіганні криптовалютним злочинам.

Обґрунтування важливості виявлення відхилень від незвичної поведінки для забезпечення кібербезпеки та захисту даних.

Значення виявлення відхилень. Виявлення відхилень від нормальної поведінки є ключовим компонентом у сфері кібербезпеки. Цей процес включає аналіз активності системи, мережі або користувачів для ідентифікації дій, які відрізняються від звичайних патернів. Такі відхилення часто можуть вказувати на можливі безпекові порушення, такі як вторгнення в систему, шкідливі програми або інші загрози.

Виявлення відхилень дозволяє організаціям швидко реагувати на потенційні загрози, мінімізуючи ризик пошкодження або втрати даних. Чим швидше вдається виявити несанкціоновану діяльність, тим менше шансів, що атакуючі зможуть завдати значної шкоди.

У сучасному світі де дані є новою валютою, захист конфіденційності цих даних є критично важливим. Виявлення відхилень допомагає запобігти несанкціонованому доступу до конфіденційної інформації, тим самим захищаючи особисті дані користувачів та комерційну інформацію компаній.

Ефективні системи виявлення відхилень можуть підвищити довіру користувачів та бізнес-партнерів до організації. Це демонструє, що компанія серйозно ставиться до захисту інформації та готова інвестувати в передові технології та процедури безпеки.

Кіберзагрози постійно еволюціонують, тому системи виявлення відхилень повинні бути гнучкими та адаптивними. Вони дозволяють організаціям швидко оцінювати нові та незнайомі види атак, адаптуючись до змін в кіберпросторі.

Аналіз відхилень також може виявити потенційні слабкі місця в інформаційних системах та процесах організації. Це надає можливість для покращення внутрішніх процедур та політик, зменшуючи ризик внутрішніх помилок або витоків інформації.

Завдяки цим аспектам, виявлення відхилень від нормальної поведінки стає ключовим елементом у стратегії забезпечення кібербезпеки та захисту важливих даних в цифровому світі.

Аналіз можливих викликів, з якими стикаються системи виявлення відхилень, включає декілька ключових аспектів:

1. Велика кількість даних. Одним із значних викликів є обробка та аналіз великих обсягів даних. Системи виявлення відхилень мають бути здатні ефективно обробляти велику кількість інформації, що постійно генерується різними джерелами.

2. З огляду на швидкість, з якою відбуваються кібератаки, системи виявлення відхилень повинні працювати в реальному часі або з мінімальною затримкою, щоб своєчасно виявляти та реагувати на потенційні загрози.

3. Важливим аспектом є мінімізація помилкових позитивних та помилкових негативних сигналів. Помилкові позитивні результати можуть призвести до непотрібних перерв у роботі, тоді як помилкові негативні результати можуть дозволити справжнім загрозам залишитися непоміченими.

4. Кіберзагрози постійно еволюціонують, тому системи мають бути гнучкими та здатними адаптуватися до нових видів атак. Це вимагає постійного оновлення знань та алгоритмів.

5. Щоб бути ефективними, системи виявлення відхилень повинні інтегруватися з іншими інструментами та системами кібербезпеки, такими як брандмауери, антивірусні програми, та системи управління подіями безпеки.

6. При обробці великих обсягів даних, особливо тих, що включають особисту інформацію, системи виявлення відхилень повинні дотримуватися законодавчих та етичних норм щодо приватності.

7. В багатьох випадках, організації можуть мати обмежені ресурси, як фінансові, так і технічні, для впровадження та підтримки ефективних систем виявлення відхилень.

8. Ефективне управління та налаштування систем вимагає наявності кваліфікованих фахівців з глибокими знаннями в області кібербезпеки, що може бути викликом для багатьох організацій.

Ці виклики потребують постійної уваги та інноваційних рішень з боку фахівців у сфері кібербезпеки, щоб системи виявлення відхилень залишалися ефективними в динамічному і постійно розвиваючомуся ландшафті кіберзагроз.

Моніторинг поведінки користувачів і виявлення відхилень від звичної поведінки є важливими елементами в стратегії забезпечення кібербезпеки. Це дозволяє своєчасно ідентифікувати потенційні загрози та реагувати на них до того, як вони спричинять серйозні збитки. Використання алгоритмів машинного навчання та штучного інтелекту в таких системах сприяє підвищенню точності та ефективності виявлення аномалій. Проте, важливо також звертати увагу на етичні аспекти та приватність даних при розробці та впровадженні цих систем. В кінцевому підсумку, збалансування між ефективним моніторингом та захистом приватності є ключовим для створення довіри та безпечного цифрового середовища.

2.2 Використання штучного інтелекту для виявлення незаконних операцій

Штучний інтелект (ШІ) [16] відноситься до систем, що імітують людську інтелектуальну поведінку, таку як навчання, аналіз та вирішення проблем. У контексті виявлення незаконних операцій, ШІ може виявляти аномалії, виконувати глибокий аналіз даних та ідентифікувати потенційні шахрайські діяльності. Типи алгоритмів ШІ, що використовуються для виявлення незаконних операцій: Це включає навчання з підкріпленням, навчання під наглядом, та навчання без нагляду. Кожен з цих типів алгоритмів має свої особливості та способи застосування для виявлення аномалій та шахрайських дій. Застосування машинного навчання у виявленні фінансових злочинів: Машинне навчання дозволяє системам ШІ самостійно вчитися з даних, виявляючи закономірності та аномалії, які можуть вказувати на незаконні операції. Це особливо корисно у фінансових секторах, де потрібно аналізувати великі обсяги транзакцій. Детекція аномалій і поведінкова аналітика: ШІ використовується для ідентифікації аномальної поведінки в транзакційних даних. Це включає аналіз відхилень від звичайних патернів поведінки, що може вказувати на шахрайські або інші незаконні дії. Інтеграція ШІ з іншими технологіями: ШІ часто інтегрується з іншими технологіями, такими як великі дані (Big Data) і блокчейн, для підвищення ефективності виявлення та аналізу

незаконних операцій. Етичні та юридичні аспекти: При використанні ШІ для виявлення незаконних операцій важливо враховувати етичні та правові норми, особливо стосовно конфіденційності даних та приватності. Виклики та обмеження: Це включає визнання потенційних викликів, таких як помилкові позитивні результати, необхідність великих датасетів для навчання, та складності у тлумаченні результатів, що генеруються ШІ.

Ці аспекти становлять основу для розуміння того, як штучний інтелект може бути застосований для ефективного виявлення та протидії незаконним фінансовим операціям.

Початкові стадії розвитку ШІ: Історія застосування штучного інтелекту (ШІ) у виявленні фінансових злочинів починається з ранніх експериментів у машинному навчанні та обробці даних. Це включало базові алгоритми, здатні аналізувати та виявляти незвичайні патерни в фінансових даних.

З часом, як технології ШІ та машинного навчання розвивалися, з'явилися більш складні алгоритми. Це дозволило проводити більш точний аналіз даних, ідентифікувати складніші шахрайські схеми та використовувати прогнозування для виявлення потенційних ризиків. Введення нейронних мереж та глибинного навчання значно підвищило здатність ШІ розпізнавати складні візерунки та здійснювати більш тонкий аналіз даних. Це значно покращило ефективність виявлення фінансових злочинів. ШІ став використовуватися для ідентифікації складних схем, таких як відмивання грошей та фінансування тероризму, що часто включають складні та приховані транзакції. З часом ШІ адаптувався до нових видів шахрайства, що виникають у постійно змінюваному фінансовому ландшафті. Це включало розробку спеціалізованих систем для виявлення шахрайства в онлайн-платежах, криптовалютах та інших цифрових фінансових інструментах. Сучасні системи ШІ часто інтегруються з іншими технологіями, такими як блокчейн і великі дані, для забезпечення більш комплексного підходу до виявлення та запобігання фінансових злочинів. Розвиток ШІ у виявленні фінансових злочинів продовжується, з новими викликами, такими як необхідність захисту конфіденційності даних, подолання юридичних та

регуляторних бар'єрів, і постійна адаптація до нових методів шахрайства (таблиця 2.1).

Таблиця 2.1- Методи машинного навчання та аналізу даних для виявлення незаконних операцій" включає декілька ключових елементів

Методи	Опис
1	2
1. Основи машинного навчання у контексті виявлення незаконних операцій	Вивчення основних типів машинного навчання, включаючи навчання під наглядом, навчання без нагляду, та навчання з підкріпленням, та як кожен з цих підходів застосовується для ідентифікації потенційних незаконних операцій.
2. Алгоритми класифікації та регресії	Дослідження, як алгоритми класифікації (наприклад, рішучі дерева, випадкові ліси, нейронні мережі) та регресії використовуються для прогнозування та виявлення аномальних фінансових транзакцій.

Продовження таблиці 2.1

1	2
3. Обробка великих даних для виявлення шахрайства	Кластеризації, які можуть виявити незвичайні патерни, що можуть вказувати на незаконні операції. Розгляд, як сучасні технології обробки великих даних, такі як Apache Hadoop та Spark, використовуються для ефективного аналізу великих наборів даних, щоб ідентифікувати потенційне шахрайство.
4. Використання часових рядів для виявлення фінансових злочинів	Аналіз, як часові ряди та їх властивості (такі як тренди, сезонність) можуть бути аналізовані для виявлення незаконних фінансових дій.
5. Інтеграція з іншими системами	Огляд, як методи машинного навчання інтегруються з традиційними системами управління ризиками та виявлення шахрайства, а також з новими технологіями, такими як блокчейн.
6. Етичні та юридичні аспекти	Обговорення етичних та юридичних викликів, пов'язаних з використанням машинного навчання для виявлення шахрайства, особливо в контексті конфіденційності та захисту даних.

Ця тема охоплює різноманітні аспекти використання машинного навчання та аналітики даних у складному процесі ідентифікації та запобігання незаконним фінансовим операціям.

Штучний інтелект [16] відіграє важливу роль у боротьбі з відмиванням грошей (AML) та фінансуванням тероризму (CFT). Ось детальний опис ключових аспектів цієї теми:

Визначення проблеми: Відмивання грошей та фінансування тероризму є складними злочинами, які часто включають різноманітні фінансові інструменти та канали. ШІ може допомогти в ідентифікації підозрілих патернів та транзакцій, які можуть бути пов'язані з цими діяльностями.

Алгоритми машинного навчання для аналізу даних: Алгоритми машинного навчання, такі як навчання з підкріпленням, навчання під наглядом та навчання без нагляду, використовуються для аналізу фінансових транзакцій. Ці алгоритми можуть виявляти аномалії, які вказують на потенційне відмивання грошей або фінансування тероризму.

Детекція аномалій та поведінковий аналіз: ШІ використовується для ідентифікації аномальної поведінки або відхилень від звичайних патернів транзакцій. Наприклад, виявлення незвичайно великих транзакцій, частих переказів коштів між рахунками, або транзакцій, що виконуються в країнах з високим ризиком.

ШІ у забезпеченні відповідності нормативним вимогам: ШІ може автоматизувати процеси моніторингу відповідності нормативним вимогам, допомагаючи фінансовим установам виявляти та звітувати про підозрілі діяльності відповідно до законодавства про AML/CFT.

Аналіз великих даних для виявлення складних схем: ШІ може обробляти та аналізувати величезні обсяги даних з різних джерел для виявлення складних схем відмивання грошей або фінансування тероризму, які були б недоступні для традиційних методів аналізу.

Неперервне навчання та адаптація: ШІ може постійно навчатися та адаптуватися до нових методів відмивання грошей та фінансування тероризму, вдосконалюючи свою здатність виявляти нові види злочинів.

Етичні та приватні аспекти: При використанні ШІ для виявлення AML/CFT важливо враховувати приватність даних і етичні міркування, особливо в контексті обробки особистих фінансових інформацій.

Інтеграція з іншими системами та технологіями: Ефективне використання ШІ часто вимагає інтеграції з іншими технологіями, такими як блокчейн або системи кібербезпеки, для створення більш повного рішення.

Використання ШІ у боротьбі з відмиванням грошей та фінансуванням тероризму є перспективним напрямком, який допомагає фінансовим установам та регулюючим органам більш ефективно ідентифікувати та протидіяти цим злочинам.

Застосування штучного інтелекту (ШІ) в аналізі криптовалют та блокчейн транзакцій відкриває нові можливості для підвищення прозорості, безпеки та ефективності в цій швидко розвиваючийся галузі. Ось детальний опис цієї теми:

Моніторинг та аналіз транзакцій: ШІ може використовуватися для моніторингу та аналізу транзакцій у блокчейні, допомагаючи виявляти підозрілі діяльності, такі як шахрайство, відмивання грошей, або інші незаконні операції. Алгоритми машинного навчання можуть виявляти аномалії, які не відповідають звичайним патернам поведінки.

Прогнозування цін на криптовалюти: ШІ може аналізувати великі обсяги даних, включаючи ринкові тренди, новини, соціальні медіа, та інші індикатори, щоб робити прогнози щодо майбутніх цін на криптовалюти.

Безпека блокчейн та смарт-контрактів: ШІ може використовуватися для аналізу та вдосконалення безпеки блокчейн мереж та смарт-контрактів, виявляючи вразливості або потенційні точки злому.

Оптимізація майнінгу: ШІ також може допомогти в оптимізації процесів майнінгу криптовалют, аналізуючи та прогнозуючи найбільш ефективні способи для видобутку та використання ресурсів.

Виявлення шахрайських ICOs та токенів: З допомогою аналітики даних та машинного навчання, ШІ може допомогти в ідентифікації потенційно шахрайських ініціатив ICO (первинне розміщення монет) або підозрілих токенів.

Ідентифікація трендів та взаємозв'язків на ринку криптовалют: ШІ може аналізувати тренди на ринку криптовалют, виявляючи взаємозв'язки між різними активами та вплив зовнішніх подій на ринок.

Аналіз соціальних медіа та впливу на криптовалютний ринок: ШІ може використовувати дані з соціальних медіа для аналізу сентименту інвесторів та його впливу на ціни криптовалют.

Регуляторний нагляд та звітність: ШІ може сприяти автоматизації та покращенню процесів регуляторного нагляду та звітності для криптовалютних компаній, допомагаючи їм відповідати нормативним вимогам.

Застосування ШІ у сфері криптовалют та блокчейн надає потужні інструменти для аналізу, прогнозування, та підвищення безпеки, відкриваючи нові можливості для інновацій та розвитку у цій динамічній галузі.

Одним з головних викликів у використанні ШІ для виявлення незаконних операцій є забезпечення високої точності при мінімальній кількості помилкових позитивних сигналів. Надмірна кількість помилкових спрацьовувань може призвести до непотрібного втручання в законні фінансові операції та зниження довіри користувачів. Ефективність ШІ сильно залежить від якості та кількості доступних даних. Недостатність або низька якість даних може вплинути на точність виявлення незаконних операцій. Крім того, існує ризик упередженості в даних, що може спотворити результати аналізу ШІ. Шахраї постійно розвивають нові методи для обходу систем виявлення. Це створює виклик для ШІ у вигляді необхідності постійного оновлення та навчання для ефективного виявлення нових видів шахрайських схем. Використання ШІ для аналізу фінансових транзакцій ставить під питання приватність та конфіденційність даних. Збір та аналіз великих обсягів персональних даних вимагають ретельного врахування юридичних та етичних норм. Результати, отримані з використанням ШІ, часто можуть бути складними для інтерпретації. Це може ускладнити зрозуміння причин, чому певні транзакції були позначені як підозрілі. Розробка та впровадження ефективних систем ШІ вимагає значних фінансових та технічних ресурсів. Це може бути значною перешкодою для малих та середніх підприємств. Використання ШІ у фінансовій сфері підпадає під строгі

регуляторні вимоги. Забезпечення відповідності цим нормам може бути складним, особливо в умовах постійно змінюваного регуляторного ландшафту.

ШІ надає значні переваги у виявленні та протидії незаконним фінансовим операціям, але його ефективність обмежується рядом викликів. Вирішення цих викликів вимагає постійного технологічного розвитку, вдосконалення алгоритмів, забезпечення захисту даних та адаптації до змінюваних методів шахрайства.

Майбутнє ШІ у виявленні злочинів обіцяє ще більш глибокий аналіз даних. Завдяки розвитку алгоритмів машинного навчання, ШІ зможе ефективніше аналізувати великі набори даних, виявляючи складні взаємозв'язки та шаблони, які можуть вказувати на злочинну діяльність. ШІ має потенціал значно покращити прогнозування злочинності, використовуючи історичні дані для ідентифікації областей та періодів з підвищеним ризиком злочинних дій. Це дозволить правоохоронним органам більш ефективно розподіляти свої ресурси. З розвитком ШІ можна очікувати покращення методів виявлення відмивання грошей та фінансування тероризму. Алгоритми ШІ зможуть швидше ідентифікувати складні фінансові мережі та незвичайні транзакції, що є ознаками злочинної діяльності. Зі зростанням кіберзлочинності, ШІ стане ключовим інструментом у її виявленні та протидії. Використання ШІ для аналізу мережевих даних допоможе виявляти шкідливі програми, фішингові атаки та інші види кіберзлочинів. Методи розпізнавання облич та інші біометричні технології, що використовують ШІ, будуть вдосконалюватися для ідентифікації підозрюваних та розшуку злочинців. Це також включає вдосконалення систем відеонагляду. ШІ буде ще більше інтегрований з іншими технологіями, такими як Інтернет речей (IoT) та блокчейн, для створення більш ефективних систем виявлення та запобігання злочинам. По мірі розвитку та впровадження ШІ у виявленні злочинів, виникнуть нові етичні та правові виклики, особливо стосовно приватності та зловживання даними. Буде важливо розвивати ШІ відповідно до етичних норм і правових вимог.

3. ІНТЕГРАЦІЯ ТА ДОСЛІДЖЕННЯ АЛГОРИТМІВ ДЛЯ ВИЯВЛЕННЯ НЕЗАКОННИХ ОПЕРАЦІЙ З КРИПТОВАЛЮТАМИ

3.1 Оптимізація алгоритмів для виявлення незаконних операцій

В сучасному світі, де набувають стрімкого розвитку цифрові технології, виникає гостра потреба в ефективних інструментах для боротьби з незаконними фінансовими операціями. Особливу увагу привертає сфера криптовалют, яка, через свою анонімність та децентралізацію, часто стає об'єктом для незаконних маніпуляцій та шахрайств які зображені на рисунку 3.1. У цьому контексті, розробка та оптимізація алгоритмів для виявлення незаконних операцій стає ключовим напрямком, який вимагає глибоких знань у сфері штучного інтелекту та машинного навчання.

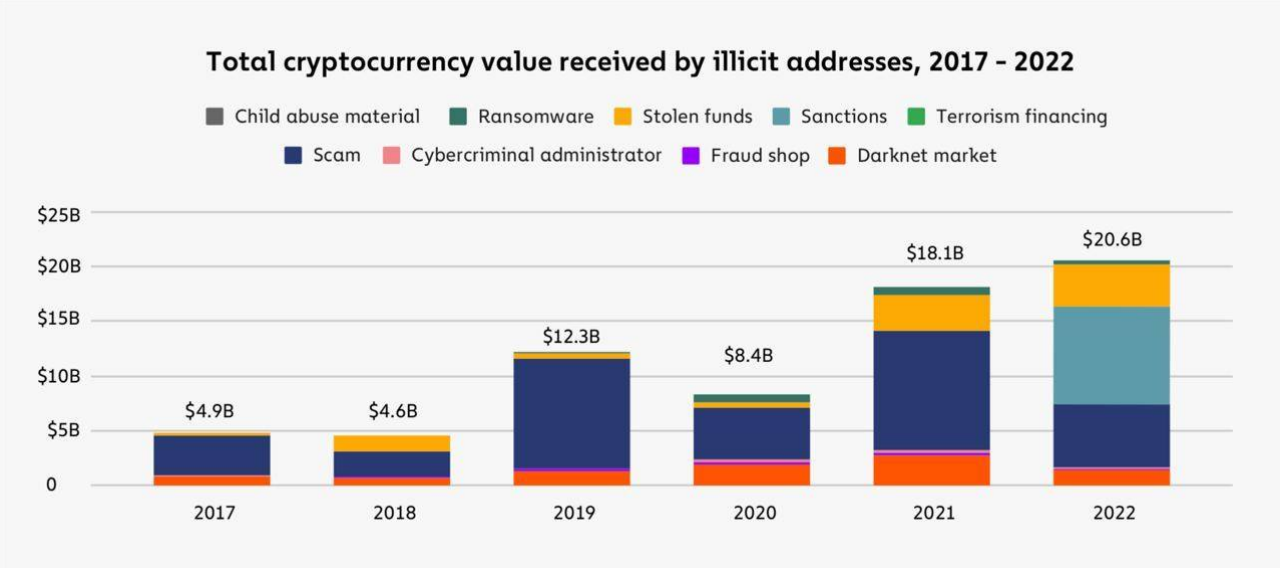

Рисунок 3.1 - Незаконні операції з криптовалютою в 2022 році

Цей процес включає не тільки створення алгоритмів, здатних ідентифікувати потенційні шахрайські дії, але й їх постійну оптимізацію для адаптації до постійно змінюваних методів шахрайства. Важливість цього завдання не може бути переоцінена, адже воно спрямоване не лише на захист інтересів окремих інвесторів, але й на підтримку загальної стабільності та безпеки фінансових ринків.

Розробка ефективних алгоритмів [17] вимагає глибокого розуміння специфіки криптовалютних транзакцій, а також знань у сфері даних, статистики та програмування. Це включає використання складних математичних моделей та обчислювальних технік для аналізу великих обсягів даних, що вимагає постійної уваги до деталей та інноваційного підходу.

Розглянемо ключові аспекти процесу розробки та оптимізації алгоритмів для виявлення незаконних операцій, включаючи їх структуру, функціональність, а також виклики та перспективи, що стоять перед дослідниками та розробниками у цій сфері.

Визначення ключових ознак та показників, які вказують на потенційно незаконні транзакції - це важлива тема у сфері криптовалют та блокчейн-технологій. Для ефективного виявлення транзакцій, які можуть бути пов'язані зі злочинністю, фінансовими злочинами або іншими незаконними діями, необхідно враховувати різні ознаки та показники. Давайте розглянемо детальніше, які ключові ознаки та показники можуть свідчити про потенційно незаконні транзакції:

– великі суми грошей. Зазвичай великі суми грошей привертають увагу, особливо якщо вони відправляються чи отримуються від певних адрес або користувачів;

– фрагментовані транзакції. Велика кількість невеликих транзакцій може свідчити про спробу приховати реальний обсяг операцій або відмити гроші. Адреси, пов'язані зі злочинністю: Використання адрес, які раніше були пов'язані зі злочинною діяльністю, може свідчити про намагання приховати походження коштів. Адреси з низьким рівнем активності: Адреси, які довгий час не брали участі в транзакціях, можуть бути підозрілими, особливо якщо вони виявляють активність без відомих причин;

– швидкі транзакції. Транзакції, які відбуваються дуже швидко, можуть бути пов'язані зі злочинною діяльністю, такою як арбітраж або передача активів для уникнення виявлення;

– транзакції в нічний час. Активність під час нічного часу може вказувати на намагання уникнути відстеження;

– нетипові зв'язки. Аналіз зв'язків між адресами та користувачами, які не мають сенсу з фінансової точки зору, може свідчити про незаконну діяльність;

– мультиплікатори адрес. Використання однієї адреси для кількох транзакцій може бути показником уникнення виявлення;

– зміна патернів поведінки: Різка зміна звичайних патернів поведінки, таких як пересилання коштів на незвичні адреси чи користувачів, може бути показником незаконності;

– часті міжнародні транзакції. Часті міжнародні перекази грошей можуть вказувати на спробу вивезення коштів за межі країни або уникнення податків;

– незвичайні коментарі до транзакцій. Наявність незвичайних коментарів до транзакцій може вказувати на незаконні мети;

– транзакції з темними ринками. Виявлення транзакцій, які пов'язані з темними ринками або нелегальними діями;

– аналіз транзакцій у зв'язку з іншими подіями. Розгляд транзакцій в контексті інших подій або новин може допомогти виявити незвичайність. Ефективне виявлення потенційно незаконних транзакцій вимагає поєднання декількох параметрів та ознак, а також використання аналітичних методів, таких як машинне навчання та графова аналітика. Важливо постійно вдосконалювати аналітичні інструменти та оновлювати алгоритми для виявлення незаконних операцій у світі криптовалют. В сучасному світі більшість фінансових транзакцій здійснюється цифровими шляхами, і це створює величезний обсяг даних. Аналіз цих даних може допомогти виявити аномальну поведінку, фінансові злочини та шахрайство. Розробка алгоритмів машинного навчання та штучного інтелекту для аналізу даних транзакцій стала необхідною для ефективного контролю та безпеки фінансових операцій;

– збір та підготовка даних. Першим кроком у розробці алгоритмів машинного навчання є збір та підготовка даних. Для аналізу транзакцій необхідно зібрати велику кількість даних про транзакції, включаючи інформацію про суми, адреси, часові штампи та інші параметри;

– вибір моделей машинного навчання. Для аналізу даних транзакцій використовуються різні моделі машинного навчання, такі як класифікаційні, кластерні та регресійні моделі. Вибір моделей залежить від конкретних завдань аналізу;

– фічі-інжиніринг - це процес створення нових ознак на основі існуючих даних. Важливо створити репрезентативні та інформативні ознаки для покращення точності аналізу;

– навчання та підгонка моделей. Після підготовки даних та вибору моделей проводиться процес навчання та підгонка моделей. Моделі навчаються на історичних даних та використовуються для передбачення майбутніх транзакцій;

– виявлення аномалій. Основним завданням алгоритмів машинного навчання та штучного інтелекту є виявлення аномальних транзакцій. Аномалії можуть включати в себе шахрайство, відмивання грошей, незаконне фінансування та інші незвичайні операції;

– валідація та підтвердження результатів. Після виявлення потенційно аномальних транзакцій проводиться процес валідації та підтвердження результатів. Це може включати в себе додатковий аналіз та перевірку даних;

– впровадження в реальний час. Розроблені алгоритми та моделі мають бути інтегровані в реальний час для негайного виявлення незаконних транзакцій;

– постійне оновлення та вдосконалення. Фінансові ринки та сфера криптовалют постійно змінюються. Тому важливо постійно оновлювати та вдосконалювати алгоритми машинного навчання та штучного інтелекту, щоб вони залишалися ефективними;

– питання безпеки та конфіденційності. Збір та аналіз фінансових даних є чутливою справою. Забезпечення безпеки та конфіденційності даних є важливим аспектом розробки алгоритмів.

Розробка алгоритмів машинного навчання та штучного інтелекту для аналізу даних транзакцій має великий потенціал для підвищення безпеки

фінансових операцій та виявлення незаконних дій у світі криптовалют та фінансових ринків. Ця тема є актуальною і вимагає подальших досліджень та розробок для досягнення найкращих результатів.

Оптимізація алгоритмів для підвищення точності виявлення та зменшення кількості помилкових спрацьовувань - це важлива тема в сфері аналізу фінансових операцій та виявлення незаконних дій. Підвищення точності виявлення та зменшення кількості помилкових спрацьовувань в алгоритмах має велике значення для ефективного контролю та безпеки фінансових транзакцій. Давайте розглянемо, які аспекти включає в себе ця тема: Пошук оптимальних параметрів є одним з перших кроків у процесі оптимізації алгоритмів є пошук оптимальних параметрів. Це включає в себе налаштування гіперпараметрів моделей машинного навчання, таких як глибина дерева у випадковому лісі або коефіцієнти регуляризації в логістичній регресії. Використання оптимальних параметрів може значно підвищити точність алгоритмів:

– збільшення обсягу даних для навчання моделей може допомогти підвищити їхню точність. Це може включати в себе збільшення вибірки даних або використання додаткових даних для навчання;

– підвищення точності моделей можливе шляхом створення нових та інформативних ознак з використанням наявних даних. Цей процес включає аналіз і відбір ключових ознак, а також генерацію нових на підставі наявних даних;

– використання ансамблів моделей, таких як випадковий ліс або градієнтний бустинг, може підвищити точність прогнозів. Комбінація декількох моделей може зменшити кількість помилкових спрацьовувань;

– постійне навчання моделей на нових даних може допомогти підтримувати їхню актуальність та ефективність в умовах змінюючогося середовища. Актуалізація моделей відповідно до останніх трендів і нових типів шахрайства є важливим аспектом оптимізації;

– використання статистичних методів, таких як тести на статистичну значущість, може допомогти виявити статистично значущі аномалії та визначити їхні причини;

– для виявлення незаконних транзакцій важливо мати можливість обробляти дані в реальному часі. Оптимізація алгоритмів для роботи в режимі реального часу може підвищити ефективність виявлення;

– перевірка точності та ефективності оптимізованих алгоритмів через валідацію та тестування на великій кількості даних є важливим кроком.

Оптимізація алгоритмів для підвищення точності виявлення та зменшення кількості помилкових спрацьовувань є надзвичайно важливою для забезпечення безпеки фінансових транзакцій та виявлення незаконних дій. Ця тема вимагає поєднання інженерії даних, статистики, машинного навчання та обчислювальної потужності для досягнення оптимальних результатів.

3.2 Інтеграція алгоритмів у криптовалютні платформи та системи безпеки

Швидкість і зручність криптовалют [19] в поєднанні з їхньою анонімністю можуть призвести до різноманітних фінансових злочинів, таких як шахрайство, відмивання грошей та інші види фінансової маніпуляції. У цьому контексті, інтеграція алгоритмів у криптовалютні платформи та системи безпеки стає важливим кроком у забезпеченні захисту та стійкості цих цифрових активів.

Завдяки поєднанню технологій машинного навчання, штучного інтелекту та аналізу даних, інтегровані алгоритми мають здатність вчасно виявляти незвичні та потенційно шкідливі транзакції, а також ідентифікувати аномалії у фінансових операціях. Це сприяє запобіганню злочинним діям та забезпечує безпеку користувачів, інвесторів і фінансових інституцій.

У цьому динамічному середовищі, де кількість криптовалютних транзакцій швидко зростає, важливо мати ефективні та інтелігентні системи, які відсіюватимуть незаконні дії та аномалії в режимі реального часу. Інтеграція передових алгоритмів у криптовалютні платформи та системи безпеки сприяє підвищенню довіри до цих технологій та ринків.

Інтеграція розроблених алгоритмів у існуючі системи криптовалютних бірж, гаманців та інших платформ є ключовим етапом для покращення безпеки та ефективності цих цифрових сервісів. У зв'язку зі зростанням популярності криптовалют та збільшенням обсягів транзакцій, необхідність у надійних інструментах для виявлення аномалій та контролю фінансових операцій стає критичною. Вбудовування алгоритмів вже розробленого програмного забезпечення дозволяє відповідати цим викликам та забезпечує більш високий рівень безпеки та надійності в цьому секторі.

Основні аспекти цієї теми включають:

– адаптація до існуючих інфраструктур: Вбудовування алгоритмів повинно відбуватися в контексті існуючих технічних рішень, що вимагає адаптації та сумісності з існуючими системами;

– забезпечення високої швидкості та надійності: Криптовалютні ринки працюють у режимі реального часу, тому вбудовані алгоритми повинні бути вкрай швидкими та надійними для забезпечення безперебійної роботи;

– виявлення аномалій: Розроблені алгоритми повинні бути спроможні виявляти незвичайну поведінку та можливі аномалії в операціях, що допоможе запобігти шахрайським діям;

– скалабельність [18]: Системи криптовалют можуть мати велику кількість користувачів та обсяги транзакцій, тому вбудовані алгоритми повинні бути скалабельними та здатними працювати в умовах великого навантаження;

– забезпечення конфіденційності та безпеки даних: Інтегровані алгоритми повинні дотримуватися найвищих стандартів безпеки та захисту конфіденційної інформації користувачів;

– сумісність з регуляторними вимогами: У багатьох країнах існують регуляторні вимоги до криптовалютних платформ, і вбудовані алгоритми повинні відповідати цим вимогам;

– постійне оновлення та підтримка: Криптовалютні ринки постійно змінюються, тому вбудовані алгоритми повинні підтримуватися та оновлюватися відповідно до нових викликів та тенденцій.

Вбудовування розроблених алгоритмів у системи криптовалютних бірж, гаманців та інших платформ є важливим кроком для забезпечення безпеки та надійності цих сервісів. Воно сприяє залученню інвесторів, забезпечує довіру користувачів і регуляторів до цього ринку та сприяє його подальшому розвитку.

Реалізація систем моніторингу та повідомлень для оперативного реагування на підозрілі транзакції є однією з ключових складових безпеки та ефективності функціонування криптовалютних платформ і бірж. У світі криптовалют, де транзакції здійснюються в режимі реального часу, важливо мати системи, які можуть швидко виявляти та реагувати на потенційно небезпечні операції. Системи моніторингу постійно аналізують дані про транзакції, що відбуваються на платформі. Вони аналізують різні параметри, такі як обсяги, час виконання та місцезнаходження користувачів. Також системи моніторингу використовують алгоритми для виявлення аномальних операцій, які можуть вказувати на можливий обман або фінансовий злочин. Для визначення, що операція є підозрілою, системи використовують різні критерії, такі як надзвичайно великий обсяг транзакції, незвичайно швидка послідовність операцій або надмірне використання певних функцій платформи. Якщо система моніторингу виявляє підозрілу операцію, вона автоматично сповіщає адміністраторів чи відповідний відділ безпеки для подальшої реакції. Ця реакція може включати в себе призупинення транзакції, блокування акаунта користувача чи подальше розслідування. Важливим аспектом є швидкість реагування на підозрілі операції. Системи повинні бути здатні вчасно виявляти та реагувати на потенційні загрози. Багато країн мають регуляторні вимоги щодо моніторингу та повідомлень про фінансові операції. Системи повинні дотримуватися цих вимог для забезпечення відповідності законодавству. Сфера криптовалют постійно змінюється, тому системи моніторингу та реагування повинні підтримуватися та оновлюватися відповідно до нових загроз та технологічних розвитків. Реалізація систем моніторингу та повідомлень для оперативного реагування на підозрілі

транзакції відіграє важливу роль у забезпеченні безпеки та надійності криптовалютних платформ. Вони допомагають вчасно виявляти та запобігати фінансовим злочинам, зміцнюють довіру користувачів та сприяють розвитку цієї сфери.

Забезпечення відповідності алгоритмів законодавчим нормам та регуляторним вимогам є важливим аспектом розробки та впровадження систем моніторингу та аналізу фінансових операцій, особливо в галузі криптовалют. Оскільки ця сфера підлягає строгим регуляторним обмеженням та періодичним змінам в законодавстві, важливо мати алгоритми, які відповідають всім вимогам та стандартам. Відповідність анти-відмиванню грошей [20] (AML) і збору податків (KYC). Важливо мати алгоритми, які дозволяють виконувати обов'язкові перевірки клієнтів (KYC) та виявляти та запобігати операціям, які можуть бути пов'язані з відмиванням грошей (AML). Криптовалютні платформи та інші учасники ринку повинні відповідати вимогам до ліцензування і реєстрації, які можуть варіюватися в залежності від регіону. Алгоритми мають забезпечувати високий рівень захисту особистих даних користувачів, відповідно до вимог Закону про захист даних. Важливо проводити регулярні оцінки ризиків і змінювати алгоритми відповідно до нових викликів та змін в законодавстві. Алгоритми повинні бути надійними та стабільними, щоб не порушувати вимоги безпеки і законодавство. З урахуванням змін в законодавстві та регуляторних вимогах, алгоритми повинні підтримуватися та оновлюватися відповідно до нових вимог. Алгоритми повинні включати заходи захисту від кібератак, оскільки фінансові сервіси завжди під загрозою. Важливо підтримувати відкрту комунікацію та співпрацю з регуляторами та відповідати на їхні запити на інформацію.

Забезпечення відповідності алгоритмів законодавчим нормам та регуляторним вимогам є важливим завданням у фінансовій сфері, особливо в контексті криптовалют. Розробка та впровадження таких алгоритмів допомагає зміцнити довіру користувачів, підтримувати законність операцій та забезпечити стабільність фінансових ринків.

3.3 Дослідження ефективності та покращення алгоритмів на основі практичного застосування

Дослідження ефективності та покращення алгоритмів на основі практичного застосування [21] стає важливою галуззю досліджень та розвитку.

Алгоритми використовуються в різних галузях, від штучного інтелекту до фінансів, медицини, технологій та інших. Вони допомагають вирішувати завдання, що раніше вважалися неможливими, оптимізувати робочі процеси та підвищувати продуктивність. Проте алгоритми також потребують постійної оцінки та вдосконалення, оскільки технології швидко розвиваються, а потреби ринку змінюються.

У даному дослідженні ми розглянемо аспекти аналізу та оцінки ефективності алгоритмів у практичних умовах. Ми дослідимо методи та метрики, які дозволяють визначити якість та продуктивність алгоритмів, а також інструменти для їх покращення. Ми також розглянемо конкретні практичні застосування алгоритмів у різних галузях та визначимо способи їхнього вдосконалення для досягнення кращих результатів.

Дослідження ефективності та покращення алгоритмів на основі практичного застосування є важливим напрямом в розвитку сучасних технологій та допомагає забезпечити їхню актуальність та відповідність потребам ринку. Від результатів таких досліджень залежить ефективність багатьох сучасних систем і технологій, і вони є ключовим чинником у досягненні успіху у цифровому світі.

Оцінка ефективності алгоритмів у реальних умовах та збір зворотного зв'язку є важливим етапом у процесі розробки та вдосконалення алгоритмів в різних областях, від штучного інтелекту до обробки даних та програмного забезпечення. Ця тема відображає необхідність не лише створити алгоритм, але й переконатися, що він працює ефективно та відповідає поставленим завданням у реальних умовах використання. Важливо визначити реальні сценарії використання для алгоритму. Це може бути вирішення конкретних завдань у сфері бізнесу, науки, медицини тощо. Необхідно розробити метрики, які

дозволять оцінити, наскільки алгоритм відповідає потребам у визначених сценаріях використання. Це можуть бути метрики швидкості, точності, робастності тощо. Для оцінки алгоритму у реальних умовах необхідно збирати дані про його функціонування та результати. Це може бути виконано за допомогою логування, моніторингу або спеціалізованих інструментів. Отримані дані про ефективність алгоритму повинні бути аналізовані для визначення його слабких і сильних сторін, а також виявлення можливостей для покращення. Збір зворотного зв'язку від користувачів або експертів є важливим елементом оцінки алгоритму. Відгуки та пропозиції можуть служити джерелом інформації для його вдосконалення. На основі отриманих даних та зворотного зв'язку можна розробити план покращення алгоритму, включаючи оптимізацію, розширення функціоналу або інші модифікації. Після внесення змін або покращень алгоритм повинен бути підданий повторному тестуванню та оцінці для перевірки ефективності покращень.

Оцінка ефективності алгоритмів у реальних умовах та збір зворотного зв'язку є невід'ємною частиною процесу їхньої розробки та впровадження. Вона дозволяє переконатися, що алгоритми відповідають потребам та досягають практичних результатів, сприяючи подальшому розвитку та вдосконаленню технологій.

Адаптація та покращення алгоритмів на основі аналізу даних про успішно виявлені незаконні операції є складним та багатогранним процесом, який включає в себе кілька ключових етапів та аспектів:

– перший крок полягає в зборі даних про фінансові злочини, які вдалося виявити та припинити за допомогою існуючих алгоритмів. Ці дані можуть включати в себе інформацію про суми операцій, типи злочинів, методи обману, географічні дані, а також інші характеристики операцій та їхніх учасників;

– на основі зібраних даних проводиться оцінка ефективності існуючих алгоритмів у виявленні незаконних операцій. Ця оцінка включає в себе розрахунок різних метрик, таких як чутливість (здатність виявити справжні

незаконні операції), специфічність (здатність уникнути помилкових спрацьовувань), точність та інші;

– на основі результатів оцінки виявляються слабкі сторони існуючих алгоритмів та ідентифікуються можливості для їхнього покращення. Це може включати в себе розробку нових методів аналізу даних, застосування розширених алгоритмів машинного навчання, оптимізацію або впровадження нових функцій та показників для виявлення фінансових злочинів;

– фінансові злочини постійно змінюються та модернізуються, тому алгоритми повинні бути адаптовані до нових видів загроз та схем обману. Це може включати в себе вдосконалення алгоритмів для виявлення нових методів атак та шахрайства;

– ефективні алгоритми повинні працювати в режимі реального часу та мати здатність оперативно реагувати на підозрілі транзакції. Це може включати в себе розробку систем оповіщення та автоматичних заходів для блокування незаконних операцій;

– для ефективного боротьби з фінансовими злочинами, алгоритми можуть служити цінним інструментом для співпраці з правоохоронними органами та службами безпеки. Вони можуть надавати докази та аналітичну інформацію для розслідування фінансових злочинів.

Адаптація та покращення алгоритмів на основі аналізу даних про успішно виявлені незаконні операції є важливим елементом забезпечення фінансової безпеки та боротьби з фінансовими злочинами. Цей процес дозволяє покращувати ефективність та надійність систем виявлення та запобігання фінансовим злочинам, забезпечуючи більшу безпеку фінансових ринків та криптовалютних платформ.

Неперервне оновлення та вдосконалення алгоритмів для відповіді на зміни у методах ведення незаконних операцій є важливим завданням у сфері фінансової безпеки та боротьби з фінансовими злочинами. Оскільки злочинці постійно шукають нові способи обходу систем виявлення та лазейки в правилах, алгоритми повинні бути готові адаптуватися та реагувати на ці зміни.

Основні аспекти цієї теми включають: Моніторинг і виявлення нових загроз: Щоб відповідати на зміни у методах ведення незаконних операцій, алгоритми повинні постійно моніторити фінансові ринки та криптовалютні платформи на предмет нових загроз і нестандартних сценаріїв.

Аналіз злочинних схем: Важливо розбирати та аналізувати злочинні схеми та методи, які використовуються злочинцями для обману систем виявлення. Це допомагає розуміти їхні підходи та розробляти відповідні контрмери.

Розвиток нових алгоритмів та моделей: На основі аналізу нових загроз і методів, розробляються нові алгоритми та моделі виявлення фінансових злочинів. Вони можуть включати в себе методи машинного навчання, штучного інтелекту та аналітики даних.

Оптимізація та підвищення чутливості: Алгоритми повинні бути оптимізовані для роботи з великими обсягами даних та підвищення чутливості до підозрілих операцій, при цьому мінімізуючи кількість помилкових спрацьовувань.

Інтеграція з іншими системами безпеки: Алгоритми мають бути інтегровані з іншими системами безпеки та моніторингу для забезпечення комплексного підходу до виявлення та запобігання фінансовим злочинам.

Тестування та валідація: Перед впровадженням нових алгоритмів важливо провести тестування та валідацію їхньої ефективності в реальних умовах, щоб переконатися, що вони відповідають потребам та вимогам.

Оновлення правил та політик: Нові алгоритми можуть вимагати оновлення правил та політик виявлення фінансових злочинів для врахування їхніх можливостей та особливостей.

Неперервне оновлення та вдосконалення алгоритмів для відповіді на зміни у методах ведення незаконних операцій є необхідною складовою систем виявлення та запобігання фінансовим злочинам. Це допомагає забезпечити більшу ефективність та надійність систем фінансової безпеки та забезпечити захист фінансових ринків та криптовалютних платформ від нових загроз.

ВИСНОВОК

В еру стрімкого розвитку цифрових технологій, коли криптовалюти набувають все більшої ваги у світовій фінансовій системі, важливість виявлення незаконних операцій з криптовалютами стає ключовим фактором для забезпечення фінансової стабільності та боротьби зі злочинністю. Це виявляється не тільки важливим з точки зору забезпечення фінансової стабільності, але й є ключовим елементом у протидії злочинності. На сьогоднішній день криптовалютні ринки зазнають впливу різноманітних незаконних дій, від відмивання грошей до фінансування тероризму, що робить задачу виявлення та запобігання таким операціям складною та багатогранною.

Передові алгоритми, розроблені на основі штучного інтелекту, машинного навчання та блокчейн-технологій, стають ефективним інструментом у виявленні таких операцій. Вони дозволяють аналізувати величезні обсяги даних, виявляти нетипові патерни поведінки, відстежувати та ідентифікувати підозрілі транзакції, що є критично важливим для попередження незаконних фінансових дій. Ці технології дозволяють виявляти складні схеми, які можуть бути непомітні для традиційних методів моніторингу.

Ефективність цих алгоритмів значною мірою залежить від їх здатності адаптуватися до нових викликів та змін у способах проведення незаконних операцій. Це вимагає постійного оновлення та вдосконалення алгоритмів, а також широкої співпраці між фінансовими установами, правоохоронцями та регуляторами. Така співпраця не тільки допомагає виявляти нові схеми та методи злочинної діяльності, але й сприяє розвитку більш прозорих та безпечних ринків криптовалют.

Крім того, зростання криптовалютних ринків та поява нових видів цифрових активів створюють додаткові виклики для регулювання та моніторингу. Розробка ефективних законодавчих та нормативних рамок є важливою для забезпечення відповідності цих ринків сучасним вимогам безпеки та прозорості. Це включає в себе не тільки регулювання діяльності

криптовалютних бірж та валютних обмінників, але й удосконалення процесів ідентифікації користувачів та моніторингу транзакцій.

Освіта та підвищення обізнаності громадськості щодо криптовалют та потенційних ризиків, пов'язаних з їх використанням, є ще одним важливим аспектом. Інформаційні кампанії та освітні програми можуть допомогти зменшити ризики шахрайства та зловживань у цій сфері. Також важливо забезпечити доступ до якісної інформації про безпечне та відповідальне використання криптовалют, що допоможе користувачам уникнути потенційних фінансових втрат.

Загалом, використання передових алгоритмів для виявлення незаконних операцій із криптовалютами стає ключовим компонентом забезпечення фінансової безпеки та стабільності в цифрову епоху. В поєднанні з міжнародною співпрацею, розвитком нормативної бази, та освітніми ініціативами, ці алгоритми сприяють створенню міцної основи для безпечного та прозорого використання криптовалют, забезпечуючи при цьому захист прав користувачів та інвесторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bitcoin: що це таке і як працює в україні та світі [Електронний ресурс]. https://www.volynnews.com/news/economics/Bitcoin-shcho-tse-take-i-iak-pratsiuye-v-ukrayini-ta-sviti/

2. What Is Ethereum and How Does It Work? [Електронний ресурс]. https://www.investopedia.com/terms/e/ethereum.asp

3. Litecoin: everything you need to know about LTC [Електронний ресурс]. https://weareblox.com/en-eu/litecoin

4. Ripple Definition [Електронний ресурс]. https://www.investopedia.com/terms/r/ripple-cryptocurrency.asp

5. The Best, Safest Ways to Store Your Cryptocurrency: What You Need to Know [Електронний ресурс]. https://bitpay.com/blog/safest-ways-to-store-crypto/

6. Моніторинг обмінників WellCrypto – Ваш помічник для вибору оптимального курсу обміну! [Електронний ресурс]. https://www.rbc.ua/rus/news/monitoring-obminnikiv-pomichnik-viboru-optimalnogo-1683190913.html

7. Blockchain Facts: What Is It, How It Works, and How It Can Be Used [Електронний ресурс]. https://www.investopedia.com/terms/b/blockchain.asp

8. Кіберзлочинність: актуальна судова практика [Електронний ресурс]. https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika

9. Право на анонімність як невід'ємне право людини [Електронний ресурс]. http://www.pgp-journal.kiev.ua/archive/2018/2/30.pdf

10. Системи зберігання даних [Електронний ресурс]. https://it-dialog.com.ua/solutions/data-center-solutions/data-storage-systems.html

11. Blockchain [Електронний ресурс]. https://www.it.ua/knowledge-base/technology-innovation/blockchain

12. Тенденції розвитку блокчейну на 2023 рік [Електронний ресурс]. https://merehead.com/ua/blog/blockchain-industry-development-trends-2023/

13. Тренди блокчейну 2023 [Електронний ресурс]. https://www.eternitylaw.com/ua/novyny/blockchain-trends-2023/

14. 13 трендів криптовалютного ринку, до яких буде прикута увага лідерів індустрії у 2022 році [Електронний ресурс]. https://itc.ua/ua/articles/13-trendiv-kriptovalyutnogo-rinku-do-yakih-bude-prikuta-uvaga-lideriv-industriyi-u-2022-roczi/

15. Новітні технологічні тенденції у криптовалюті [Електронний ресурс]. http://surl.li/nihxy

16. Artificial Intelligence (AI): What It Is and How It Is Used [Електронний ресурс].https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp

17. Принципи та алгоритми створення автоматизованих інтелектуальних систем управління електронним банкінгом [Електронний ресурс]. https://finap.com.ua/pryntsypy-ta-algorytmy-stvorennya-avtomatyzovanyh-intelektualnyh-system-upravlinnya-elektronnym-bankingom/

18. Принцип роботи, Блокчейн ALEO [Електронний ресурс]. http://surl.li/nzmdi

19. Швидкість транзакцій криптовалюти 2022 [Електронний ресурс]. https://www.escrypto.com/uk/blog/cryptocurrency-transaction-speed-2022

20. Боротьба з відмиванням грошей: Що таке БВГ і чому це важливо [Електронний ресурс]. https://www.sas.com/ru_ua/insights/fraud/anti-money-laundering.html

21.Алгоритми та структури даних для початківців: переваги, методики вивчення та корисні ресурси [Електронний ресурс]. https://dan-it.com.ua/uk/blog/algoritmy-i-struktury-dannyh-dlja-nachinajushhih-preimushhestva-metodiki-izuchenija-i-poleznye-resursy/

22. Максимчук Р.О., Цаволик Т.Г. Налаштування та оцінка поширених програм по збору інформації транзакцій з криптовалютами "Автоматизація та комп’ютерно-інтегровані технології" (АКІТ-2023), Тернопіль, 2023. С. 137 - 138.

23. Максимчук Р.О., Цаволик Т.Г. Технологічні тренди в галузі криптовалют та блокчейну «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. С. 40 – 41.

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

(АКІТ – 2023)

23—25 лютого 2023 року

Тернопіль

Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2023), Тернопіль, 2023. -178 с.

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Адреса редакції:
Західноукраїнський національний університет
кафедра спеціалізованих комп'ютерних систем
вул. Олени Теліги 8, м. Тернопіль 46003

Контактний телефон
тел. (0352) 50-17-87

УДК 004.056.5

Максимчук Р.О.[1], Цаволик Т.Г.[1]

[1]Західноукраїнський національний університет

АНАЛІЗ ТА ОЦІНКА ПОШИРЕНИХ ПРОГРАМ ПО ЗБОРУ ІНФОРМАЦІЇ ТРАНЗАКЦІЙ З КРИПТОВАЛЮТАМИ

Вступ: В сучасному світі криптовалюти стають все більш популярними інструментами фінансових операцій, привертаючи увагу як інвесторів, так і дослідників. За останні роки зростає попит на програми, які збирають інформацію про транзакції з криптовалют, надаючи цінні дані та аналітичні висновки для розуміння ринкових тенденцій, виявлення шаблонів та визначення ризикових факторів. Однак, перед тим як використовувати такі програми, важливо провести аналіз та оцінку їхньої функціональності, безпеки, комплексності даних, використання зібраних даних, приватності та доступності. Цей аналіз допомагає користувачам усвідомити переваги та ризики, пов'язані з використанням таких програм.

Мета: Дослідження та оцінювати поширені програми по збору інформації транзакцій з криптовалют.

1. Аналіз поширених програм по збору інформації транзакцій з криптовалют

Дослідження програм по збору інформації транзакцій з криптовалютами є важливим завданням, щоб краще зрозуміти їхню функціональність, ефективність та вплив на користувачів. Основна мета такого дослідження полягає в аналізі та оцінці різних програм, які допомагають збирати, відстежувати та аналізувати дані про транзакції з криптовалютами. Дослідження може включати наступні аспекти:

- функціональність програм - які функції та можливості надають програми для збору інформації про транзакції, наприклад функції імпорту даних з криптовалютних бірж та гаманців, аналітичні інструменти, статистика та звіти, а також можливості податкової звітності.
- аналіз заходів, які програми вживають для захисту зібраної інформації, а також приватності користувачів, наприклад шифрування даних, захист від кібератак, анонімізація особистої інформації тощо.
- оцінка того, наскільки зручний та простий інтерфейс програми для користувачі, наприклад аналіз доступності функцій, легкість імпорту даних, навігацію та інші параметри, що впливають на зручність використання програми.

В таблиці 1 наведено порівняння найбільш поширених програм для збору інформації про транзакції криптовалют [1-3].

Таблиця 1 - Порівняння програм збору інформації транзакцій

Назва	Опис	Переваги	Недоліки
Coin Tracking	збір, відстеження та аналіз даних про транзакції з різних криптовалютних бірж	комплексний аналіз, інтеграція з біржами, розширені функції податкової звітності, - історія	складність використання, вартість, обмеження інтеграції, залежність від

		транзакцій та підтримка різних типів криптовалют	сторонніх джерел та приватність і безпека
Coin Market Cap	спеціалізується на аналізі даних криптовалютних ринків і надає доступ до розширеної аналітики, прогнозів та інструментів для виявлення трендів	широкий обсяг даних, рейтинги та рейтингові списки, новини та оновлення, API та інтеграція, користувальницький інтерфейс	надмірна концентрація на метриці ринкової капіталізації, відсутність повної прозорості та інтегрованої підтримки для трейдингу, обмеженість аналітичних інструментів
Blockfolio	інструмент для відстеження портфеля криптовалют та аналізу транзакцій, що дозволяє користувачам вносити свої транзакції, отримувати сповіщення про зміни цін, а також аналізувати графіки та ринкові дані	відстеження портфеля, налаштування сповіщень, новини та оновлення, аналітика, простий інтерфейс та доступність на різних платформах	обмежені можливості аналітики, відсутність автоматичного синхронізування та розширених функцій портфеля, обмеженість платформ, необов'язкові рекламні матеріали

Висновок: Аналіз та оцінка поширених програм збору інформації про транзакції з криптовалютами виявляються критичними для забезпечення безпеки користувачів. Цей процес дозволяє виявити їхні методи дії, вразливості та потенційні наслідки. Дослідники та експерти з кібербезпеки активно займаються аналізом цих програм та розробкою заходів для їхнього виявлення та усунення. Розробка антивірусних та антишпигунських рішень сприяє захисту користувачів і інфраструктури криптовалют. Забезпечення безпеки та конфіденційності використання криптовалют є вирішальним фактором для підтримки довіри та успіху цих цифрових активів. Продовження аналізу та удосконалення заходів безпеки є важливими для забезпечення стабільного розвитку криптовалютного простору.

Перелік використаних джерел.

1. Що таке CoinTracking, Програмне забезпечення Crypto Tax [Електронний ресурс]. https://morioh.com/p/aac9607e4e0e - лінк.

2. Топ-3 мобільних додатки для контролю інвестиційного портфеля [Електронний ресурс]. http://surl.li/hlivo - лінк

3. Детальний огляд Coinmarketcap: реєстрація, налаштування, відстеження графіків [Електронний ресурс]. http://surl.li/hlizi - лінк

4. 19 Best Crypto Portfolio Tracker Apps [Електронний ресурс]. - https://www.softwaretestinghelp.com/crypto-portfolio-tracker-apps/



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2023)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2023
Тернопіль

Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. - 227 с.

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Адреса редакції:
Західноукраїнський національний університет, кафедра кібербезпеки,
вул. Олени Теліги 8, м. Тернопіль 46003
Контактний телефон: (0352) 50-17-87
e-mail: kb.tneu@gmail.com

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

УДК 004.056.5

Максимчук Р.О., Цаволик Т.Г.

[1]Західноукраїнський національний університет

ТЕХНОЛОГІЧНІ ТРЕНДИ В ГАЛУЗІ КРИПТОВАЛЮТ ТА БЛОКЧЕЙНУ

Вступ. Сучасний світ переживає захоплюючий етап технологічного розвитку, а однією з найбільш захоплюючих та впливових областей цього розвитку є криптовалюти та блокчейн. Криптовалюти, такі як Bitcoin та Ethereum, разом з технологією блокчейну, стали не просто поняттями в сфері фінансів, але і підставою для революційних змін у способі, яким ми сприймаємо та використовуємо гроші, здійснюємо фінансові операції, а також управляємо даними та діловими процесами.

Мета: Дослідження та оцінка криптовалют і блокчейну та їх вплив на безпеку транзакцій

1.Розвиток технологій блокчейну та їх вплив на криптовалюти

Востаннє роки принесли значні зміни в галузі блокчейну та криптовалют. Один з основних трендів полягає в подальшому розвитку самої технології блокчейну. Розширення можливостей шару та розумних контрактів, а також покращення швидкості та масштабованості стали пріоритетами для багатьох розробників. Нові консенсус-протоколи, такі як Proof of Stake (PoS), отримали популярність завдяки своїм перевагам у відношенні до класичного Proof of Work (PoW). Ці зміни в технології блокчейну можуть покращити продуктивність мережі та зменшити споживання енергії. Крім того, важливим трендом є інтеграція інших технологій, таких як штучний інтелект (AI) та Інтернет речей (IoT) з блокчейном. Це дозволяє створити нові застосування для криптовалют та розширює їхні можливості в сферах, таких як управління ланцюжком постачання, медицина, фінанси та багато інших.

2. Регуляторні аспекти та прийняття криптовалют та блокчейну

Іншим ключовим аспектом розвитку галузі криптовалют та блокчейну є питання регуляції. У багатьох країнах по всьому світу уряди та регуляторні органи розглядають способи регулювання цих нових технологій. Важливо забезпечити баланс між захистом споживачів, боротьбою зі зловживаннями та стимулюванням інновацій.

Деякі країни вже впроваджують строгі правила щодо обміну криптовалютами та видачі токенів (ICO), в той час як інші активно працюють над створенням нових нормативних актів для цих сфер. Питання оподаткування криптовалют та відповідальності за кримінальну діяльність в цій галузі також є актуальними темами для обговорення. На рисунку 1 схематично представлені загальні потенційні ризики що можуть виникнути при впровадженні технології блокчейн.

Загалом, регуляторні аспекти впливають на розвиток криптовалют та блокчейну, і важливо слідкувати за змінами в цих правилах та стандартах, оскільки вони можуть вплинути на способи використання та інвестування в ці технології.

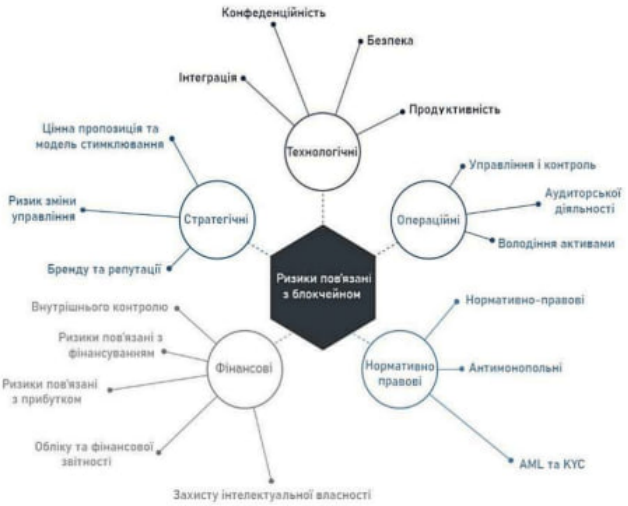

Рисунок 1 - Загальні ризики пов'язані з впровадженням блокчейну

Висновок. Технологічні тренди в галузі криптовалют та блокчейну впливають на сучасний світ і мають значущий потенціал для подальшого розвитку. Розвиток технології блокчейну, включаючи розширення можливостей шару, нові консенсус-протоколи і інтеграцію з іншими сучасними технологіями, відкриває нові можливості для створення ефективних та безпечних рішень у багатьох сферах.

Одночасно регуляторні аспекти грають важливу роль у формуванні майбутнього цієї галузі. Уряди та регуляторні органи працюють над встановленням стандартів та нормативів, щоб забезпечити безпеку та захист прав споживачів, а також підтримати інновації.

Загалом, технологічні тренди у галузі криптовалют та блокчейну свідчать про постійний розвиток цих технологій і їх важливе місце у сучасному світі. Перед нами стоять нові виклики і можливості, і подальше спостереження та аналіз цих трендів є важливим завданням для всіх, хто цікавиться цією динамічною галуззю.

Перелік використаних джерел.

1. Blockchain. [Електронний ресурс]. – Режим доступу: https://www.it.ua/knowledge-base/technology-innovation/blockchain - лінк.

2. Тенденції розвитку блокчейну на 2023 рік. [Електронний ресурс]. – Режим доступу: https://merehead.com/ua/blog/blockchain-industry-development-trends-2023/ - лінк.

3. Тренди блокчейну 2023. [Електронний ресурс]. – Режим доступу: https://www.eternitylaw.com/ua/novyny/blockchain-trends-2023/.

4. 13 трендів криптовалютного ринку, до яких буде прикута увага лідерів індустрії у 2022 році. [Електронний ресурс]. – Режим доступу: https://itc.ua/ua/articles/13-trendiv-kriptovalyutnogo-rinku-do-yakih-bude-prikuta-uvaga-lideriv-industriyi-u-2022-roczi/.

5. Новітні технологічні тенденції у криптовалюті. [Електронний ресурс]. – Режим доступу: http://surl.li/nihxy.