ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ,ЩОДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В BLOCKCHAIN У СЕРИДОВИЩІ CRYSTAL»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Лелюх В.О.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 8

ВСТУП ……..……... 9

1 АНАЛІЗ ПРОБЛЕМИ НАЯВНОСТІ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN …...…… 11

1.1 Дослідження шляхів та зміст розслідування кіберінцидентів у Blockchain …… 11

1.2 Аналіз існуючих інструментів розслідування інцидентів у Blockchain …… 14

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN ІЗ ЗАСТОСУВАННЯМ CRYSTAL……...…… 30

2.1 Дослідження інструменту Crystal, його можливості та функції……. 30

2.2 Можливості середовища Crystal, за допомогою яких ведеться розслідування кіберінцидентів та їх наслідків……..... 32

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ, ЩОДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN У СЕРИДОВИЩІ CRYSTAL……. 45

3.1 Етапи у розслідуванні кіберінцидентів у Blockchain……..…..……. 48

3.2 Розробка рекомендацій, щодо розслідування інцидентів у Blockchain ……... 55

ВИСНОВКИ …….. 63

ПЕРЕЛІК ПОСИЛАНЬ 64

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IDS – Intrusion Detection System

ML – Machine learning

ВСТУП

Актуальність дослідження. У сучасному світі криптовалюти стали однією з найбільш інноваційних і перспективних форм фінансових інвестицій. Їх важливість і значущість у фінансовій сфері визнають експерти, і за їх оцінками, вартість криптовалютного ринку на сьогоднішній день становить більше мільярда доларів США, і цей ринок продовжує швидко зростати.

Проте, разом із зростанням популярності криптовалют збільшується й ризик їх використання для злочинних цілей. Несанкціонований доступ до криптовалют та крадіжки стають серйозними проблемами, а втрати криптовалют через кібератаки можуть досягати мільйонів доларів США. Це викликало необхідність звернути особливу увагу на безпеку криптогаманців, оскільки вони є основними інструментами збереження криптовалют. Забезпечення безпеки криптогаманців має вирішальне значення, оскільки хакерські атаки та крадіжки можуть призвести до серйозних фінансових втрат і порушення конфіденційності особистих даних користувачів. Криптогаманці повинні бути захищені від цих загроз шляхом використання надійних методів шифрування, міцних алгоритмів автентифікації та розумних практик управління ключами. Додатково, безпека криптогаманців також залежить від кінцевого користувача, який повинен дотримуватися надійних методів захисту, таких як використання складних паролів, двофакторної аутентифікації і актуального програмного забезпечення. Враховуючи ризики і потенційні загрози, пов'язані з криптовалютами, необхідною є постійна праця над удосконаленням безпекових механізмів і розробка нових стандартів для забезпечення найвищого рівня безпеки. Тільки тоді криптовалюти зможуть стати ще більшій кількості людей доступними і надійними фінансовими інструментами.

Об’єкт дослідження – розслідування кіберінцидентів у Блокчейн.

Предмет дослідження – методи та засоби багатовимірного візуального аналізу під час розслідування кіберінцидентів.

Мета роботи – розробити рекомендації, щодо розслідування кіберінцидентів в Blockchain у серидовищі Crystal.

Завдання бакалавської роботи:

дослідити існуючі загрози, які можуть бути використані у Blockchain;

проаналізувати існуючі інструменти для захисту криптоактивів;

ознайомитись із процесами, які дозволяють вирішувати проблеми у Blockchain в серидовищі Crystal;

дослідити можливості застосування Crystal у боротьбі з кіберінцидентами та їх наслідками;

Методи дослідження – опрацювання літератури за даною темою, розробити ефективні рекомендації задля розслідування кіберінцидентів у Blockchain. Пропрацювати методи та засоби розслідування. Зробити на базі усієї інформації висновок.

Практичне значення одержаних результатів: рекомендації щодо розслідування кіберінцидентів можуть бути використані у сфері захисту криптоактивів.

1 АНАЛІЗ ПРОБЛЕМИ НАЯВНОСТІ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN

1.1 Дослідження шляхів та зміст розслідування кіберінцидентів у Blockchain

Розслідування кіберінцидентів у Блокчейн може бути складним завданням, оскільки технологія Блокчейн за своєю природою створює надійну імутабельну систему запису даних, що ускладнює виявлення інцидентів та встановлення осіб, які їх здійснили.

Однак, існують деякі шляхи, які можуть бути використані при розслідуванні кіберінцидентів у Blockchain:

Аналіз транзакцій: Кожна транзакція в Блокчейні має унікальний ідентифікатор, який може бути використаний для відстеження переказів між різними адресами гаманців. Цей аналіз може допомогти встановити, які адреси гаманців були втягнуті в інцидент. Наприклад, якщо злочинець використовував одну адресу гаманця для отримання виплат від жертв і іншу адресу гаманця для переказу коштів, що отримані в результаті цих виплат, то аналіз транзакцій може допомогти встановити, які адреси гаманців були використані у цьому процесі.

Іншим прикладом може бути використання аналізу транзакцій для відстеження походження коштів, що були вкрадені. Якщо злочинець переводив кошти через кілька адрес гаманців, то аналіз транзакцій може допомогти встановити, з яких гаманців було викрадено кошти та до яких гаманців вони були переказані.

Аналіз транзакцій може також допомогти виявити відносини між різними гаманцями. Наприклад, якщо дві адреси гаманців часто здійснюють транзакції одна з одною, то це може свідчити про те, що вони належать до однієї і тієї ж людини або компанії.

Також у цьому питанні доволі практичним є інструмент «Orbit», який не предназначений для деанонімізації користувачів, але допомагає зібрати цікаву інформацію про транзакції у вигляді графів (рис 1.2).

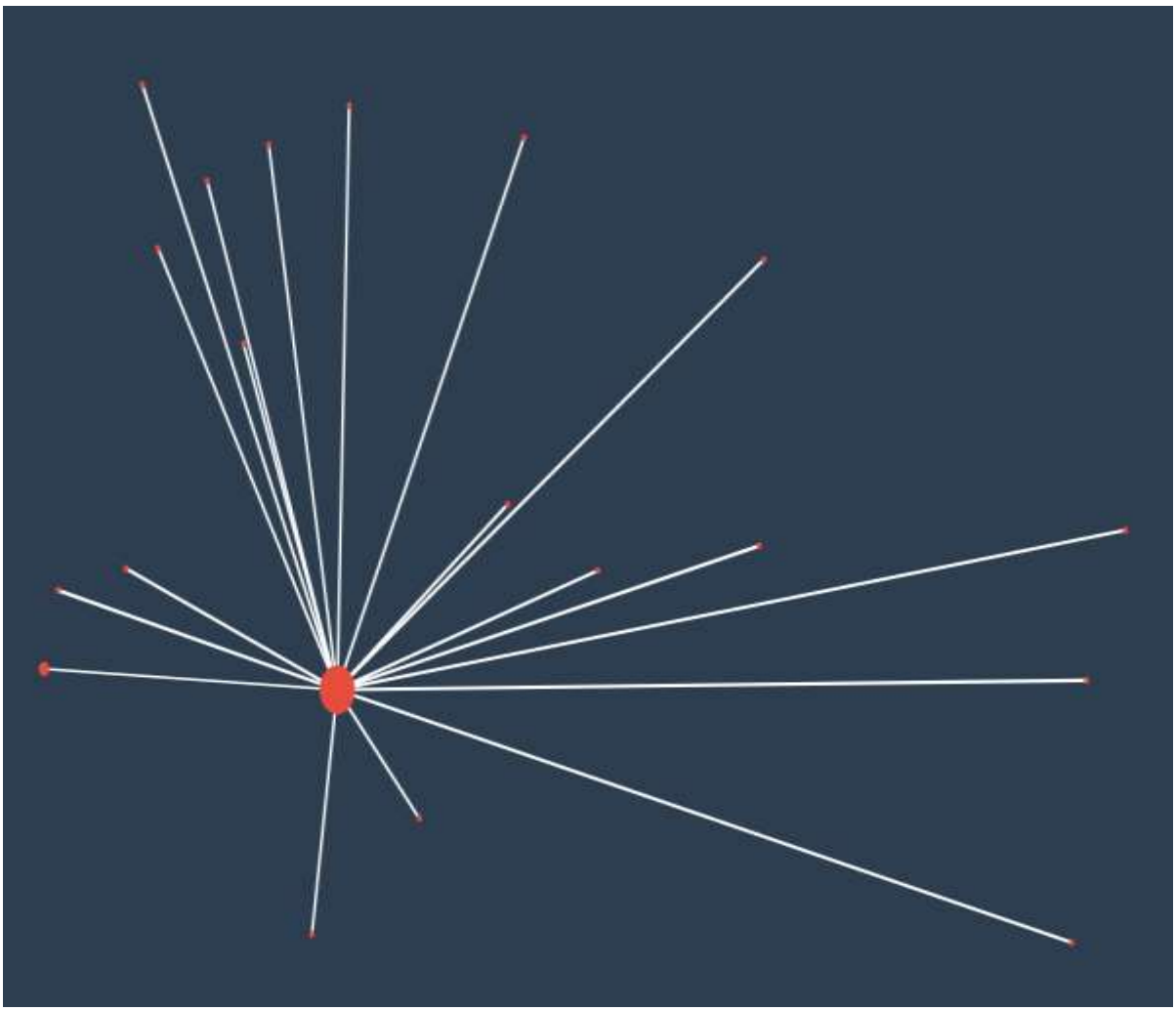


Рис. 1.1. Демонстрація графів у інструменті «Orbit» [2]

Відслідковування IP-адрес: Кіберзлочинці можуть використовувати віртуальні приватні мережі або мережі з анонімізацією, щоб залишити сліди, але вони все ще можуть залишатися відкритими в певних моментах. Відслідковування IP-адрес, які здійснювали підключення до Блокчейну, може допомогти встановити місцезнаходження злочинця. Кожен раз, коли кіберзлочинець здійснює транзакцію в Блокчейні, його IP-адрес залишає слід, який може бути відслідкований. Цей інформаційний слід може допомогти встановити

місцезнаходження злочинця, якщо він не використовує спеціальні мережі для захисту своєї анонімності.

За допомогою відслідковування IP-адрес можливо відслідкувати мережеву активність кіберзлочинця та встановити, з якого місця він здійснював транзакції в Блокчейні. Це може бути корисним для правоохоронних органів, які ведуть розслідування відносно кіберзлочинів.

Аналіз метаданих: Деякі Блокчейн-платформи можуть надавати метадані про транзакції, які містять додаткову інформацію про адреси гаманців, які беруть участь у транзакції. Ці метадані можуть бути використані для встановлення зв'язків між адресами гаманців та ідентифікації злочинця. За допомогою аналізу метаданих можна виявити певні відомості, які можуть допомогти в ідентифікації кіберзлочинця. Наприклад, якщо певна адреса гаманця бере участь у багатьох транзакціях, які пов'язані з незаконною діяльністю, то можна зробити висновок, що ця адреса належить кіберзлочинцю.

Також аналіз метаданих може допомогти виявити зв'язки між різними адресами гаманців. Наприклад, якщо дві адреси гаманців були пов'язані зі злочинними діями, то аналіз метаданих може допомогти встановити, що ці адреси належать одному кіберзлочинцю.

Використання різних Блокчейн-аналітичних інструментів: Існує кілька аналітичних інструментів, які можуть бути використані для розслідування кіберінцидентів у Blockchain, таких як Блокчейн-аналітика, розумний контракт-аналітика та інші інструменти, які дозволяють аналізувати транзакції, відстежувати грошові потоки та знаходити зв'язки між різними адресами гаманців. Один з таких інструментів - Блокчейн-аналітика, яка використовується для аналізування даних транзакцій та виявлення підозрілих дій у Блокчейні. Блокчейн-аналітика дозволяє відстежувати грошові потоки, знаходити зв'язки між адресами гаманців та ідентифікувати потенційних злочинців.

Іншим важливим інструментом є розумна контракт-аналітика, яка дозволяє аналізувати розумні контракти, які зберігаються у Блокчейні. Розумна контракт-

аналітика може виявити підозрілі контракти та виявити потенційні уразливості у системі.

Співпраця зі спеціалізованими компаніями: На ринку існує кілька компаній, які спеціалізуються на розслідуванні кіберінцидентів у Блокчейн. Вони можуть надати необхідні інструменти та ресурси для виявлення злочинців та встановлення їх осіб.

У зміст розслідування кіберінцидентів у Blockchain входить визначення втрачених активів, встановлення осіб, які здійснили інцидент, та збір доказів для подальшого преслідування. При розслідуванні кіберінцидентів у Blockchain також важливо враховувати відповідність законодавства та нормативних актів щодо збору та використання даних.

1.2 Аналіз існуючих інструментів розслідування інцидентів у Blockchain

Існує декілька інструментів, які використовуються для розслідування кіберінцидентів у Blockchain. Розглянемо кілька з них:

Blockchain Explorer: це онлайн-інструмент, який дозволяє аналізувати транзакції, блоки та адреси гаманців у Блокчейн. Він надає інформацію про розмір транзакції, час та дату її виконання, адреси відправника та отримувача та іншу корисну інформацію. [1]

Основна функціональність Blockchain Explorer включає наступні можливості:

– *аналіз транзакцій:* Ви можете ввести ідентифікатор транзакції або адресу гаманця у Blockchain Explorer, щоб переглянути деталі про цю транзакцію. Інформація про транзакцію може включати розмір транзакції, час та дату виконання, адреси відправника та отримувача, підтвердження транзакції та інші дані.

– *перегляд блоків:* ви можете переглядати окремі блоки у Блокчейні, включаючи деталі про блок, такі як номер блоку, час створення, кількість транзакцій, хеш блоку та інші параметри.

– *пошук адрес гаманців:* Blockchain Explorer надає можливість пошуку адрес гаманців у Блокчейні. Ви можете ввести адресу гаманця та отримати інформацію про стан балансу, історію транзакцій та інші дані, пов'язані з цим адресом.

– *відстеження грошових потоків:* Ви можете використовувати Blockchain Explorer для відстеження грошових потоків у Блокчейні. Наприклад, ви можете переглянути всі транзакції, пов'язані з певним гаманцем, або відстежувати рух коштів між різними адресами.

– *виявлення зв'язків між адресами:* За допомогою Blockchain Explorer ви можете знайти зв'язки між різними адресами гаманців. Наприклад, ви можете встановити, які адреси пов'язані

Blockchain forensics tools: це програмні засоби, які дозволяють аналізувати транзакції, виявляти несправні транзакції та встановлювати осіб, які здійснили кіберінцидент. Вони використовують алгоритми аналізу поведінки, що допомагають виявляти незвичайні активності та надмірні транзакції, що можуть бути пов'язані з кіберінцидентом.

Ось кілька прикладів того, що дають змогу робити blockchain forensics tools

– *Аналіз транзакцій*: ці інструменти дозволяють детально аналізувати транзакції Блокчейну. Вони можуть відстежувати потік коштів і аналізувати деталі транзакцій, такі як адреси відправника та одержувача, суми транзакцій, мітки часу та дані введення та виведення транзакцій.

– *Кластеризація адрес*: інструменти аналізу Блокчейнів використовують алгоритми кластеризації адрес для групування пов’язаних адрес. Це допомагає визначити право власності та контроль над кількома адресами, пов’язаними з однією особою чи організацією. Створюючи кластери адрес, слідчі можуть отримати інформацію про моделі транзакцій і зміцнити зв’язок адрес із певними об’єктами.

Існує багато прикладів, тому пропоную розглянути їх та їхній зовнішній вигляд.

– *Uppsala Security***:** Uppsala Security надає рішення з управління ризиками для боротьби з відмиванням грошей, дотримання нормативних вимог та кібербезпеки. Заснована в січні 2018 року, Uppsala Security є першою краудсорсинговою платформою для аналізу загроз. Продукти Uppsala включають в себе Crypto Analysis Risk Assessment (CARA), яка використовує технологію машинного навчання для класифікації рівня ризику криптоадрес на основі вивченої поведінки як відомих шкідливих, так і звичайних гаманців. Crypto Analysis Transaction Visualisation (CATV) - це криптографічний інструмент, який відстежує вхідні та вихідні транзакції для перевірених гаманців. Він надає візуальний інтерфейс (рис 1.2) для аналізу типів гаманців, що взаємодіють з потоками токенів, і допомагає виявити підозрілу поведінку потоків. [3]

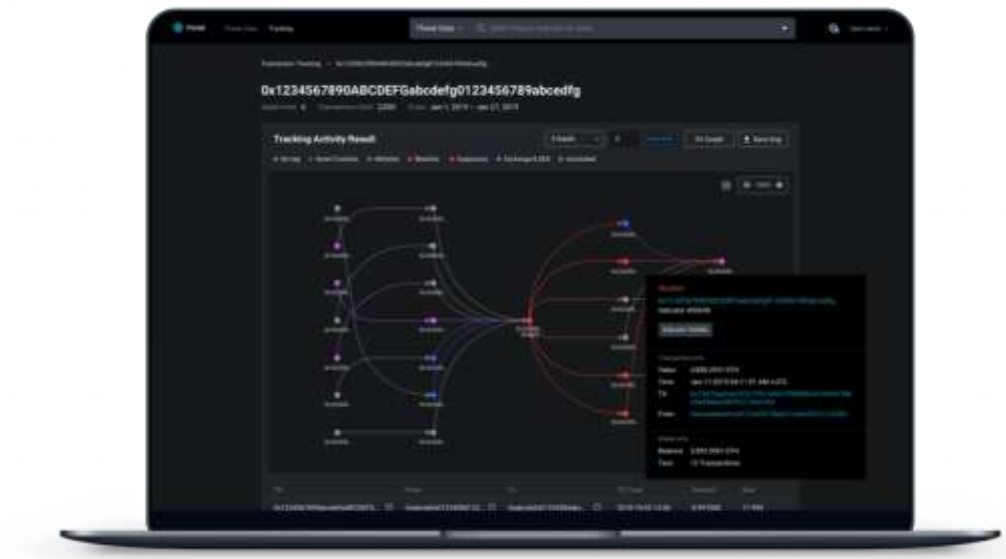


Рис. 1.2. Приклад візуалізації у серидовищі Uppsala Security [4]

– *TRM Labs***:** TRM допомагає фінансовим установам боротися з відмиванням криптовалютних грошей, запобігати шахрайству та дотримуватися нормативних вимог, які включають продукти TRM Labs: TRM Investigator - простий у

використанні інтерфейс (рис. 1.3) для криптовалютних розслідувань. Автоматичне визначення шляху забезпечує видимість транзакцій і грошових потоків у Блокчейні. Моніторинг транзакцій постійно відстежує Блокчейн-гаманці, щоб запобігти шахрайським діям. Він також надає оцінку ризику транзакцій, відстежуючи незвичну поведінку та її шаблони.

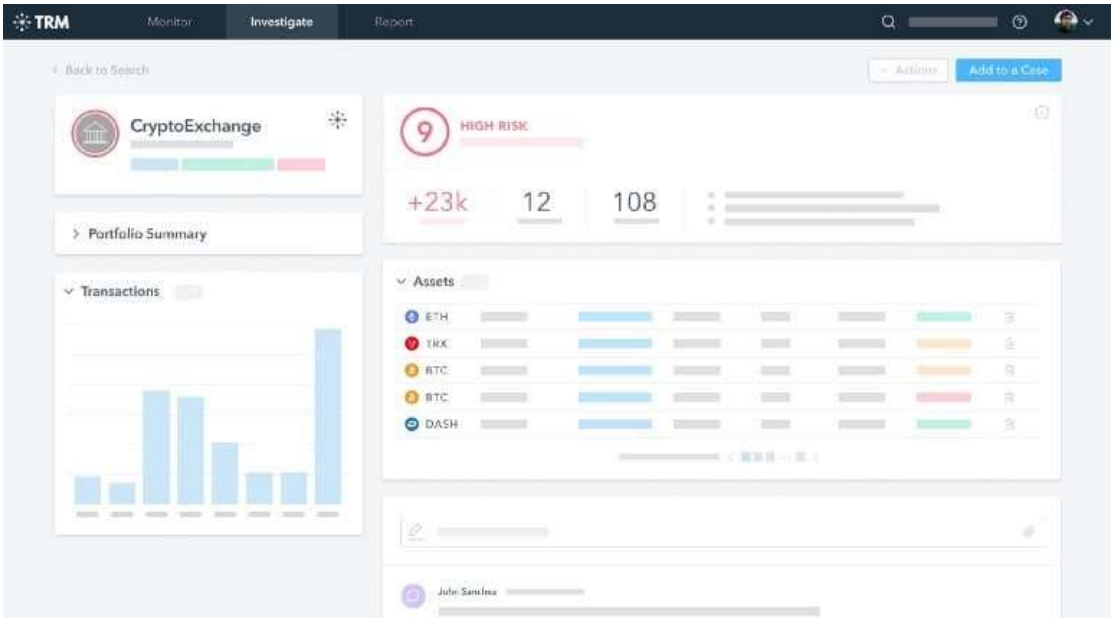


Рис. 1.3. Зовнішній вигляд TRM Labs [4]

– *Coinpath***:** Coinpath - це продукт компанії Bitqurey, який надає API грошових потоків у Блокчейні; API Coinpath можна використовувати для створення інструментів моніторингу та візуалізації транзакцій (рис. 1.4) для розслідування криптовалютних злочинів, таких як відмивання біткойн-грошей.

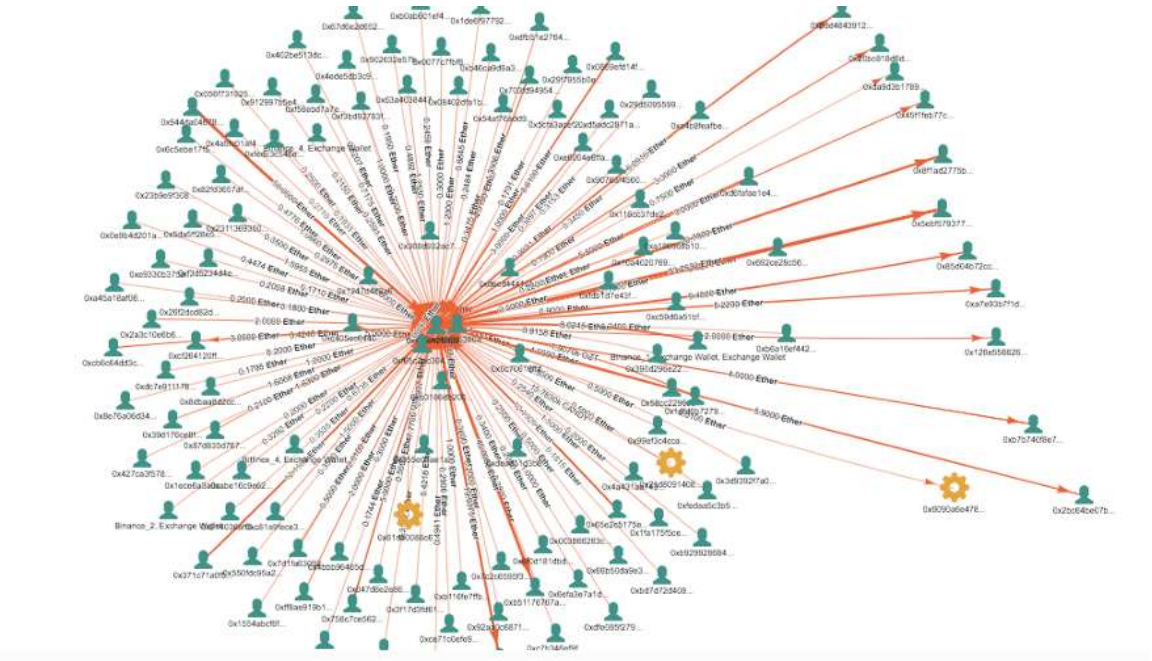


Рис. 1.4. Візуалізація транзакцій за допомогою Coinpath [4]

– *Elliptic*: Elliptic використовується найбільшими криптовалютними біржами та фінансовими установами по всьому світу. Продукти Elliptic пропонують безліч рішень для дотримання криптовалютного законодавства та дослідження Блокчейну: Elliptic Lens надає інформацію, необхідну для захисту вашого бізнесу та клієнтів. Lens використовується командами по боротьбі з шахрайством, комплаєнсом та операційними командами для забезпечення доступу до криптогаманців, даючи уявлення про те, хто стоїть за кожною адресою і про грошові потоки всередині гаманця (рис. 1.5). Потужні можливості Elliptic Navigator з відстеження та настроювані правила ризику забезпечують послідовне і точне розуміння походження і призначення коштів у понад 100 криптовалютах.

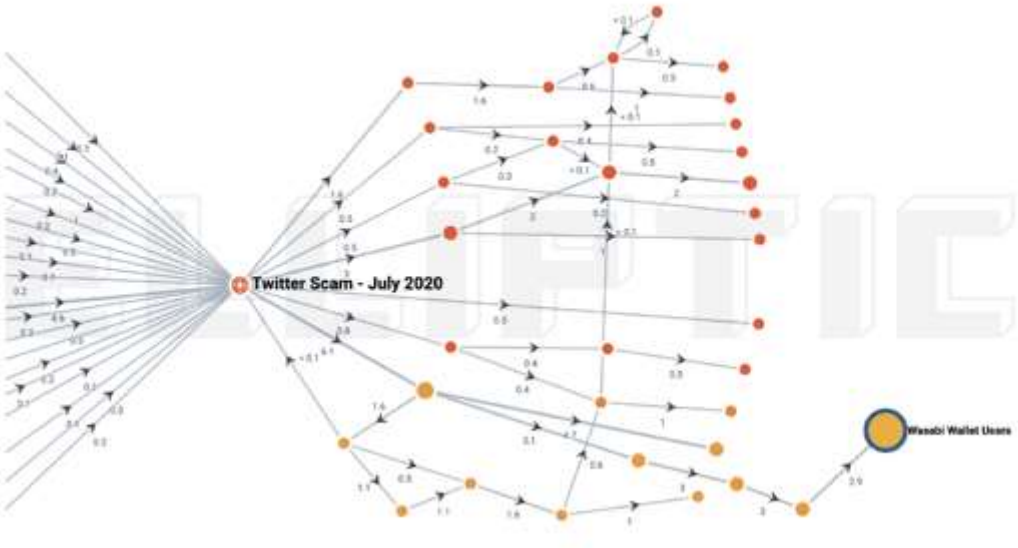


Рис. 1.5. Візуаліційна павутина у Elliptic [4]

– *Chainalysis*: Chainalysis - одна з провідних аналітичних компаній у сфері Блокчейн, що надає програмне забезпечення для забезпечення відповідності та проведення розслідувань банкам, криптовалютним компаніям і державним установам. Вона пропонує безліч інструментів для моніторингу транзакцій, оцінки ризиків і візуалізації. (рис 1.6)

Chainalysis KYT (Know Your Transaction) виявляє високоризиковані криптовалютні транзакції з даркнет-ринків, шахрайство та авторизовані адреси. Він надає простий у використанні інтерфейс для аналізу та розслідування транзакцій. Reactor забезпечує видимість грошових потоків у Блокчейні для будь-якої криптовалютної адреси, включно з Bitcoin і Ethereum. Він також надає інформацію про реальну ідентичність адрес Блокчейну, що дуже важливо для криптовалютних розслідувань. Chainalysis Kryptos надає повний профіль понад 1800 криптовалютних підприємств на основі їхніх даних KYC. Це галузевий довідник з криптовалютних сервісів та їхньої діяльності на ланцюжку.

Рис. 1.6. Наглядне зображення візуалізації Chainalysis [4]

У звіті Chainalysis, провідної аналітичної компанії в галузі Блокчейну, йдеться про те, що у 2019 році було зафіксовано 11,5 мільярдів доларів США криптовалютних транзакцій, пов'язаних з різноманітною кримінальною діяльністю (рис. 1.7). Ці транзакції охоплюють широкий спектр злочинної діяльності, включаючи відмивання грошей, фінансування тероризму, торгівлю наркотиками, кіберзлочинність та інші негативні дії. Виявлення такого великого обсягу злочинних транзакцій підкреслює необхідність посилення заходів безпеки, регулювання та контролю у криптовалютному секторі з метою ефективної боротьби зі злочинністю та забезпечення безпеки фінансової системи. [6]

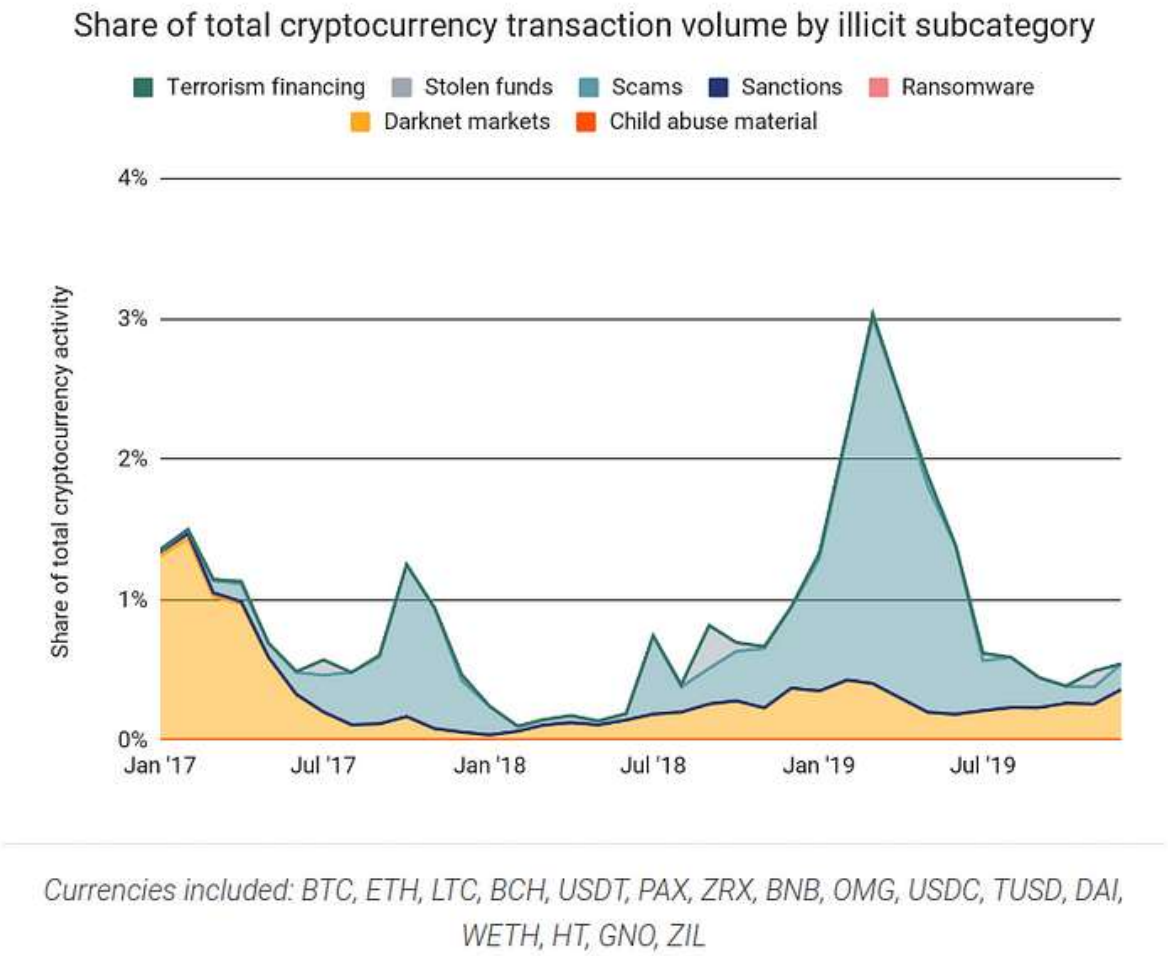


Рис. 1.7. Аналітичний графік динаміки кримінальних активів [6]

– *CipherTrace*: CipherTrace надає повний набір рішень для моніторингу ризиків і забезпечення відповідності вимогам для VASPs (постачальників послуг віртуальних активів), підтримуючи понад 800 токенів, виявляючи діяльність з відмивання криптовалютних грошей, розслідування правоохоронних органів і нагляд регулюючих органів і забезпечити відповідність вашого бізнесу вимогам до криптовалют.

Продукти ChiperTrace включають: Armada відмічає платежі з високим рівнем ризику між банками та VASPs і використовує глибоку аналітику в практиці "Знай свого клієнта" (KYC) і AML для виявлення ризиків, пов'язаних із сотнями VASPs та іншими об'єктами віртуальних активів. Sentry допомагає розслідувати діяльність з відмивання криптовалютних грошей, інтегруючись з відкритими і закритими джерелами інформації, швидко агрегуючи і співвідносячи

різні показники за допомогою власних алгоритмів кластеризації, щоб забезпечити ефективну атрибуцію для користувачів. Inspector - це інструмент пошуку та візуалізації для розслідування криптовалютних транзакцій (рис. 1.8).

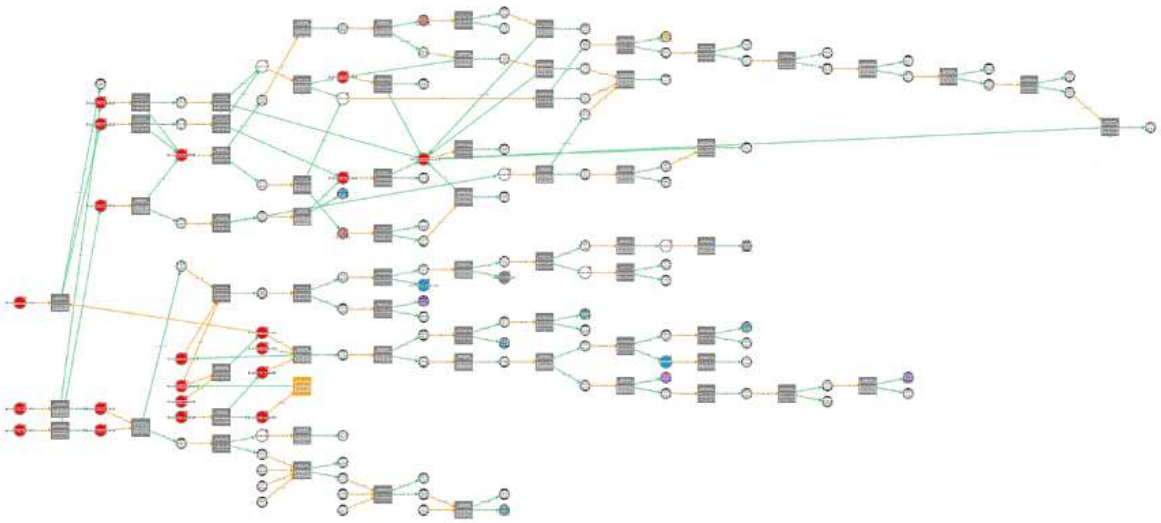


Рис. 1.8. Графи візуалізації у CipherTrace [4]

– *Smart contract analytics tools:* це програмні засоби, які дозволяють аналізувати розумні контракти в Blockchain. Вони перевіряють наявність помилок у коді контракту, виявляють можливість використання його для злочинних цілей та допомагають встановлювати осіб, які здійснили кіберінцидент.

Основні функції та можливості Smart contract analytics tools включають наступне:

– *Аналіз коду контракту*: Ці інструменти дозволяють аналізувати код розумних контрактів з метою виявлення потенційних помилок, проблем безпеки або вразливостей. Вони перевіряють відповідність контракту найкращим практикам безпеки, ідентифікують можливі вразливості та рекомендують покращення для забезпечення надійності та безпеки контракту.

– *Виявлення злочинних схем*: Smart contract analytics tools можуть виявляти можливість використання розумного контракту для злочинних цілей, таких як відмивання грошей, шахрайство або кібератаки. Вони можуть виявляти

незвичайні шаблони поведінки, виявляти підозрілі операції та ідентифікувати контракти, які можуть бути пов'язані зі злочинними діями.

– *Аудит контракту*: Smart contract analytics tools можуть проводити аудит контракту з метою виявлення потенційних проблем безпеки, ділових правил, або невідповідностей вимогам. Вони перевіряють правильність логіки контракту, дотримання криптографічних принципів, забезпечення виконання умов та інших аспектів контракту, що можуть вплинути на його надійність та безпеку.

– *Встановлення осіб, які здійснили кіберінциденти*: В разі кіберінциденту або незаконних дій у контексті розумних контрактів, Smart contract analytics tools можуть допомогти встановити осіб, які здійснили ці дії. Вони аналізують записи транзакцій, використовують методи деанонімізації та аналізують мережеві зв'язки для ідентифікації потенційних зловмисників або залучених сторін.

Smart contract analytics tools використовуються як аудиторські та безпекові інструменти для розумних контрактів, що дозволяють забезпечити надійність, безпеку та виявлення можливих кіберзагроз у Блокчейн-мережах. Вони сприяють підвищенню довіри до розумних контрактів та допомагають запобігти вразливостям та неправомірним діям у Блокчейн-середовищі.

Blockchain-based forensic analysis platforms: це програмні платформи, які використовують Blockchain для збору та аналізу даних про транзакції. Вони дозволяють відстежувати грошові потоки та знаходити зв'язки між різними адресами гаманців, що допомагає виявляти та встановлювати осіб, які здійснили кіберінцидент. Вони надають розширені можливості для проведення детального аналізу Блокчейн-транзакцій, ідентифікації джерела та адреси, аналізу зв'язків та встановлення шаблонів поведінки. [7] Основні складові частини Blockchain-based forensic analysis platforms включають наступне:

– *Збір та агрегація даних*: Платформи для форензіки Блокчейну збирають дані з різних джерел, таких як Блокчейн-мережі, блок експлорери, Блокчейн-громадські дані тощо. Вони агрегують ці дані та зберігають у відповідних форматах для подальшого аналізу.

– *Аналіз транзакцій та блоків*: Платформи надають можливість детального аналізу транзакцій та блоків, що здійснюються в Блокчейні. Вони досліджують властивості транзакцій, включаючи адреси відправника та отримувача, суми, час та дату, використані валюти тощо. Це дозволяє виявити незвичайні або підозрілі активності.

– *Відстеження грошових потоків*: Платформи для форензіки Блокчейну дозволяють відстежувати грошові потоки між різними адресами та гаманцями. Вони аналізують шляхи руху коштів, виявляють потенційні зв'язки між адресами та рахунками, що допомагає встановити зв'язки між різними суб'єктами.

– *Виявлення вразливостей та кіберзагроз*: Blockchain-based forensic analysis platforms використовують алгоритми аналізу та виявлення вразливостей, що дозволяють ідентифікувати потенційні кіберзагрози та вразливості в Блокчейн-мережах. Вони аналізують контракти, протоколи та інші складові Блокчейн-системи для виявлення можливих проблем безпеки.

– *Кластерний аналіз та графові візуалізації*: Платформи надають можливості для кластерного аналізу та графової візуалізації даних. Вони допомагають виявити зв'язки між різними суб'єктами, адресами, транзакціями та блоками у Блокчейн-мережі. Це дозволяє легше розуміти складні зв'язки та встановлювати шаблони поведінки.

– *Юридичні та регуляторні аспекти*: Деякі Blockchain-based forensic analysis platforms надають інструменти та функціональність, що сприяють вирішенню юридичних та регуляторних аспектів у сфері Блокчейн-технологій. Вони можуть надавати засоби для документування результатів аналізу, генерації звітів, підтримки правової вимоги і встановлення ланцюжків доведень.

– *Інтеграція з іншими системами безпеки*: Деякі платформи Блокчейну можуть інтегруватися з іншими системами безпеки, такими як системи виявлення вторгнень (IDS), системи управління подіями та інші. Це дозволяє підвищити ефективність і комплексність аналізу Блокчейн-даних та забезпечити цілісність

цифрової безпеки. Системи виявлення вторгнень можна розглянути більш детально.

Системи виявлення вторгнень – це програмні або апаратні засоби виявлення атак і шкідливих дій. Вони допомагають мереж і комп'ютерних систем давати їм належну відсіч. Для досягнення цієї мети IDS здійснює збір інформації з численних системних або мережевих джерел. Потім система IDS аналізує її на предмет наявності атак. [8]

До елементів IDS відносяться:

– детекторная підсистема, мета якої – накопичення подій мережі або комп'ютерної системи;

– підсистема аналізу, яка виявляє кібер-атаки і сумнівну активність;

– сховище для накопичення інформації про події, а також результати аналізу кібер-атак і несанкціонованих дій;

– консоль управління, за допомогою якої можна задавати параметри IDS, стежити за станом мережі (чи комп'ютерної системи), мати доступ до інформації про виявлені підсистемою аналізу атаки і неправомірні дії. [8]

Основні завдання, які вирішують системи виявлення вторгнень це аналіз джерел інформації та адекватна реакція, заснована на результатах цього аналізу. Для виконання цих завдань система IDS здійснює наступні дії:

– моніторить і аналізує активність користувачів;

– займається аудитом конфігурації системи і її слабких місць;

– перевіряє цілісність найважливіших системних файлів, а також файлів даних;

– проводить статистичний аналіз станів системи, заснований на порівнянні з тими станами, які мали місце під час вже відомих атак;

– здійснює аудит операційної системи.

Також у IDS є продовження, яке має назву IPS. IPS розшифровується як «система запобігання вторгненням». Це вдосконалені та більш функціональні варіанти IDS. Реактивна система IDS IPS (на відміну від традиційної системи). Це означає, що він може не лише виявляти, записувати та повідомляти про напади,

але й виконувати роль захисту. Ці функції включають скидання з’єднань і блокування пакетів вхідного трафіку. Ще одна особливість IPS полягає в тому, що він працює онлайн і може автоматично блокувати атаки. [8]

Група компаній ID Systems сьогодні є одним з лідерів у створенні систем безпеки комп'ютерних мереж. Забезпечує надійний захист від кіберзлочинців. Завдяки системі захисту ID Systems вам ніколи не доведеться турбуватися про свої конфіденційні дані. Завдяки цьому ви матимете менше турбот і зможете більше насолоджуватися життям.

– *Open source intelligence (OSINT) tools:* це програмні засоби, які дозволяють збирати інформацію про користувачів та інші ресурси в Інтернеті. Вони можуть бути корисними для збору інформації про осіб, які здійснили кіберінцидент, їх зв'язки та взаємодії з іншими користувачами. Деякі інструменти OSINT можуть також використовуватися для виявлення інших елементів, пов'язаних з кіберінцидентом, наприклад, електронної пошти, IP-адрес, та ін. Це програмні засоби, розроблені з метою полегшення та автоматизації процесу збору та аналізу відкритої інформації. Вони допомагають відшукати, фільтрувати, обробляти та аналізувати дані, що були зібрані з різних джерел.

Ось кілька прикладів популярних інструментів OSINT:

- Maltego: Це потужний графічний інструмент аналізу даних (рис. 1.9), який дозволяє візуалізувати зв'язки між різними об'єктами. Він забезпечує можливість використовувати різні модулі для отримання інформації зі соціальних мереж, пошукових систем, веб-сайтів та інших джерел. [9]

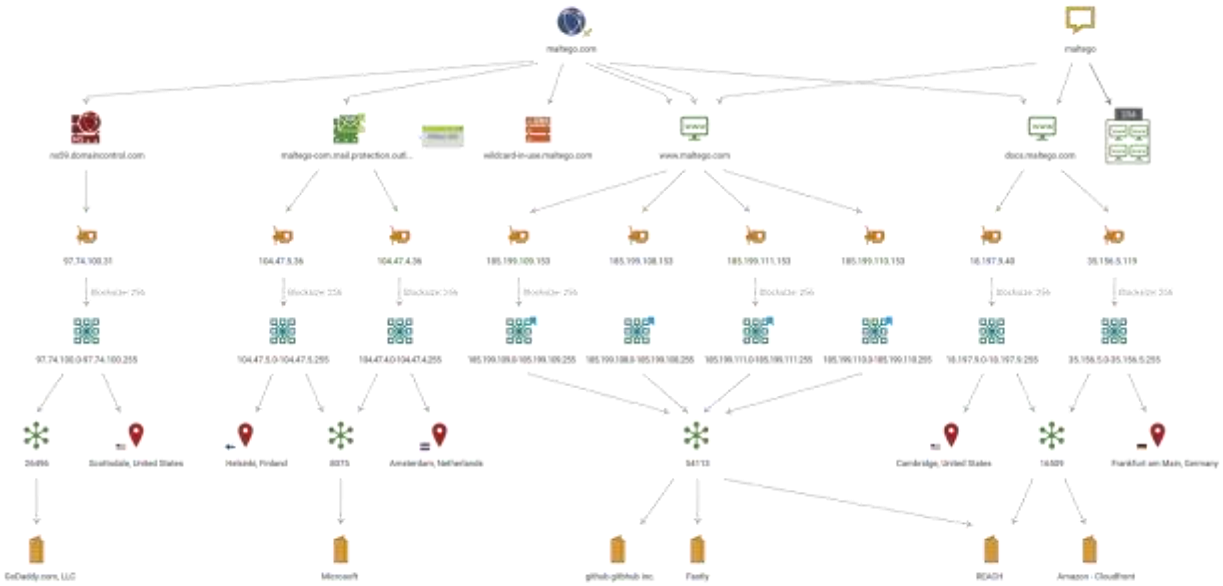


Рис. 1.9. Нгалядний приклад графічної частини інструменту Maltego [9]

– *Shodan*: Цей пошуковий двигун дозволяє знаходити підключені до Інтернету пристрої, такі як сервери, маршрутизатори, камери спостереження тощо (рис. 1.10). Він надає доступ до різноманітної інформації, включаючи відкриті порти, протоколи, сертифікати та інше, що може бути корисним для аналізу безпеки.[10]

Однією з головних особливостей Shodan є те, що він не просто знаходить ці пристрої, але також надає доступ до додаткової інформації про них. Наприклад, він може виявити відкриті порти на пристроях, які можуть використовуватися для комунікації з цими пристроями. Відомі відкриті порти, такі як HTTP (порт 80) або FTP (порт 21), можуть свідчити про те, що пристрій може бути доступним для зовнішніх підключень або має відкриті служби, які можуть бути вразливими до атак.

Крім того, Shodan може надавати інформацію про використовувані протоколи, сертифікати безпеки та інші деталі пристроїв, які можуть бути корисними для аналізу безпеки. Це може включати версії програмного

забезпечення, служби, які працюють на пристрої, та інші важливі дані, які можуть вказувати на наявність потенційних вразливостей або проблем з безпекою.

Shodan використовується в різних сферах, включаючи кібербезпеку, дослідження безпеки мереж та веб-сайтів, виявлення розташування пристроїв та багато іншого.

Організації також можуть використовувати Shodan для моніторингу своєї мережі та виявлення можливих проблем з безпекою. Вони можуть сканувати свої власні пристрої та порти, щоб переконатися, що вони належним чином захищені і не мають вразливостей, які можуть бути використані зловмисниками.

Shodan також може бути корисним для кібербезпекових команд організацій, які відповідають за виявлення та відповідь на кібератаки. Вони можуть використовувати Shodan для виявлення нових або незвичайних пристроїв, які можуть бути пов'язані з потенційними загрозами, та реагувати на них вчасно.

Узагалі, даний засіб надає важливі інструменти для виявлення та аналізу безпекових проблем у підключених до Інтернету пристроях. Він допомагає забезпечити більшу свідомість про потенційні загрози та забезпечити відповідні заходи безпеки для захисту систем та мереж від можливих атак і вразливостей.

Рис. 1.10. Пошук онлай-пристроїв за допомогою Shodan [10]

Threat intelligence platforms: це програмні платформи, які дозволяють аналізувати дані про кіберзагрози та виявляти нові загрози. Вони можуть бути корисними для виявлення нових кіберінцидентів та встановлення зв'язків між різними кіберзагрозами.

Основні функції та можливості Threat intelligence platforms включають наступне:

– *збір та агрегація даних*: TIP збирають дані про кіберзагрози з різних джерел, таких як внутрішні логи, зовнішні інформаційні ресурси, публічні бази даних, соціальні медіа, дослідницькі звіти та інші джерела. Вони агрегують ці дані та структурують їх для подальшого аналізу.

– *аналіз та класифікація загроз*: TIP використовують різні методи та алгоритми для аналізу та класифікації кіберзагроз. Вони можуть використовувати техніки машинного навчання, штучного інтелекту та інші методи, щоб виявити підозрілі активності, розпізнати шаблони та встановити відношення між різними загрозами.

– *передбачення та прогнозування*: З використанням отриманої інформації, TIP можуть намагатися передбачити майбутні кіберзагрози та напрямки розвитку загроз. Вони можуть надавати організаціям рекомендації щодо запобігання або мінімізації ризиків, пов'язаних з певними загрозами.

Застосування цих інструментів дозволяє покращити ефективність розслідування кіберінцидентів у Блокчейн. Вони дозволяють швидко знаходити зв'язки між різними адресами гаманців, встановлювати осіб, які здійснили кіберінцидент, та виявляти інші елементи, пов'язані з кіберінцидентом.

Серидовище, про яке буде йтись у наступному розділі має назву Crystal Analysis, в ній будуть описані та продемонстровані сильні та слабкі сторони серидовища, а також показано його практичну цінність у подоланні кіберінцидентів.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN ІЗ ЗАСТОСУВАННЯМ CRYSTAL

2.1. Дослідження інструменту Crystal, його можливості та функції

Crystal – це інструмент для аналізу транзакцій у Blockchain, який використовує штучний інтелект для виявлення підозрілих транзакцій та ідентифікації осіб, які здійснюють ці транзакції. Цей інструмент може бути корисним для розслідування кіберінцидентів, таких як крадіжки криптовалюти, шахрайства та фінансові злочини, які виконуються через Blockchain.

Crystal надає цілісне уявлення про Блокчейн та Bitcoin і відображає підозрілі транзакції та пов'язані з ними структури за допомогою розширеного аналізу та очищення даних. Інноваційний інструмент також надає унікальну систему оцінки ризиків, яка допомагає слідчим виявляти та відстежувати зловмисну поведінку; Crystal був розроблений для правоохоронних органів, щоб відстежувати підозрілі біткоїн-транзакції до реальних цілей та виявляти зв'язки між злочинними суб'єктами.

Інструмент може аналізувати дані з різних Блокчейнів, таких як Bitcoin, Ethereum та інші, та надавати користувачам детальну інформацію про транзакції, включаючи інформацію про адреси гаманців, суми транзакцій та час виконання транзакцій. Крім того, Crystal Analysis може застосовувати аналіз графів для виявлення зв'язків між різними адресами гаманців та встановлення шаблонів поведінки осіб, які здійснюють підозрілі транзакції.

За даними Crystal з 2011 року загальна вартість викраденої криптовалюти, еквівалентна понад 12 мільярдам доларів США, досягла значного рівня, що перевищує весь валовий внутрішній продукт (ВВП) молдовської держави (рис. 2.1). Це вражаюча цифра, яка свідчить про значний обсяг крадіжок і шахрайства у сфері торгівлі криптовалютою. Крадіжки криптовалют включають хакерські

атаки, фішинг, шахрайські ICO (первинне розміщення монет), підроблені ICO, підкуп людей, які мають доступ до приватних ключів, і багато інших видів шахрайства. Ця сума, яка перевищує весь ВВП Молдови, ілюструє серйозні виклики, з якими стикається криптовалютна індустрія. Втрати, пов'язані з крадіжками криптовалют, мають значний вплив на фінансову стабільність і довіру до цього виду цифрових активів. Довіра та безпека криптовалютної інфраструктури є важливим аспектом і вимагає посилення заходів безпеки, регулювання та ефективних механізмів боротьби з шахрайством і крадіжками в цій сфері.

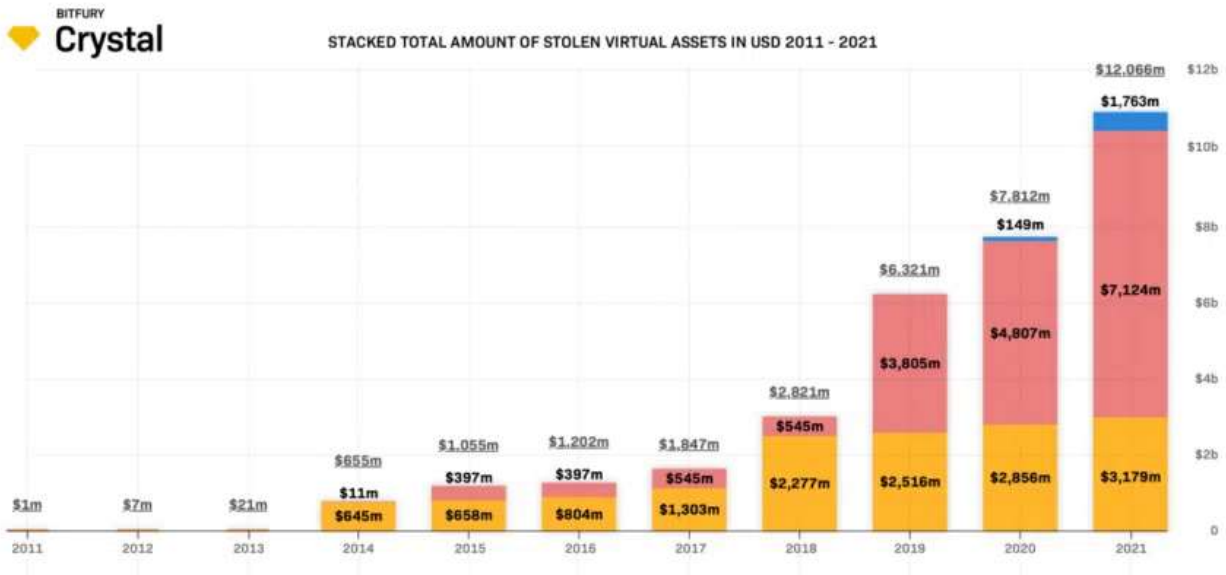


Рис. 2.1. Викрадання криптовалюти [5]

Crystal також може забезпечувати детальний аналіз активності різних адрес гаманців, таких як кількість вихідних та вхідних транзакцій, сума криптовалюти, що перекладається, та інші параметри. Ці дані можуть бути корисними для виявлення нелегальної активності потенційних злочинців. (рис. 2.2)

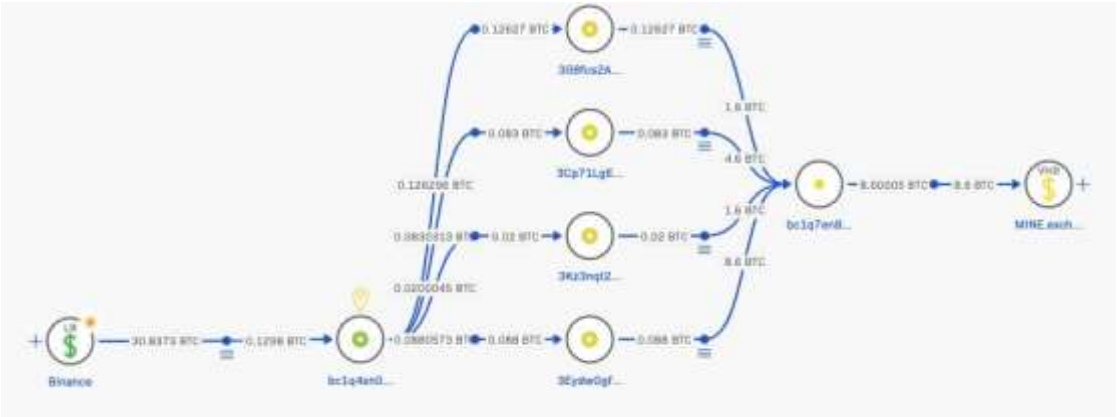


Рис. 2.2. Схема руху коштів по гаманцях у серидовищі Crystal

Crystal може допомогти виявити шаблони поведінки користувачів, які можуть вказувати на злочинну діяльність, такі як використання криптовалют для фінансування тероризму, кіберзлочинності або інших злочинів. Дане серидовище чудово справляється з даною задачею, адже кожний працівник правоохоронних органів прекрасно розуміє, що чим раніше він зрозуміє як мислить злочинець – тим бистріше він зможе його виявити.

2.2. Можливості середовища Crystal, за допомогою яких ведеться розслідування кіберінцидентів та їх наслідків

Розберемо основні можливості серидовища Crystal, за допомогою яких ми можемо вести рослідування кіберінцидентів:

Аналіз транзакцій: Crystal дозволяє аналізувати транзакції Блокчейну, включаючи адреси відправника та одержувача, суми, час і дату виконання. Інструмент надає можливість проводити детальний аналіз графіків транзакцій, визначати зв’язки між різними адресами та розуміти, куди надходять кошти.

Виявлення незвичайної активності: Crystal використовує алгоритми та моделі для виявлення незвичайної або підозрілої активності в мережі Блокчейн. Він може виявляти моделі поведінки, які можуть вказувати на незаконну діяльність або кіберзагрози.

Пошук зв’язків: Crystal допомагає створювати зв’язки між різними адресами, гаманцями та транзакціями в Блокчейні. Він може аналізувати зв’язки

між темами, ідентифікуючи групи чи організації, які мають спільну адресу або взаємодіють одна з одною. Це дозволяє слідчим ідентифікувати складні кіберзлочинні мережі та встановлювати зв'язки між ними.

Аналіз ризиків і виявлення моделей поведінки: Crystal використовує інструменти аналітики для оцінки ризиків і виявлення незвичайних моделей поведінки в Блокчейні. Він може ідентифікувати потенційно шкідливі або небезпечні транзакції, зіставляючи їх зі сценаріями злочинів або попередніми інцидентами, допомагаючи виявляти підозрілу активність.

Візуалізація даних: Crystal надає інструменти візуалізації даних, які допоможуть вам зрозуміти складні зв'язки та відносини між різними об'єктами в мережі Блокчейн. Візуальне представлення даних у вигляді графіків, діаграм і дерев допомагає дослідникам швидше отримати розуміння та зробити висновки.

Юридична підтримка: Crystal надає функціонал, що допомагає забезпечити юридичну підтримку під час розслідування кіберінцидентів. Інструмент дозволяє генерувати звіти, створювати довідкові матеріали та підтримувати ланцюжки доведень, що може бути корисним.

Не зайвим буде розглянути кожний з цих пунктів більш детально.

– *Аналіз транзакцій:*

Аналіз транзакцій за допомогою Crystal дозволяє виявляти адреси відправника та одержувача в транзакціях Блокчейну. Це допомагає слідчим визначити, хто бере участь у транзакціях і які адреси взаємодіють одна з одною.

Однією з переваг Crystal є те, що це середовище дозволяє визначати суми транзакції (рис. 2.3). Crystal надає інформацію про суму, перераховану в кожній транзакції.

У самому середовищі це виглядає наступним чином:

Рис. 2.3. Детальний розгляд транзакцій

Ми можемо вибрати кілька транзакцій та створити візуалізації, які дають більш краще розуміння ситуації.

Аналіз часу й дати виконання: Crystal зберігає дані про час і дату виконання для кожної транзакції. Це дозволяє відстежувати історію подій і встановлювати зв’язки між різними транзакціями, що корисно для виявлення закономірностей або незвичайної активності. Під аналізом часу маються на увазі наступні процеси:

Шаблони активності: виявляє незвичайні шаблони активності, спостерігаючи часові інтервали між транзакціями. Наприклад, він може виявити випадки, коли користувач здійснює надто багато транзакцій протягом короткого проміжку часу або здійснює дії в незвичайні години. Це може свідчити про автоматизовану діяльність або спробу ухилення від виявлення.

Взаємодія між адресами: Аналіз часу виконання допомагає встановити зв'язки між різними адресами у мережі Блокчейн. Crystal може виявляти випадки, коли дві або більше адрес здійснюють транзакції майже одночасно або з незвичайними інтервалами. Це може вказувати на спільну участь в небезпечних або шахрайських діях.

Також чудовим інструментом є аналіз графіка транзакцій. Crystal надає можливість будувати графік транзакцій для візуалізації зв’язку між різними адресами та транзакціями в мережі Блокчейн (рис. 2.4). Це допомагає дослідникам легше зрозуміти взаємодію між різними суб’єктами та встановити моделі поведінки.

Рис. 2.4. Демонстраційний графік транзакцій [13]

Завдяки можливості побудови транзакцій на графіку дослідники можуть отримати графічне представлення взаємодії між різними об’єктами в мережі. Це допомагає виявити зв’язки між різними адресами, транзакціями та учасниками мережі Блокчейн. Аналіз графіків транзакцій дозволяє дослідникам побачити групи адрес, які взаємодіють одна з одною, і встановити моделі поведінки. Наприклад, вони можуть виявити певні адреси, які часто взаємодіють одна з одною, що може вказувати на якусь фінансову діяльність або зв’язок між учасниками.

Аналіз графіка транзакцій також може допомогти виявити незвичні моделі поведінки, наприклад групові транзакції або обмін активами між певними адресами. Це корисно для виявлення потенційно підозрілої або шахрайської діяльності в мережі Блокчейн. Загалом, аналіз графіків транзакцій у середовищі Crystal допомагає виявити складні взаємозв’язки та визначити моделі поведінки між адресами та транзакціями в мережі Блокчейн. Це допомагає нам зрозуміти фінансову взаємодію та виявити потенційно підозрілу діяльність.

– *Виявлення незвичайної активності:*

Crystal аналізує різні аспекти транзакцій і взаємодій у мережах Блокчейнів, щоб виявити аномальні моделі поведінки. Вивчіть такі характеристики, як суми транзакцій, час виконання, взаємодіючі сторони, шаблони транзакцій і зв’язки між ними. Використовуючи аналітичні алгоритми, Crystal може виявити такі незвичайні моделі:

– *незвичні суми:* Серидовище аналізує суми транзакцій та порівнює їх з типовими або очікуваними значеннями. Він виявляє великі або надзвичайно малі транзакції, які можуть свідчити про нелегальні дії або використання мережі для відмивання грошей.

– *незвичайні шаблони:* Crystal аналізує послідовність транзакцій і виявляє незвичайні шаблони або повторювані дії. Наприклад, він може виявити часті обміни між певними адресами або надмірну активність в короткий період часу, що може свідчити про шахрайство або злочинну діяльність.

– *підозрілі зв'язки:* даний інструмент аналізує зв'язки між адресами, контрагентами та транзакціями, щоб виявити підозрілі зв'язки або спільну участь у незаконних діях. Він виявляє складні мережі взаємодій між різними суб'єктами та встановлює залежності, які можуть вказувати на шахрайство, фінансові злочини або інші підозрілі дії.

- *нові моделі поведінки:* Crystal постійно оновлює свої алгоритми та моделі, щоб виявляти нові моделі поведінки, які можуть свідчити про незаконну або підозрілу активність. Він аналізує нові тренди, методи атак та шахрайство для ідентифікації небезпечних сценаріїв та попередження можливих загроз.

Діаграма підключень (рис 2.5) також являється невід’ємною частиною розслідування кіберінцидентів. Вона надає візуальне зображення зв'язків між адресою і всіма типами суб'єктів. Ліва сторона діаграми показує типи суб'єктів, які надіслали кошти на адресу. Права сторона діаграми показує типи суб'єктів, які отримали кошти від адреси або суб'єкта (для всіх підключень це може бути через ланцюжок транзакцій) та частку загальної суми, яка була відправлена. Ви можете побачити суму, відправлену/отриману від певного типу суб'єкта, навівши курсор

миші на відповідну лінію. Також є можливість побачити загальну суму, відправлену та отриману, у верхній частині діаграми. Лінії представляють суми, ширина лінії вказує на величину взаємодії.

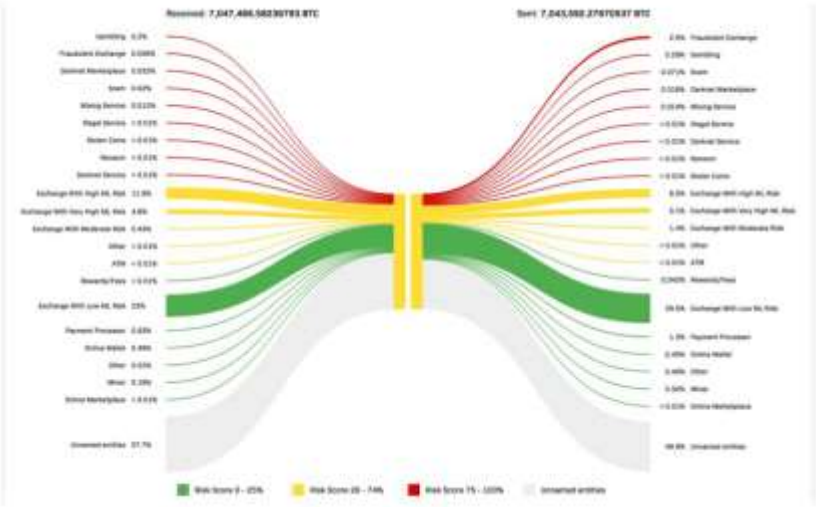


Рис. 2.5. Візуалізація діаграми підключень [14]

– Пошук зв'язків

Crystal може ідентифікувати групи чи організації, які мають спільну адресу або взаємодіють одна з одною. Наприклад, ви можете виявити групи людей, які здійснюють операції разом або використовують один гаманець. Це допомагає слідчим і правоохоронним органам виявляти складні мережі кіберзлочинців і встановлювати зв'язки між різними суб'єктами.

Цей аналіз зв'язків допомагає розкрити складні фінансові злочинні схеми, такі як відмивання грошей, шахрайство та фінансування тероризму. Це дозволяє бачити залежності між різними адресами та транзакціями (рис., таким чином будуючи повну картину фінансових відносин і встановлюючи зв'язки між різними учасниками.

Рис. 2.6. Детальна інформація, яка допомагає порівнювати транзакції [15]

Якщо розглядати проблему відмивання коштів, то Crystal використовує моделі поведінки, щоб визначити незвичайні сценарії, які можуть свідчити про відмивання грошей. Аналізує такі фактори, як обсяг транзакцій, часовий інтервал між транзакціями, тип діяльності та інші аспекти, щоб виявити аномальні моделі.

Застосунок використовує базу даних Sanctions and High-Risk Company для виявлення зв'язків із особами чи підприємствами, пов'язаними зі злочинною діяльністю чи фінансуванням тероризму. Ознак, які можуть вказувати на спробу відмиття грошей є багато, а саме: великі суми переказів, часті зміни гаманців або використання анонімних адрес.

Також у середовища є можливість отримати доступ до зовнішніх джерел інформації, таких як бази даних фінансових установ, правоохоронних органів та інших постачальників послуг, щоб виявляти підозрілі операції та ідентифікувати осіб, причетних до відмивання грошей.

Не обійшлось і без застосування нормативних стандартів. З цим у Crystal також немає проблем, адже середовище враховує нормативні стандарти та вимоги щодо боротьби з відмиванням грошей і надає інструменти та звіти, необхідні для дотримання цих стандартів.

– *Аналіз ризиків і виявлення моделей поведінки*

Аналіз ризиків використовується для оцінки ризиків, пов'язаних з різними адресами, гаманцями та транзакціями. Crystal аналізує різні фактори, такі як сума

переказу грошей, часовий інтервал між транзакціями, тип транзакції, кількість контрагентів і використовувані активи. На основі цих факторів Crystal оцінює ризики ідентифікованих осіб та їх діяльності.

Щоб виявити шаблони поведінки, Crystal аналізує історичні дані та створює шаблони або моделі, які відображають типову поведінку об’єктів у мережі Блокчейн. Виявляє незвичні моделі діяльності, які відхиляються від цих моделей. Наприклад, ви можете виявити надзвичайно високі обсяги трафіку, несподівані з’єднання між адресами або незвичні послідовності транзакцій.

Розпізнавання моделей поведінки може допомогти виявити підозрілі або незаконні дії, такі як відмивання грошей, фінансування тероризму та шахрайство. Це допомагає компаніям з обмеженою відповідальністю та іншим організаціям з кібербезпеки виявляти такі загрози та реагувати на них.

Crystal використовує різні методи аналізу, включаючи статистичний аналіз, машинне навчання та штучний інтелект, для виявлення незвичайних моделей поведінки. Він навчається на основі великого обсягу даних про транзакції та активність у Блокчейні, що дозволяє йому розпізнавати зразки та зв'язки між різними адресами, гаманцями та транзакціями.

Крім того, Crystal використовує сигнатури та правила, які визначають характеристики відомих шаблонів атак або незаконної діяльності. Він порівнює активність у мережі Блокчейн з цими сигнатурами та правилами, щоб виявити відповідність та сповістити про можливі підозрілі ситуації.

У разі виявлення незвичайної активності або підозрілого зв'язку, Crystal може генерувати сповіщення, які допомагають слідчим та кібербезпековим командам вжити відповідних заходів. Це може включати подальший аналіз, розслідування та дії щодо постраждалих суб’єктів або адрес. Усі ці функції Crystal спрямовані на покращення кібербезпеки та виявлення незаконної чи зловмисної активності в мережах Блокчейн. Забезпечуючи безпеку даних і активів у Блокчейні, ми допомагаємо організаціям і слідчим виявляти та боротися з діяльністю кіберзлочинців.

Моніторинг та виявлення ризикових сигналів: Crystal перевіряє різні показники ризику, такі як зв'язки з відомими шахраями, використання небезпечних адрес або надмірна активність, щоб виявити потенційну підозрілу активність (рис. 2.7). Він аналізує транзакції та взаємодію з підозрілими об'єктами або шаблонами, що можуть вказувати на небезпечну або нелегальну діяльність.

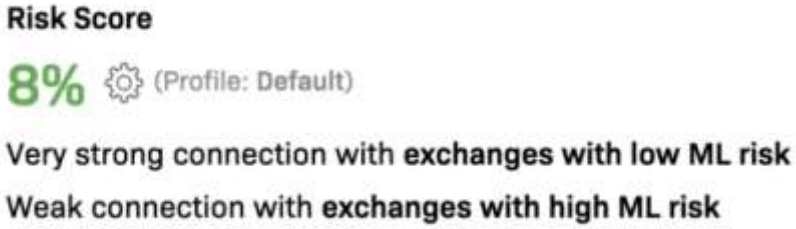


Рис. 2.7. Інформація щодо ризику транзакції [14]

Оцінка ризику – це міра, яка допомагає оцінити ймовірність того, що адреса пов’язана з незаконною діяльністю. Значення можуть бути від 0% до 100%. Відповідно 0% означають, що адреса є безпечною, та немає нічого спільного з кримінальним світом, а 100% означають, що адреса залучена до незаконної діяльності. Якщо адреса належить суб’єкту господарювання, його оцінка ризику відповідає оцінці ризику суб’єкта. Значення оцінки ризику відображаються у вигляді чисел і є декілька кольорових категорій:

- Червоний – 75-100%
- Жовтий – 25-74%
- Зелений – 0-24%
- Чорний – н/д

– Візуалізація даних

За допомогою рішень візуалізації від Crystal ви можете стежити за потоком криптовалют, візуально досліджувати, що відбувається в Блокчейні, і використовувати дані в дії. Цей інструмент дозволяє візуалізувати дані Блокчейна за адресою або сутністю. [11]

Щоб запустити візуалізацію на інформаційній панелі Crystal, відкрийте сторінку організації, адреси або транзакції та натисніть кнопку візуалізації. Якщо ви переглядаєте сутності, доступна опція «Перегляд за сутністю». Однак якщо ви починаєте візуалізацію зі сторінки «Транзакції» або «Адреси», у вас є можливість вибрати візуалізацію (рис. 2.8) за адресою або за сутністю.

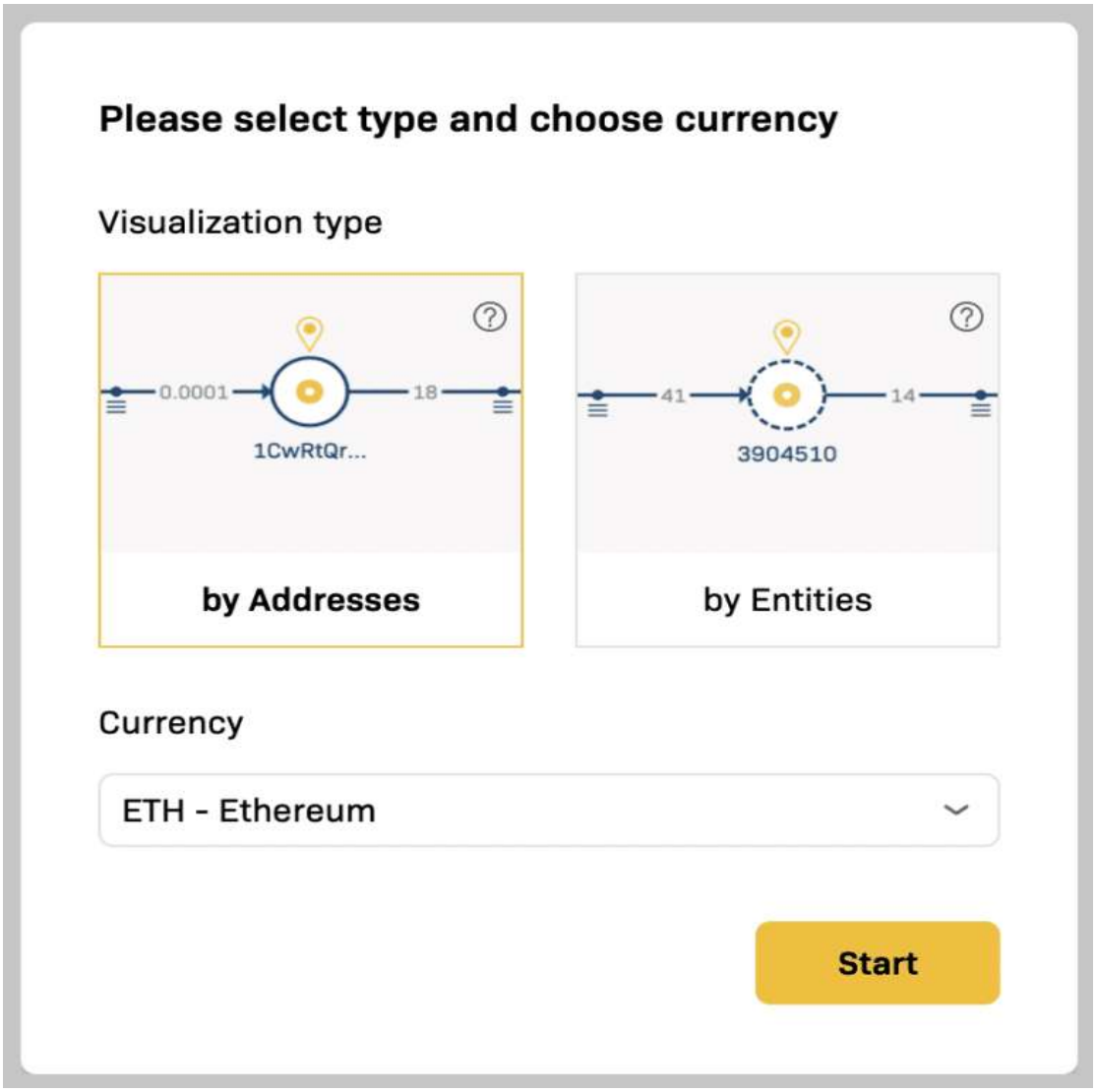


Рис. 2.8. Наявні типи візуалізацій [14]

Один із прикладів графіків це графіки залежностей (рис. 2.9). Ці графіки показують залежності між різними суб'єктами та їх взаємодію в мережі Блокчейн. Вони дозволяють візуалізувати складні мережі залежностей, виявляти основні учасники та ролі, а також встановлювати взаємозв'язки між ними.

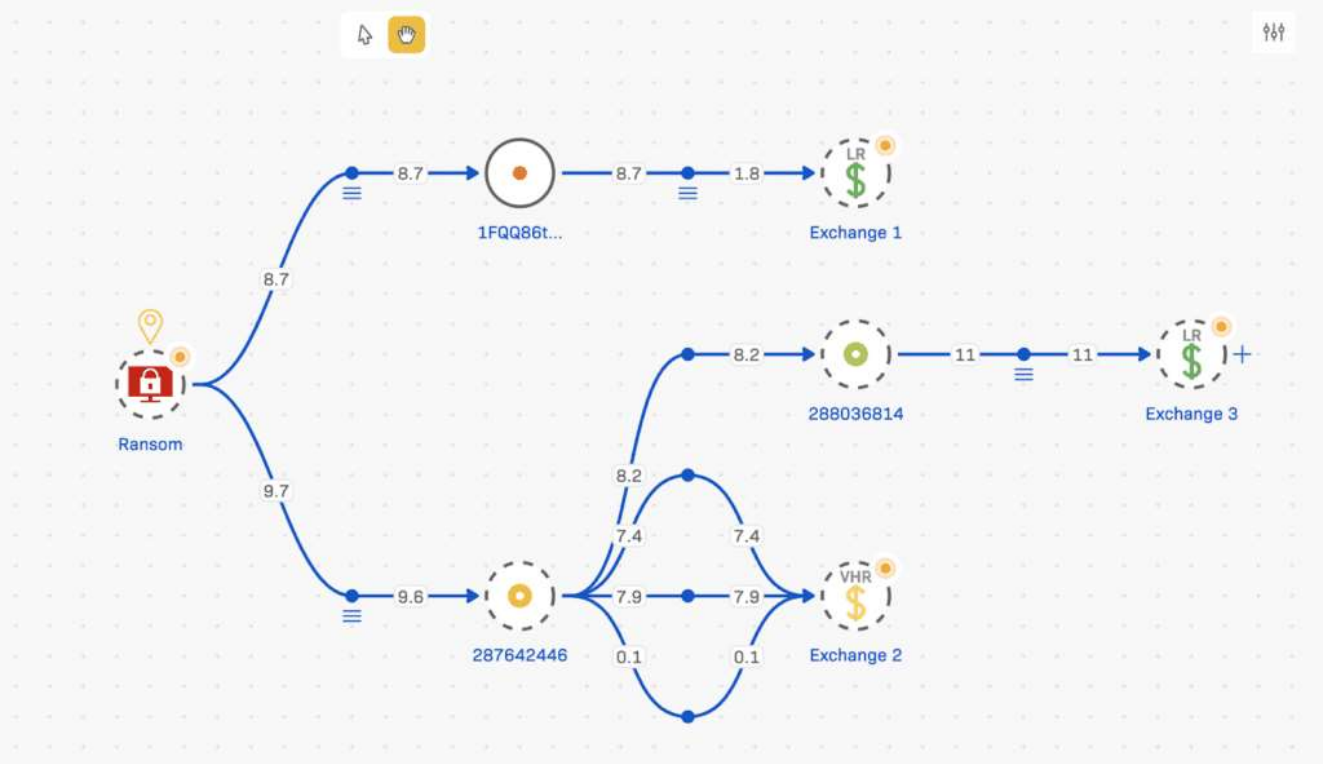


Рис. 2.9. графік залежності [11]

– Юридична підтримка

Crystal надає пряму юридичну підтримку в секторі Блокчейн: Crystal - це аналітичний інструмент, призначений для аналізу Блокчейн-транзакцій та виявлення аномальної активності. Він допомагає виявити підозрілі транзакції та моделі поведінки, які можуть свідчити про злочинну діяльність або кіберзагрози. Однак юридичний супровід у сфері Блокчейну може потребувати консультацій юристів та правових експертів з глибокими знаннями технології Блокчейну, криптовалют та регулювання.

Експерти у сфері Блокчейну можуть надати необхідні консультації щодо правових аспектів використання Блокчейну, реалізації криптовалютних проектів, вирішення спорів, пов'язаних з Блокчейном, та дотримання відповідного законодавства. Організації, які використовують Crystal для аналізу транзакцій, можуть співпрацювати з юридичними консультантами та компаніями, що мають досвід у сфері Блокчейну та криптовалют. Це дає їм комплексний підхід до

вирішення юридичних питань, пов'язаних з технологією Блокчейн і криптовалютами, і забезпечує дотримання відповідної законодавчої бази.

Важливо зазначити, що юридичні консультації є важливим фактором успіху Блокчейн- та криптовалютних проектів. Юридичний супровід допоможе розібратися в правових аспектах, забезпечити дотримання законодавства, запобігти порушенням і зберегти інтереси компанії. Конкретні послуги, які можуть надавати фахівці з Блокчейн-права, включають Консультації щодо регуляторного середовища: юристи можуть допомогти вам розібратися в законах, правилах і нормах, що стосуються використання Блокчейну і криптовалют. Вони також можуть надати поради щодо дотримання нормативних вимог та впровадження необхідних комплаєнс-заходів.

Складання юридичних договорів і контрактів: Ми можемо допомогти в розробці та належному формулюванні договорів, що регулюють взаємодію з партнерами, клієнтами та іншими зацікавленими сторонами в секторі Блокчейн. Це можуть бути договори про розробку та використання Блокчейн-проектів, договори про зберігання цифрових активів та договори про залучення коштів через первинне розміщення монет (ICO). Захист від злочинів та спорів Юридичні експерти можуть допомогти у розробці стратегій запобігання злочинам, пов'язаним з Блокчейном та криптовалютами. Вони також можуть надавати консультації з правової безпеки та розробляти плани дій для уникнення спорів та їх вирішення, якщо вони виникають.

Забезпечення дотримання відповідності: Юристи допоможуть вам розробити політики та процедури з дотримання відповідності, що стосуються Блокчейну та криптовалют. Вони нададуть поради щодо відповідності антигрошовому відмиванню коштів (AML) та зневірізації клієнтів (KYC), а також інших регулятивних вимог. Вони також допоможуть вам розробити механізми перевірки та ідентифікації користувачів, щоб забезпечити безпеку та виключити можливість зловживання.

Розробка стратегій інтелектуальної власності: Юридичні фахівці з Блокчейну допоможуть вам захистити ваші інтелектуальні права, пов'язані з інноваційними Блокчейн-рішеннями або криптовалютними технологіями. Вони допоможуть вам зареєструвати патенти, товарні знаки та авторські права, а також розробити стратегію забезпечення конфіденційності та захисту інформації.

Враховуючи складність юридичних питань у сфері Блокчейну та криптовалют, важливо співпрацювати з досвідченими юридичними фахівцями, які мають глибокі знання в цій галузі. Вони допоможуть вам зрозуміти правові ризики, визначити потенційні проблеми та розробити ефективні стратегії для успішного використання Блокчейну та криптовалют у вашому бізнесі.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ, ЩОДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ У BLOCKCHAIN У СЕРИДОВИЩІ CRYSTAL

Загалом надання рекомендацій щодо розслідування кіберінцидентів у середовищах Crystal передбачає комплексний аналіз даних, виявлення потенційних загроз, надання рекомендацій і надання юридичної підтримки. Це допомагає ефективно боротися з кіберінцидентами в Блокчейні, захищати користувачів і забезпечувати безпеку всієї системи. Розробка рекомендацій в середовищі Crystal базується на використанні високотехнологічних методів аналізу даних і спеціалізованих алгоритмів.

Перший етап – є збір даних про кіберінциденти в Блокчейні. Crystal взаємодіє з різноманітними джерелами даних, включаючи мережі Блокчейну, дані транзакцій, інформацію про гаманець та інші важливі аспекти. Ці дані узагальнюються та підлягають подальшому аналізу.

Другий етап – це аналіз даних за допомогою різних методів і алгоритмів машинного навчання. Crystal виявляє незвичайну активність, аномалії та підозрілі моделі поведінки учасників мережі. Наприклад, ви можете виявити надмірну активність певного гаманця, незвичні зв’язки між адресами або незаконні транзакції.

*Третій етап – н*а третьому етапі визначаються ризики та оцінюються можливі наслідки. Crystal аналізує виявлені кіберінциденти та оцінює їх значимість і потенційний вплив на Блокчейн. Це допомагає нам визначити пріоритетність наших розслідувань і визначити наш подальший курс дій. Це важлива частина розслідування, оскільки вона допомагає нам визначити пріоритетність конкретних подій і визначити наш подальший курс дій. Аналіз, проведений Crystal, надає детальну інформацію про можливі наслідки кіберінцидентів і пов’язані з ними ризики. Це дозволяє нам ефективно розподіляти ресурси та зосереджуватися на дослідженні та реагуванні на

найбільші загрози Блокчейну. Систематичний аналіз і оцінка забезпечують об'єктивність у визначенні пріоритетів і раціональному використанні ресурсів і зусиль для забезпечення безпеки і надійності Блокчейн-платформ.

Четвертий етап – передбачає візуалізацію даних для легшого розпізнавання та аналізу. Crystal надає можливість відображати дані у вигляді графіків, діаграм, діаграм або інших візуальних елементів. Допомагає визначити зв’язки, залежності та аномалії в даних, які можуть вказувати на кіберінциденти. Візуалізація даних полегшує розуміння складних взаємозв’язків і допомагає визначити закономірності та тенденції, які допомагають розслідуванню.

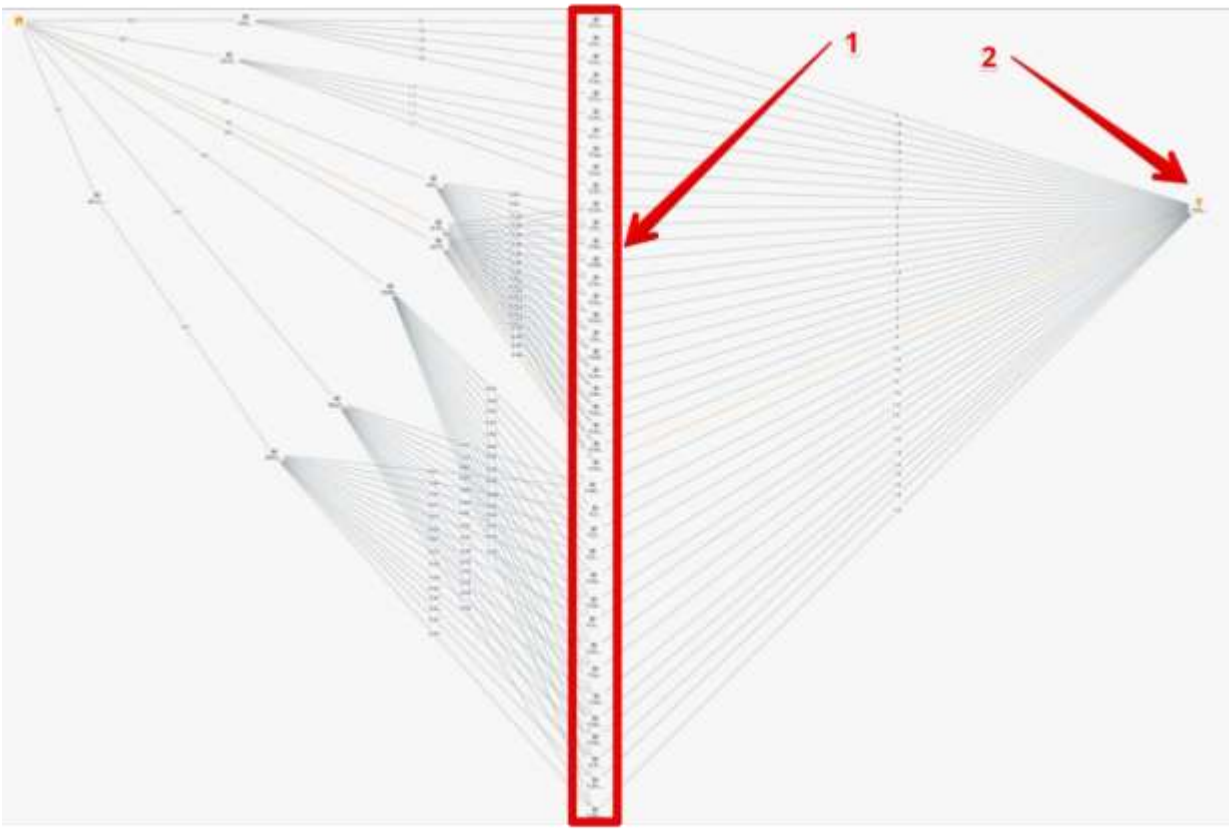


Рис. 3.1. Візуалізація зв’язків залежності [13]

П’ятий етап – складання рекомендацій. На основі зібраних даних, аналізу, ідентифікації та візуалізації ризиків Crystal дає конкретні рекомендації щодо наступних кроків у розслідуванні кіберінциденту. Це можуть бути рекомендації щодо збору додаткових доказів, співпраці зі спеціалізованими органами, заборони

певних адрес або транзакцій, вжиття заходів для забезпечення безпеки мережі тощо.

Шостий етап – юридичний супровід. Як вже було сказано раніше, Crystal надає юридичну експертизу та підтримку для вирішення юридичних аспектів розслідування кіберінцидентів Блокчейну. Це допомагає нам визначити відповідні судові заходи, виявити порушення закону та забезпечити дотримання нормативних вимог. В цілому, розроблення рекомендацій щодо розслідування кіберінцидентів у середовищі Crystal передбачає комплексний підхід, починаючи зі збору та аналізу даних, виявлення незвичайних активностей, визначення ризиків, візуалізації даних, розробки рекомендацій та надання юридичної підтримки. Цей процес допомагає виявляти, розслідувати та ефективно вирішувати кіберінциденти у Блокчейні, сприяючи підвищенню безпеки та довіри до цифрових активів.

Застосування Crystal для розслідування кіберінцидентів у Блокчейні має декілька переваг. По-перше, він використовує передові аналітичні методи та алгоритми, що дозволяють швидко та ефективно виявляти підозрілі активності та загрози. По-друге, Crystal надає велику кількість інформації та візуалізаційних засобів, що полегшують розуміння складних зв'язків та шаблонів у Блокчейні. По-третє, його юридична підтримка допомагає враховувати правові аспекти та забезпечувати відповідність регуляторним вимогам.

Важливо також зазначити, що розроблення рекомендацій у середовищі Crystal є динамічним процесом. З огляду на постійний розвиток технологій та зміну кіберзагроз, Crystal постійно оновлюється та адаптується для забезпечення ефективного виявлення та розслідування нових типів кіберінцидентів.

Узагальнюючи, розроблення рекомендацій щодо розслідування кіберінцидентів у середовищі Crystal є складним процесом, що включає збір та аналіз даних, виявлення підозрілих активностей, визначення ризиків, візуалізацію даних, розробку конкретних рекомендацій та надання юридичної підтримки. Використання Crystal допомагає підвищити ефективність розслідування та

забезпечити безпеку Блокчейн-мережі шляхом ідентифікації, аналізу та реагування на кіберінциденти. Завдяки розробленню рекомендацій у середовищі Crystal, організації та правоохоронні органи можуть швидше виявляти та вирішувати кіберзагрози, зменшуючи їхні наслідки та запобігаючи подібним інцидентам у майбутньому.

Розроблення рекомендацій у середовищі Crystal також сприяє співпраці та обміну інформацією між різними сторонами, такими як організації, правоохоронні органи, регулятори та експерти з кібербезпеки. Це дозволяє створити спільні стратегії та практики для ефективного розслідування та запобігання кіберінцидентам у Блокчейні.

Окрім того, розроблення рекомендацій у середовищі Crystal може сприяти вдосконаленню процесу забезпечення безпеки у Блокчейні. Виявлення та аналіз кіберінцидентів дозволяє виявити слабкі місця та недоліки у системі, що можуть бути використані зловмисниками. На основі цих даних можна розробити та впровадити відповідні заходи безпеки, щоб запобігти подібним інцидентам у майбутньому. Загалом розробка рекомендацій щодо розслідування кіберінцидентів у середовищі Crystal є важливим кроком у боротьбі з кіберзагрозами на Блокчейні. Це полегшує виявлення, аналіз та ефективне вирішення кіберінцидентів, сприяючи безпеці та довірі до цифрових активів у мережах Блокчейн.

3.1 Етапи у розслідуванні кіберінцидентів у Blockchain

У розслідуванні кіберінцидентів у Блокчейні використовуються різні алгоритми, нюанси та аналізи для ефективного виявлення та розкриття злочинних дій. Це включає аналіз транзакційного потоку, виявлення незвичайної активності, аналіз поведінки адрес, використання візуалізації графіків транзакцій, застосування алгоритмів машинного навчання та комбінацію даних з різних джерел. Метою цих алгоритмів та аналізів є виявлення незаконних дій, встановлення зв'язків між суб'єктами та виявлення підозрілого активу. Вони

допомагають розробити рекомендації для поліпшення розслідування кіберінцидентів у Блокчейні та забезпечити ефективність процесу розкриття злочинних дій.

Ось кілька ключових аспектів, які варто врахувати:

Аналіз поведінки адреси: Аналізуючи поведінку окремих адрес у Блокчейні, ми можемо виявити закономірності та норми їх діяльності. Відстежуючи зміни в поведінці адреси, ви можете виявити незвичну або підозрілу активність, як-от: В. Збільшення обсягу транзакцій, спроби маршрутизації активів через інші адреси або використання нових шаблонів транзакцій. Цей аналіз допомагає виявити підозрілих зловмисників і з'ясувати їх роль у кіберінцидентах.

Використання машинного навчання: Машинне навчання є потужним інструментом для аналізу даних під час розслідування кіберінцидентів. Це дозволяє розробляти моделі, які розпізнають закономірності та аномалії в поведінці адрес, транзакцій або Блокчейн-мереж. Це дозволяє автоматизувати процес виявлення та аналізу підозрілої активності та швидше виявляти кіберзагрози (рис. 3.1).

Блокчейн широко застосовується в банківському секторі завдяки використанню Bitcoin. Зовсім недавно він був інтегрований у багато інших сфер, включаючи фармацевтичне виробництво, операції в ланцюзі поставок, охорону здоров'я та багато інших важливих сфер. У той час як ML відомий тим, що автоматизує вирішення проблем за допомогою застосування статистичних комп'ютерних алгоритмів або моделей, Блокчейн підтримує розподілену цифрову книгу, яка зберігає всі дані в дуже безпечний спосіб. , широко використовується для зберігання фінансових транзакцій і даних. [12]

Окрім обробки величезних обсягів бізнес-даних і побудови ефективної системи прогнозування, яка автоматично приймає рішення, ML добре відомий своєю здатністю аналізувати шаблони в наборі даних і інтерпретувати шаблони в бізнес-даних для створення чудових візуальних графіків і інтерполяції, які можна використовувати надати уявлення про топ-менеджмент. У страховому секторі

нещодавно для прогнозування фінансових ризиків використовували передові алгоритми ML. [12]

Страхові фірми можуть точно оцінити ризики, пов'язані зі стягненням нових страхових премій, завдяки ML, який запускає свої алгоритми на величезних обсягах фінансової інформації та виявляє певну приховану закономірність. Blockchain створює розподілену книгу із захищеною транзакційною базою даних, яка має точні мітки часу та незмінні та постійні екземпляри даних. [12]

Основна причина, чому Блокчейн настільки відомий, полягає в тому, що він використовує цифрові підписи як особливий метод досягнення угоди щодо об'єктів фінансових даних. Для створення надійних моделей ML потрібна велика кількість даних. Збір, систематизація та перевірка даних — це простий підхід, що підтримується Блокчейном і може підвищити точність даних. [12]

Блокчейн значно покращує безпеку даних шляхом автоматизації передбачення того, які типи даних слід зберігати та обробляти в ланцюжку, щоб зробити примірник максимально доступним. Блокчейни пропонують чудову підтримку стандартів для захисту великих обсягів даних на кількох вузлах, роблячи дані доступними в зашифрованому вигляді. Блокчейни децентралізовані, що може призвести до прогалин у безпеці[41]. Найбільш поширеною проблемою є те, що атаки можуть порушити процес консенсусу та дозволити декільком фермам майнінгу контролювати блоки, розміщені в мережі. Цей конкретний ризик існує в публічних Блокчейнах. Приватні версії несприйнятливі до цієї атаки, оскільки кожен вузол унікально ідентифікований і встановлено процес консенсусу.

У сфері безпеки поєднання Блокчейну та машинного навчання пропонує нові та більш надійні рішення (рис. 3.1). Наприклад, Блокчейн можна використовувати для створення незмінних записів транзакцій, які неможливо змінити, або для навчання алгоритмів машинного навчання розпізнаванню шахрайських моделей у фінансових транзакціях. Блокчейн також можна використовувати для безпечного зберігання даних про мережеву активність, а

алгоритми ML можна використовувати для виявлення та запобігання кібератакам у режимі реального часу. [12]

ML можна використовувати для підтвердження особи користувача за допомогою біометричних даних, які можна використовувати для підтвердження особи. Якщо дані безпечно поширюються та зберігаються за допомогою Блокчейну, хакерам стає важче отримати та використовувати ці дані. За допомогою алгоритмів ML ці дані можна оцінити для пошуку підозрілих моделей поведінки та потенційних прогалин у безпеці ланцюга постачання. За допомогою Блокчейну можна надійно та прозоро задокументувати кожен крок ланцюжка поставок. Нарешті, ML можна використовувати для аналізу поведінки цих контрактів, виявлення потенційних вразливих місць у безпеці та запобігання втраті грошей та інших активів. Розумні контракти виконуються автоматично на основі попередньо визначених умов і можуть бути створені за допомогою Блокчейну. [12]

Рис. 3.1. Приклад реалізації машинного навчання

Запровадження технології Блокчейн у різних галузях підвищило обізнаність про важливість безпеки мережі Блокчейн. ML з’явився як потенційний спосіб покращити безпеку систем Блокчейну шляхом аналізу даних, розпізнавання шаблонів і виявлення потенційних загроз безпеці в режимі реального часу. Забезпечуючи безпечну, децентралізовану та незмінну цифрову книгу, Блокчейн може підвищити довіру до даних, які використовуються в алгоритмах ML. [12]

Проте Блокчейн-мережі вразливі до вразливостей безпеки та вимагають впровадження відповідних заходів безпеки та механізмів консенсусу. Поєднання Блокчейну та машинного навчання має потенціал для революції в безпеці даних, але безпеку потрібно підтримувати завжди. [12]

Кількість статей про ML і Блокчейн у контексті безпеки стабільно зростала протягом останніх чотирьох років з 2012 по 2022 рік. На рис. 3.1 наведено річну кількість публікацій за темами з 2012 по 2022 рік. Наступна діаграма показує, як змінювалися дати публікації з часом. [12]

У 2019 році було опубліковано 3 статті (9,10%), у 2021 році – 9 статей (27,27%), у 2022 році – 21 стаття (63,63%). Важливо зазначити, що використання Блокчейну та машинного навчання значно зросте, особливо у 2022 році. Найбільше опублікованих досліджень у цій сфері було проведено у 2022 році. У зв'язку зі збільшенням використання цих технологій у різних галузях промисловості, занепокоєнням щодо потенційних загроз безпеці та вдосконаленням методів машинного навчання та протоколів Блокчейну, що відкриває нові шляхи для інновацій, безпеки. У світі з'являється все більше публікацій про перетин Блокчейну та машинного навчання. поле збільшився з часом. Тому експерти в обох областях інтенсивно працюють над пошуком способів покращити безпеку Блокчейну та програм машинного навчання. [12]

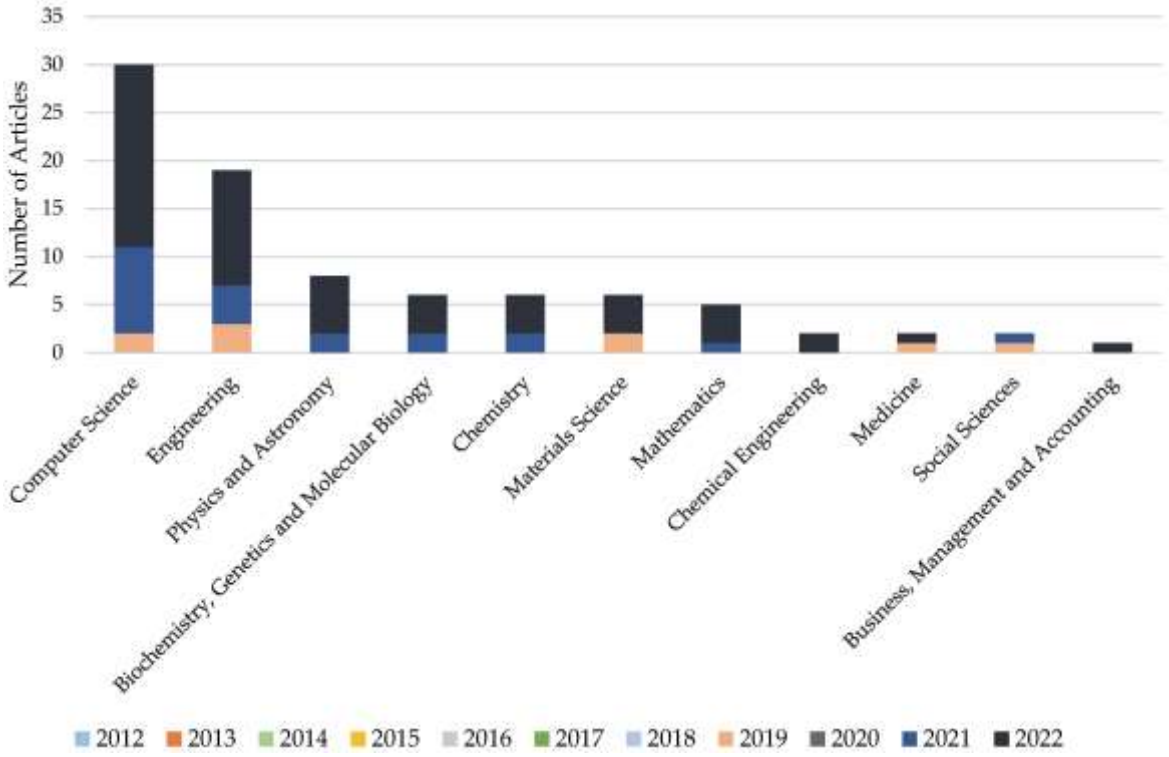


Рис. 3.1. Річна кількість публікацій про використання ML [12]

Важливо визнати швидке зростання технологій машинного навчання та Блокчейну, особливо у 2022 році. ML може зробити розподілені книги, які використовуються Блокчейнами, більш безпечними. Інформатика та інженерія є ключовими для цього. Тенденція мультидисциплінарного написання есе зростає. У застосуванні до управління Блокчейном ML має потенціал для подальшого посилення вже вражаючої безпеки мережі. Крім того, децентралізована структура Блокчейну відкриває величезну можливість створювати більш потужні моделі, що особливо привабливо, враховуючи, що ML може краще обробляти великі обсяги даних. Разом вони роблять світ безпечнішим і відкритим. У деяких випадках поєднання алгоритмів ML з Блокчейном може бути дуже корисним. Подані документи підкреслюють важливість впливу ML на безпеку Блокчейну, незважаючи на їх поточні обмеження. [12]

Незважаючи на те, що ML і blockchain мають потенціал для революції в безпеці, все ще є проблеми, які потрібно вирішити, такі як масштабованість, сумісність і конфіденційність, а також вразливість алгоритмів ML до атак грубої

сили. Поєднання навчання з нульовим знанням і перевірки є великим прогресом, і токенізація може використовуватися разом з алгоритмами ML для виявлення можливого шахрайства або ризиків безпеки. Майбутні дослідження мають бути зосереджені на методах збереження конфіденційності, покращенні ефективності та масштабованості алгоритмів ML, а також на вивченні інтеграції інших передових методів із ML і blockchain для створення нових і передових рішень для широкого спектру галузей і випадків використання. [12]

Поєднання даних і інформації: Виявлення та розслідування кіберінцидентів Блокчейну вимагає поєднання різних даних і джерел розвідки. Окрім самої мережі Блокчейн, можна використовувати й інші дані, наприклад інформацію з бірж, веб-сканерів, пошукових систем, форумів та інших джерел. Об’єднання цих даних дозволяє нам отримати більш повну картину злочинної діяльності, встановити зв’язки та ідентифікувати злочинців.

Узагальнюючи, розслідування кіберінцидентів у Блокчейні вимагає використання різних алгоритмів, аналітичних інструментів та методів для аналізу поведінки адрес, виявлення незвичайних схем транзакцій, встановлення зв'язків між різними суб'єктами та виявлення підозрілого активу. Це може включати аналіз транзакційного потоку, виявлення аномалій, використання візуалізації графіків транзакцій, застосування алгоритмів машинного навчання та комбінацію даних з різних джерел.

Розроблення рекомендацій щодо розслідування кіберінцидентів у Блокчейні у середовищі Crystal передбачає вдосконалення цих методів та інструментів. Це означає постійне оновлення алгоритмів для виявлення нових кіберзагроз, розробку моделей поведінки та аналітичних методів, адаптованих до специфіки Блокчейн-середовища.

Крім того, рекомендації можуть включати розробку інструментів для автоматизованого аналізу даних, виявлення аномалій та патернів, а також побудову ефективних моделей ризик-аналізу. Для цього можна використовувати методи машинного навчання, статистичні моделі та інші аналітичні підходи.

Ключовим фактором у виробленні рекомендацій є постійне вдосконалення знань і досвіду команди Crystal. Це включає в себе знання про нові кіберзагрози, взаємодію з експертами з кібербезпеки та використання уроків, отриманих у дослідженнях Блокчейну.

3.2 Розробка рекомендацій, щодо розслідування інцидентів у Blockchain

Розробка політики для розслідування інцидентів Блокчейну передбачає аналіз та оцінку загроз кібербезпеці, розробку стратегій реагування на інциденти та надання рекомендацій щодо покращення безпеки системи. Цей процес вимагає глибокого розуміння технології Блокчейн, використання спеціалізованих інструментів аналізу даних і врахування конкретних характеристик і проблем, пов’язаних з інфраструктурою Блокчейну. Розробка рекомендацій призведе до встановлення ефективних процедур, практик і політик, спрямованих на забезпечення безпеки Блокчейн-систем і зниження ризику кібератак.

Етапів розслідування та рекомендацій щодо них доволі багато, тому не буде лишнім поділити їх на етапи, як це робилось у минулих пунктах:

Перший етап — аналіз стану: цей етап передбачає збір і аналіз існуючої інформації про інфраструктуру Блокчейну, включаючи архітектуру мережі, протоколи зв’язку, криптографічні алгоритми, рівні безпеки та контроль доступу. Важливо визначити потенційні ризики та вразливі місця, якими можуть скористатися зловмисники.

Другий етап — визначте вимоги безпеки: на цьому етапі встановіть основні вимоги безпеки, яким повинна відповідати система Блокчейн. Це можуть бути автентифікація, авторизація, шифрування даних, зберігання ключів, контроль доступу та інші вимоги безпеки.

Однією з найважливіших вимог є аутентифікація. Це гарантує ідентифікацію та автентифікацію користувачів перед наданням доступу до системи Блокчейн. Це може включати використання криптографічних методів, біометричних даних або інших методів ідентифікації.

Авторизація — ще одна ключова вимога безпеки, яка регулює рівень доступу користувачів до різноманітних функцій і ресурсів Блокчейн-систем. Це означає встановлення правил і політик, які визначають, які дії можуть виконувати різні користувачі та які права вони мають.

Шифрування даних є ще одним важливим компонентом безпеки Блокчейн-систем. Воно забезпечує захист конфіденційності інформації, шляхом перетворення даних в зашифровану форму, яку можуть розшифрувати лише авторизовані користувачі.

Зберігання ключів є також важливою вимогою безпеки, оскільки ключі використовуються для підпису транзакцій та доступу до гаманців у системі Блокчейн. Забезпечення безпеки ключів, їх захист від втрати, крадіжки або несанкціонованого використання є критичним аспектом безпеки в Блокчейн-середовищі. Контроль доступу є ще однією важливою складовою безпеки у системі Блокчейн. Це означає встановлення механізмів, які регулюють доступ користувачів до конкретних ресурсів і функцій системи, забезпечуючи обмеження прав доступу на основі ролей, політик безпеки та інших критеріїв. Усі ці вимоги безпеки слід враховувати при розробці та впровадженні системи Блокчейн, щоб забезпечити її стійкість проти кібератак, втручання та інших загроз безпеці. Реалізація цих вимог вимагає постійного моніторингу, аналізу та оновлення заходів безпеки для забезпечення найвищого рівня безпеки для систем Блокчейн.

Третій етап - стандарти досліджень і найкращі практики: щоб розробити ефективні рекомендації, варто прочитати стандарти безпеки Блокчейну, такі як OWASP Blockchain Top 10, а також дослідити найкращі практики, які використовують відомі проекти Блокчейну.

Четвертий етап — розробка аналітичного методу: розробка аналітичних методів має допомогти виявити та розслідувати потенційні інциденти в Блокчейнах. Це методи аналізу транзакцій, виявлення незвичайних моделей поведінки, аналізу мережевої активності тощо. Аналітичні методи дозволяють

збирати, обробляти та аналізувати дані для виявлення підозрілих або незаконних дій у Блокчейні.

П’ятий етап — складання рекомендацій: на основі аналізу стандартів безпеки та результатів досліджень розроблено конкретні рекомендації щодо розслідування інцидентів у Блокчейні. Ці рекомендації можуть стосуватися використання захищених протоколів зв’язку, налаштування систем спостереження, встановлення правил контролю доступу та інших заходів безпеки.

Шостий етап — тестування та перевірка: розроблені рекомендації перевіряються та підтверджуються для забезпечення їх ефективності та відповідності вимогам безпеки. Це може включати проведення пілотних проектів, перевірку реальних даних і використання моделювання для перевірки розроблених рекомендацій.

Сьомий етап - документація та розповсюдження: остаточні рекомендації документуються та надаються зацікавленим сторонам, таким як групи безпеки, розробники проектів Блокчейну та правоохоронні органи. Це дозволяє повністю використовувати рекомендації та підвищує безпеку іспиту.

Восьмий етап — підтримка та оновлення: Політика розслідування інцидентів у Блокчейні потребує постійного моніторингу та оновлення. Технологія Блокчейн постійно розвивається, а зловмисники вдосконалюють свої методи. Тому важливо стежити за останніми тенденціями та новими загрозами, адаптувати наші рекомендації до нових викликів і забезпечувати їх актуальність.

Дев’ятий етап — освіта та навчання: Розробка політики розслідування інцидентів Блокчейну вимагає знань і досвіду в криптографії, технології Блокчейн, кібербезпеці та розслідуваннях. Тому важливо забезпечити навчання та можливості професійного розвитку для дослідників Блокчейн-кіберінцидентів.

Десятий етап — співпраця та обмін інформацією: У сфері розслідування інцидентів Блокчейну співпраця та обмін інформацією між різними сторонами, такими як компанії з кібербезпеки, правоохоронні органи та Блокчейн-компанії, є критично важливими. Це дозволить швидше виявляти і розслідувати інциденти,

обмінюватися найкращими практиками та співпрацювати для боротьби з кіберзлочинністю на Блокчейні.

Одинадцятий етап — аналіз логів Блокчейну: Перш ніж давати будь-які рекомендації, нам слід уважніше розглянути основні протоколи Блокчейну, які використовує система. Це допоможе вам зрозуміти, які функції та вразливості є унікальними для кожного протоколу, і визначити, які вдосконалення потрібно внести для покращення безпеки.

При аналізі логів Блокчейну перевіряються записи транзакцій, блоків і взаємодій між учасниками мережі. Це дозволяє нам виявляти проблеми, помилки, аномалії та вразливості, які можуть виникнути під час використання Блокчейну.

Аналізуючи протоколи Блокчейну, ми досліджуємо різні аспекти, такі як структури даних, криптографічні алгоритми, механізми консенсусу та мережева безпека. Це допомагає нам зрозуміти, які функції та вразливості має кожен протокол і які вдосконалення потрібні для покращення безпеки.

Під час аналізу ми виявляємо можливі проблемні області, такі як слабкі криптографічні алгоритми, погана автентифікація та вразливості мережевого протоколу. На основі цих відомостей ми можемо розробити конкретні рекомендації щодо покращення безпеки. Розробка рекомендацій щодо розслідування інцидентів у Блокчейн - це процес, який має на меті створення конкретних рекомендацій для покращення ефективності та безпеки в розслідуванні кіберінцидентів у Блокчейні. Цей процес включає аналіз вже існуючих інцидентів, вивчення нюансів та особливостей Блокчейн-платформи, а також розробку відповідних рекомендацій для запобігання майбутнім інцидентам.

Одним з ключових аспектів розробки рекомендацій є аналіз попередніх кіберінцидентів, які сталися в Блокчейн-мережі. Це включає дослідження типів атак, які вже відбулися, способів їх виявлення та ліквідації, а також наслідків цих інцидентів. Цей аналіз є основою для надання рекомендацій, спрямованих на запобігання подібних атак у майбутньому.

У рамках вироблення рекомендацій також проводиться детальний аналіз характеристик використовуваної технології Блокчейн. Це включає дослідження протоколів, механізмів консенсусу, криптографічних алгоритмів та інших технічних деталей. Цей аналіз дозволяє нам виявити потенційні вразливості та вразливості в нашій мережі Блокчейн і надати рекомендації щодо їх усунення.

Крім того, розробка рекомендацій вимагає співпраці з експертами з глибокими знаннями у сфері Блокчейну та кібербезпеки. Це можуть бути професіонали зі сфери кібербезпеки, розробники Блокчейн-проектів, аудитори та інші спеціалісти. Їхні внутрішні знання та досвід допомагають розробити комплексні рекомендації, що враховують різноманітні аспекти безпеки та розслідування інцидентів у Блокчейн.

У результаті розробки рекомендацій отримується документ, який містить конкретні заходи та рекомендації щодо покращення безпеки та ефективності розслідування кіберінцидентів у Блокчейн-мережі. Ці рекомендації можуть стосуватися оновлення протоколів, вдосконалення механізмів безпеки, встановлення нових процедур та розробки політик безпеки. Крім того, важливо забезпечити впровадження цих рекомендацій та оцінити їх ефективність у реальному середовищі розслідування кіберінцидентів у Блокчейн.

Дванадцятий етап — визначте потенційні загрози: На цьому етапі виконується аналіз потенційних загроз безпеці, які можуть вплинути на систему Блокчейн. Це можуть бути атаки на протоколи, зловживання властивостями Блокчейна, уразливості смарт-контрактів тощо. Визначивши ці загрози, ви можете зосередитися на їх усуненні та заходах безпеки.

Тринадцятий етап — розробка методів аналізу та виявлення: Встановлення методів для аналізу та виявлення кіберінцидентів у Блокчейні є важливим для надання рекомендацій. Це такі методи, як моніторинг мережі, виявлення аномалій, аналіз сигнатур і перевірка смарт-контрактів. Розробка ефективних методів може допомогти виявити аномальну або підозрілу активність у Блокчейні та розпочати розслідування.

Чотирнадцятий етап — визначення процедур реагування: При розробці політики також важливо визначити процедури реагування на кіберінциденти Блокчейна. Це включає розробку протоколів і процедур для негайного реагування на виявлені інциденти та швидкого припинення атак для мінімізації збитків. Розробка таких процедур повинна враховувати деталі систем Блокчейн і відповідати стандартам безпеки.

П’ятнадцятий етап — введення заходів безпеки: На основі аналізу загроз і вимог до безпеки слід розробити набір заходів безпеки для запобігання інцидентам Блокчейну. Це засоби автентифікації та авторизації користувачів, шифрування даних, захисту закритих ключів, налаштування правил контролю доступу тощо. Впроваджуючи ці заходи, ви можете зменшити ризик уразливості та забезпечити безпеку вашої системи.

Шістнадцятий етап — розробка навчального матеріалу: Для ефективного впровадження рекомендацій слід підготувати навчальні матеріали, які допоможуть користувачам і фахівцям з кібербезпеки зрозуміти принципи безпеки Блокчейна та застосувати рекомендації на практиці. Це включає посібники, навчальні курси, вебінари та інші форми навчальних матеріалів.

Сімнадцятий етап — впровадження та оцінка ефективності: Після того, як рекомендація була зроблена, її необхідно виконати. Важливо оцінити ефективність рекомендацій шляхом моніторингу кіберінцидентів, виявлення вразливостей і пошкоджень, а також збору відгуків від користувачів і експертів. Це допомагає виявити потенційні слабкі місця та сфери, які потребують покращення в рекомендаціях.

Реалізація рекомендацій вимагає активної співпраці з командою технічних експертів і розробників для впровадження необхідних змін у систему. Це може включати встановлення нових протоколів безпеки, налаштування інструментів моніторингу, впровадження криптографічних схем або інших технічних заходів для покращення безпеки Блокчейну.

Оцінка ефективності рекомендацій також включає моніторинг кіберінцидентів після виконання рекомендацій. Його метою є систематичне визначення, аналіз і реагування на потенційні загрози та вразливі місця, які можуть виникнути в системах Блокчейн. Цей процес дозволяє нам оцінити ефективність наших рекомендацій і визначити, наскільки добре наші рекомендації запобігали або обмежували кіберінциденти.

Окрім моніторингу кіберінцидентів, важливо також збирати відгуки від користувачів та експертів. Це можна здійснювати через опитування, діалоги, обговорення на спеціалізованих форумах або взаємодію зі спільнотою користувачів Блокчейн-системи. Збір відгуків допомагає отримати цінну інформацію про те, як рекомендації сприймаються користувачами та експертами, а також виявити можливі недоліки або додаткові побажання щодо рекомендацій.

Після отримання відгуків із спільноти користувачів та експертів проводиться їх аналіз та врахування при подальшому вдосконаленні рекомендацій. Цей процес допомагає виявити потенційні слабкі місця у виконанні рекомендацій та ідентифікувати області, які потребують додаткового покращення. Даючи рекомендації щодо розслідування інцидентів Блокчейну, ви можете постійно вдосконалювати процеси безпеки та реагування на кіберінциденти. Це дозволяє нам забезпечити оптимальний захист Блокчейн-систем, запобігати виникненню загроз, а також ефективно виявляти й досліджувати потенційні проблеми. В результаті забезпечується довіра, конфіденційність і цілісність систем Блокчейн, що сприяє довірі користувачів і стабільному функціонуванню цифрового середовища.

Вісімнадцятий етап — постійні оновлення та адаптації: Технологія Блокчейн стрімко розвивається, а загрози кібербезпеці постійно змінюються. Тому створення рекомендацій має бути процесом постійного оновлення та адаптації. Щоб забезпечити найвищий рівень безпеки, важливо відстежувати нові загрози, технічні зміни, найкращі практики та надавати рекомендації щодо оновлення.

Дев’ятнадцятий етап — міжнародна співпраця: Розробка рекомендацій щодо розслідування інцидентів Блокчейну має включати міжнародну співпрацю та обмін досвідом. Співпраця з іншими країнами, міжнародними організаціями та органами стандартизації допоможе створити загальні стандарти безпеки та розробити взаємозалежні політики, спрямовані на глобальну кібербезпеку на Блокчейні.

Загальний процес розробки політики розслідування інцидентів Блокчейну включає аналіз, розробку методів, визначення процедур реагування, заходи безпеки, навчання, оцінку ефективності та поточні оновлення. Співпраця, обмін інформацією та міжнародна співпраця також відіграють важливу роль у створенні ефективної політики.

ВИСНОВКИ

В ході виконання бакалаврської роботи мною вдалось дослідити проблемні питання у Блокчейні, які прагнули вдосконалення. Також вдалось дослідити велику кількість середовищ, які допопомагають вести розслідування кіберіцнидентів. Було розроблено етапи, які допоможуть боротись із шахрайством більш якісно. Був розглянутий інструмент Crystal, який на мою думку є універсальним ключем для усунення проблемних питань у Блокчейні. У цілому, Crystal відкриває нові можливості для розслідування, допомагаючи виявляти та розкривати злочинні дії, встановлювати зв'язки між учасниками та покращувати безпеку. Цей інструмент необхідний для правоохоронних органів, аналітиків з кібербезпеки та організацій, які працюють у сфері технології Блокчейн.

Використання рекомендацій, які були розроблені мною, дозволять зменшити ризик кібератак та мінімізувати можливі наслідки в разі кіберінцидентів. Посилення захисту криптоактивів не лише збереже індивідуальний фінансовий добробут користувачів, але й сприятиме загальній стабільності та розвитку криптовалютного ринку.

ПЕРЕЛІК ПОСИЛАНЬ

1. NC Wallet – Zafiro International Ltd. [Електронний ресурс] – URL: https://ncwallet.net/ru/news/why-do-you-need-a-blockchain-explorer/#:~:text=Блокчейн%20эксплореры%20(от%20англ.,текущего%20состояния%20и%20исторических%20данных.

2. HackWare – Информация о Биткоин кошельках, [Електронний ресурс] – URL: https://hackware.ru/?p=9482

3. Uppsala Security / Protect Your Cryptocurrencies with Advanced Software Solutions from Uppsala Security!, [Електронний ресурс] – URL: https://uppsalasecurity.com

4. Bitquery / 9 Best Blockchain Analysis Tools, [Електронний ресурс] – URL: https://bitquery.io/blog/best-blockchain-analysis-tools-and-software

5. Beincrypto / За 10 лет на крипторынке украли больше денег, чем ВВП Молдавии, [Електронний ресурс] – URL: https://ru.beincrypto.com/hishhenij-kriptorynke-vvp-moldavii-crystal/

6. Blog Chainalysis The Chainalysis Crypto Crime Report, [Електронний ресурс] – URL: https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report/

7. Cointelegraph / How do blockchain forensics and asset tracking work?, [Електронний ресурс] – URL: https://cointelegraph.com/explained/how-do-blockchain-forensics-and-asset-tracking-work

8. Poradumo Анатолій Лазар, IDS – що це таке? Система виявлення вторгнень (IDS) як працює?, [Електронний ресурс] – URL: https://poradumo.com.ua/49510-ids-sho-ce-take-sistema-viiavlennia-vtorgnen-ids-iak-pracuye/

9. Maltego / Версія 4.2.11 (4 червня 2020; 2 роки назад), Википедия : Свободная энциклопедия, [Електронний ресурс] – URL: https://ru.wikipedia.org/wiki/Maltego

10. Russianblogs / Использование Шодана, [Електронний ресурс] – URL: https://russianblogs.com/article/8055192375/

11. Crystal Blockchain / Crystal's blockchain visualization tool: Dig deeper into crypto asset data, [Електронний ресурс] – URL: https://crystalblockchain.com/articles/crystals-blockchain-visualization-tool-dig-deeper-into-crypto-asset-data-with-our-best-in-class-solution/

12. MDPI / Blockchain and Machine Learning: A Critical Review on Security, [Електронний ресурс] – URL: https://www.mdpi.com/2078-2489/14/5/295

13. Habr / Bitfury Crystal: как работает и где используется наш инструмент для отслеживания подозрительных крипто-транзакций, [Електронний ресурс] – URL: https://habr.com/ru/companies/bitfury/articles/434282/

14. Crystal User Guide / Application version: 3.1, [Електронний ресурс] – URL: https://www.avaloq.com/_Resources/Persistent/1/b/7/8/1b78949be1bc10968239efe2c0b93a9b7c33a8a2/avaloq-marketplace-crystal-blockchain-analytics-documents1.pdf

15. Avaloq / Crystal Blockchain Analytics Platform for Crypto AML/ KYT Compliance, [Електронний ресурс] – URL: https://www.avaloq.com/solutions/services/avaloq-one-ecosystem/crystal-blockchain-analytics-platform-for-crypto-aml-kyt-compliance

16. Crystal Blockchain / 5 steps to identify suspicious entities on blockchains, [Електронний ресурс] – URL: https://crystalblockchain.com/articles/5-steps-to-identifying-potentially-suspicious-entities-on-blockchains/

17. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ :

Київ. нац. торг.-екон. ун-т, 2020. – 101 с. –URL: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

18. Дослідження методів аналізу транзакцій криптовалют для перевірки їх законності, 88с / URL: https://openarchive.nure.ua/server/api/core/bitstreams/753725f7-386b-451d-a4f7-44b6f7ebe487/content

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Бакалаврська робота на тему:

«Дослідження шляхів та розробка рекомендацій, щодо розслідування кіберінцидентів в Blockchain у серидовищі Crystal»

Виконав: ЛЕЛЮХ Вадим
Олександрович
Керівник: ГАХОВ Сергій Олександрович,
к.військ.н.,доцент

АКТУАЛЬНІСТЬ

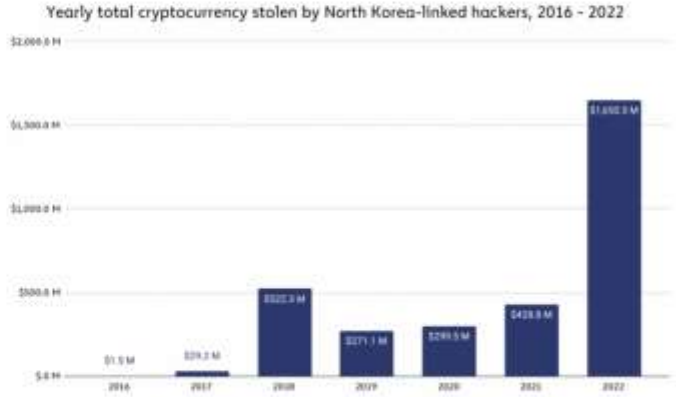
- На сьогоднішній день захист власних криптоактивів є надзвичайно важливою задачею, оскільки криптовалюти стають все більш популярними та використовуваними, а зловмисники активно спрямовують свої зусилля на кібератаки та крадіжки цифрових активів.
- Все більше і більше людей стикаються з проблемою викрадення їхніх віртуальних активів, але при цьому мало хто знає, що з цим можна заподіяти.

Crystal

Розслідування кіберінцидентів у Crystal

Зростаюча частота кіберінцидентів становить серйозну проблему, яка загрожує безпеці та конфіденційності нашого цифрового світу. Цей тривожний тренд відображає швидке розвиток кіберзлочинності та зростання потенційних загроз для організацій, користувачів та суспільства в цілому.

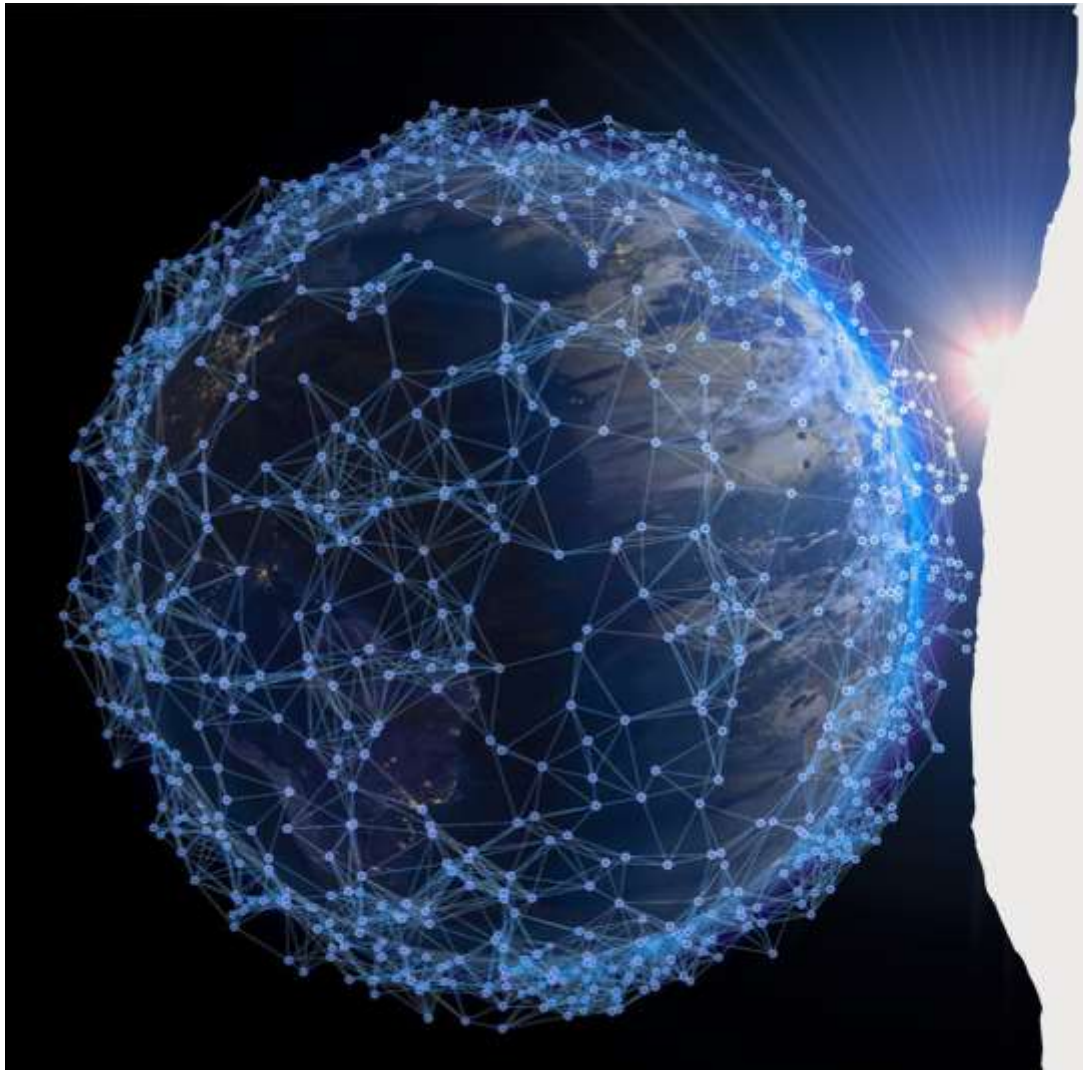
Крім того, широке використання технологій Інтернету речей (IoT), хмарних сервісів та мобільних пристроїв сприяє збільшенню поверхні атаки.



Неймовірна кількість доларів США викрадається у криптоактивах, і з кожним роком ця тенденція зростає.

Розробка рекомендацій – це один з кроків до поліпшення різних аспектів захисту

- Розробка рекомендацій дозволить ідентифікувати потенційні вразливості в блокчейні та пропонувати заходи для їх усунення. Це рекомендації щодо поліпшення механізмів аутентифікації, шифрування даних, контролю доступу та моніторингу мережі. Усе це сприятиме запобіганню атакам та зменшенню ризиків кіберінцидентів. Також рекомендації передбачають впровадження механізмів постійного моніторингу даних, які допоможуть вчасно реагувати на інциденти.



Цією дипломною роботою я хочу акцентувати увагу на необхідності покращення захисту криптовалюти.

- Blockchain, як розподілена технологія, має потенціал покращити кібербезпеку. Однак, для ефективного використання Blockchain у цілях розслідування кіберінцидентів, необхідно провести дослідження та розробити рекомендації щодо використання цієї технології.
- Моя дипломна робота може мати практичне значення, оскільки розроблені рекомендації можуть бути використані в реальних ситуаціях розслідування кіберінцидентів.
- Також інстумент Crystal є однією з провідних платформ для аналізу криптовалютних транзакцій і розслідування кіберінцидентів. Розробка рекомендацій щодо використання Crystal у розслідуванні кіберінцидентів в Blockchain може покращити ефективність роботи цієї платформи та сприяти точному та швидкому виявленню та аналізу потенційно небезпечної активності.

ВИКРАДЕННЯ КРИПТОАКТИВІВ ЗА 2021 РІК

Однієї із розроблених мною рекомендацій є Машинне навчання

- **Чому був вибраний цей напрямок?**

Тому що ML показує як потенційний спосіб покращити безпеку систем Блокчейну шляхом аналізу даних, розпізнавання шаблонів і виявлення потенційних загроз безпеці в режимі реального часу. ML можна використовувати для підтвердження особи користувача за допомогою біометричних даних. На мою думку цей напрямок буде ставати з роками все краще і краще.

Розглянемо основні етапи та особливості рекомендацій, які були розроблені

1 **ЗБІР ДАНИХ ПРО КІБЕРІНЦИДЕНТИ В БЛОКЧЕЙН**

2 **АНАЛІЗ ДАНИХ ЗА ДОПОМОГОЮ РІЗНИХ МЕТОДІВ І АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ**

3 **ВИЗНАЧИТИ РИЗИКИ ТА ОЦІНИТИ МОЖЛИВІ НАСЛІДКИ**

4 **ВІЗУАЛІЗАЦІЯ ДАНИХ**

5 СКЛАДАННЯ РЕКОМЕНДАЦІЙ НА ОСНОВІ ЗІБРАНИХ ДАНИХ

6 ЮРИДИЧНИЙ СУПРОВІД

Використовуючи Crystal для розробки рекомендацій ми використовуємо передові аналітичні методи та алгоритми, що дозволяють швидко та ефективно виявляти та боротись з кіберінцидентами

ДЯКУЮ ЗА УВАГУ!

Презентацію підготував студент групи БСД-41:
ЛЕЛЮХ Вадим Олександрович