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

До захисту допущено
В.о. завідувача кафедри

_____ **Микола ГРАЙВОРОНСЬКИЙ**
(підпис)

«_____»_____2021 р.

Дипломна робота

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

на тему: __Розробка структури блокчейн-сховища для індикаторів компрометації в розподіленій системі обміну загрозами_____

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи _ФБ-73____
(шифр групи)

Дем'яненко Дмитро Олексійович_____ _____
(прізвище, ім'я, по батькові) (підпис)

Керівник к.е.н., доц. Ткач Володимир Миколайович_____ _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

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

Київ - 2021 року

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

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

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Микола ГРАЙВОРОНСЬКИЙ
(підпис)
«___»_____2021 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Дем'яненку Дмитру Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Розробка структури блокчейн-сховища для індикаторів компрометації в розподіленій системі обміну загрозами»,

керівник роботи к.е.н., доц. Ткач Володимир Миколайович,

затверджені наказом по університету від « » _____ 2021 р. №

2. Термін подання здобувачем вищої освіти роботи 07 червня 2021 р.

3. Вихідні дані до роботи _____

_____

4. Зміст роботи:

Вступ

1 Теоретичне підґрунтя

2 Концетп та переваги системи

3 Розробка архітектури

Висновки

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо):

Презентація

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Огляд літератури, вивчення предметної області	01.10.20 – 31.01.21	Виконано
2	Формулювання теми дипломної роботи, визначення мети та постановка задач.	01.10.20 - 12.03.21	Виконано
3	Визначення структури дипломної роботи	01.02.21- 12.04.21	Виконано
4	Робота над першим розділом. Опис теоретичних відомостей	01.02.21 - 23.05.21	Виконано
5	Робота над другим розділом. Визначення актуальності та переваг системи	13.03.21 – 23.05.21	Виконано
6	Робота над третім розділом. Створення архітектури.	12.04.21 – 23.05.21	Виконано
7	Підготовка ілюстративного матеріалу. Оформлення роботи	02.06.21	Виконано

Здобувач вищої освіти _____ Дмитро ДЕМ’ЯНЕНКО
(підпис)

Керівник роботи _____ Володимир ТКАЧ
(підпис)

РЕФЕРАТ

Дипломна робота має обсяг 62 сторінки, складається з 3 розділів, містить 8 рисунків, 1 таблицю та 19 літературних посилань.

Завданням роботи є розробка архітектури розподіленої системи обміну IoC та створення порівняльних характеристик технологій для реалізації архітектурних елементів.

Мета цієї дипломної роботи полягає у створенні системи для ефективного зберігання та обміну індикаторами компрометації.

Об’єктом дослідження є архітектура розподіленої системи обміну індикаторами компрометації з блокчейн сховищем для IoC.

Предметом дослідження є можливість ефективного збереження та обміну чутливими даними, таким як IoC.

Актуальність роботи зумовлюється тим, що технологія блокчейн є стрімко розвиваючоюся та залучення її до міжгалузевих сфер життя є новітнім трендом.

Методами дослідження є аналіз інформаційних джерел та публікацій за темою дослідження. Синтез отриманих знань для розробки нової архітектури та моделі довіри до постачальників даних.

Наукова новизна зумовлюється тим, що зумовлюється тим, що для досягнення мети дипломної роботи потрібно створити абсолютно нову архітектурну модель, якої не існувало раніше.

Практичне застосування полягає в тому, що на основі розробленою архітектури можна реалізувати систему зберігання та обміну IoC на базі блокчейну.

Ключові слова: блокчейн, блокчейн платформа, IoC, індикатор компрометації, алгоритм консенсусу, розподілений реєстр, механізми довіри, CTI, TIP.

ABSTRACT

The work has a volume of 62 pages and consists of 3 sections, contains 8 figures, 1 table and 19 references.

The task of the work is to develop the architecture of a distributed IoC exchange system and create comparative characteristics of the technology for the implementation of architectural elements, such as databases or blockchains.

The purpose of this graduate work is to create a system for effective storage and exchange of indicators of compromise.

The object of research is the architecture of a distributed system of exchange of compromise indicators with blockchain storage for IoC.

The subject of the study is the ability to efficiently store and exchange sensitive data such as IoC.

The relevancy of the work is the fact that today blockchain technology is rapidly evolving and its involvement in intersectoral spheres of life is the latest trend.

The research methods are the analysis of information sources and publications on the research topic. Synthesis of acquired knowledge to develop a new architecture and model of trust in data providers.

The scientific novelty is the fact that to achieve the goal of the thesis needs to create a completely new architectural model, which did not exist before.

The practical application is that on the basis of the developed architecture it is possible to implement a system of storage and exchange of IoC on the basis of a blockchain.

Keywords: blockchain, blockchain platform, IoC, consensus algorithm, distributed ledger, CTI, TIP

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AB – Analyze information Block

AoI - Analyzer of Indicators

CTI - Cyber Threat Intelligence

Dapp - decentralized application

DCS - Decentralized Cloud Storage

DPoS - Delegated Proof of Stake

DoS - Denial of Service

IDS - Intrusion Detection System

IP - Internet Protocol

ISACs - Information Sharing and Analysis Centers

IoC - Indicator of Compromise

IoC Storage - Indicator of Compromise Storage

MISP - Malware Information Sharing Platform

NoSQL - not only SQL

OSINT - Open Source INTelligence

P2P - Peer to Peer

PBFT - Practical Byzantine Fault Tolerance

PoS - Proof of Stake

PoW – Proof of Work

SIEM - Security information and event management

SQL - Structured Query Language

THB – Trusted History Blockchain

TPS - Transactions Per Second

ВСТУП

Дослідження, проведене IBM, свідчить, що з 3000 C-level керівників, 33% організацій розглядають можливість взаємодії з технологією блокчейн[1]. Виходячи з цього, на сьогоднішній день технологія блокчейн користується великим попитом і все більше компаній бажають залучити її в свої застосунки та системи.

IT-спільнота стикається з інцидентами різного характеру та природи, щодня з'являються нові загрози. Боротися з цими інцидентами в галузі безпеки практично неможливо. Обмін інформацією про загрози серед IT-спільноти став ключовим елементом у реагуванні на інциденти, щоб виявляти та знешкоджувати атаки зловмисників. Отже, надійні інформаційні ресурси, що забезпечують інформацію, є надзвичайно важливими для IT-спільноти або, навіть, у більш широкому масштабі для Threat Intelligence спільнот або груп виявлення інтернет-шахрайства. Члени цих віртуальних спільнот, як правило, класифікуються як ті, що заслуговують на довіру та ті, що не заслуговують на довіру. Довіра та репутація стали необхідними властивостями для забезпечення безпеки, завдяки швидкому зростанню невизначеності та ризику. Цей ризик є результатом кібератак, здійснених ненадійними акторами. Зловмисна атака може впровадити оманливу інформацію, що робить спільноту ненадійною. Механізм довіри є важливим інструментом для забезпечення безпечного функціонування в межах спільноти. Більшість віртуальних спільнот є централізованими, що означає, що вони володіють, керують та контролюють інформацію без дозволу законного власника, тобто того хто цю інформацію безпосередньо надав.

Ця робота представляє систему зберігання та обміну індикаторами компрометації (IoC), та модель оцінки довіри до публічних та приватних організацій постачальників Threat Intelligence даних на основі технології

блокчейн. Модель довіри на основі блокчейну розроблена для вирішення проблеми визначення надійності інших CTI систем та приватних осіб та забезпечується завдяки прозорій простежуваності даних, які зберігаються у блокчейні та неможливості їх зміни чи видалення. Ефективність запропонованої системи, здебільшого, ґрунтується на технології блокчейн та на тім рівні безпеки, який надає ця технологія. Мета системи - допомогти у встановленні превентивних дій та контрзаходів, що застосовуються проти цілеспрямованих атак. Зробити виявлення загроз легшим за допомогою спільного обміну знаннями про наявні індикатори компрометації.

Мета цієї дипломної роботи полягає у створенні системи для ефективного зберігання та обміну індикаторами компрометації.

Об’єктом дослідження є архітектура розподіленої системи обміну індикаторами компрометації з блокчейн сховищем для IoC.

Предметом дослідження є можливість ефективного збереження та обміну чутливими даними, таким як IoC

Актуальність роботи зумовлюється тим, що на сьогодні технологія блокчейн є стрімко розвиваючоюся та залучення її до міжгалузевих сфер життя є новітнім трендом.

Методами дослідження є аналіз інформаційних джерел та публікацій за темою дослідження. Синтез отриманих знань для розробки нової архітектури та моделі довіри до постачальників даних.

Наукова новизна зумовлюється тим, що зумовлюється тим, що для досягнення мети дипломної роботи потрібно створити абсолютно нову архітектурну модель, якої не існувало раніше.

Публікації: дослідження було представлено у вигляді доповіді у збірнику наукових матеріалів LXVI міжнародної науково-практичної інтернет - конференції el-conf.com.ua «Інновації науки XXI століття» [2].

1 ТЕОРИТИЧНЕ ПІДҐРУНТЯ

1.1 Термін «блокчейн» та пов’язані з ним терміни

Блокчейн – це, розподілена децентралізована база даних (або ж публічна книга), яка містить записи різного характеру (транзакції або цифрові подій, які вже насали), копія якої зберігається на кожному вузлі системи. Вузол – це локальний комп’ютер кожного учасника блокченйну. Кожна транзакція в цій книзі верефікується та стає дійсною завдяки вирішенню проблеми консенсусу мережі. Існує досить багато алгоритмів досягнення консенсусу, найпопулярніші ми розглянемо пізніше. Після занесення до спільного реєстру інформація ніколи не може бути видалена або змінена, окрім випадку атаки 51% (коли в системі буде щонайменше 51% зловмисників, які будуть мати одну спільну мету – зламати систему), яка до цього моменту ще не була успішною через складність її реалізації. Блокчейн містить певний і верифікований запис кожної транзакції, коли-небудь здійсненої. А це означає, що будь якому учаснику системи у будь-який момент часу доступна історія всіх транзакцій і, гарантовано, що ці транзакції є справжніми та незмінними з моменту їх настання. Головною відмінністю технології блокчейн від централізованої бази даних є те, що в будь-якому блокчейні дозвелені тільки операції читання та запису, на відміну від баз даних, які підтримують операції читання, запису, оновлення та видалення інформації.

Далі, пропонується розглянути основні характеристики та нюанси блокчейн платформ. На базі цих характеристик в підрозділі 3.5 буде порівняно відомі блокчейн платформи та обрано найбільш підходящу для реалізації сховища IoC розподіленої системи обміну загрозами.

1.1.1 Покоління блокчейну

Першим критерієм відмінності існуючих платформ є покоління блокчейну. Базуючись на [3] можна розділити всі блокчейни на чотири покоління 1.0, 2.0, 3.0 та 4.0. Рисунок 1.1 ілюструє основні відмінності між блокчейнами різних поколінь.

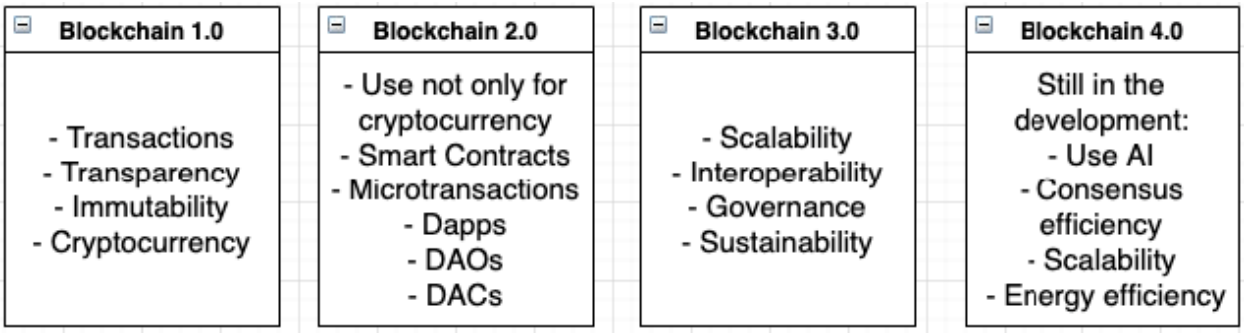

Рисунок 1.1 - Покоління блокчейнів за [1.1]

Як бачимо кожне покоління представлене набором характеристик, які мають блокчейни цього конкретного покоління. Слід сказати, що блокчейни покоління 1.0 використовуються виключно для обміну криптовалютами, блокчейни покоління 2.0 та 3.0 здебільшого використовуються у міжгалузевих сферах, тобто можуть бути використані для зберігання даних різного походження. На відміну від перших трьох, блокчейна четвертого покоління ще не існує, однак ведуться активні роботи над його створенням.

1.1.2 Алгоритм консенсусу

Консенсус - це надійний, стійкий до несправностей механізм, що використовується для досягнення згоди щодо стану мережі блокчейнів. Він потрібен для забезпечення впевненості користувачів мережі, що вони мають

однакові ланцюги блоків даних на своїх локальних комп'ютерах. Протокол передбачає перевірку та автентифікацію кожної транзакції, яка стає частиною нового блоку. Простими словами, консенсус гарантує, що дані, які стануть частиною сховища, є дійсними та справжніми, а також що інші учасники підтвердили їх достовірність[4]. На сьогодні існує дуже багато алгоритмів консенсусу, але найбільш відомими є наступні алгоритми:

PoW (Proof-of-Work) - обчислювальний алгоритм, який гарантує, що майнери (див. підрозділ 1.1.3) можуть перевірити новий блок транзакцій лише в тому випадку, якщо інші участники мережі спільно погоджуються, що хеш блоку, наданий майнером як доказ його роботи, є рішенням односторонньої функції по валідації блоку.

PoS (Proof-of-Stake) - альтернатива PoW, яка не є обчислювальною, тобто не вимагає величезних трат природних ресурсів. На відміну від PoW, PoS вибирає вузол, який може додати блок за рахунок кількості монет на рахунку. Кількість блоків, які може валідувати один вузол прямо пропорційна статку цього вузла. Використовуючи даний алгоритм в блкочейні валідатори, які діятимуть зловмисно, втратять частину своїх монет.

Існують також і інші алгоритми консенсусу так як DPos, HPos, PoA, PoB та інші.

1.1.3 Майнінг блоків

У технології Blockchain процес додавання деталей транзакцій до розподіленого реєстру називається майнінгом (з англ mining). Хоча цей термін асоціюється з біткойнами, насправді він також використовується у всіх системах, побудованих на технології blockchain. Майнінг передбачає знаходження хешу блоку, який потрібен для того щоб валідувати блок та всі транзакції, які до нього

входять, забезпечуючи тим самим безпеку всього блокчейну. Щоб стимулювати майнерів, винагорода видається майнеру, який першим знаходить хеш блоку в циклі генерації блоку, але в залежності від алгоритму консенсусу процес майнінгу може сильно відрізнятись. Наприклад для алгоритму PoS учасники мережі одночасно є майнерами блоків. Кількість блоків, які може підписати кожен учасник пропорційна частці монет на його блокчейн рахунку (в разі використання блокчейна, як платформи для обміну криптовалютою).

1.1.4 Тип блокчейну

Мережі блокчейнів можна класифікувати на основі їх моделі дозволу, яка визначає, хто може користуватись мережею. Якщо будь-хто може опублікувати новий блок – це публічна мережа. Якщо лише окремі користувачі можуть публікувати блоки – це приватна мережа. Приватні мережі блокчейнів часто розгортаються для групи організацій та приватних осіб [5].

Публічні блокчейни повністю відкриті для громадськості та доступні кожному, тому будь-хто, маючи підключення до Інтернету, може робити внески та взаємодіяти з даним блокчейном. Таким чином, будь-яка людина або організація може завантажити програмне забезпечення загальнодоступного блокчейну та запустити власний вузол, дозволяючи ПЗ перевіряти його інформацію та додавати нові транзакції до блокчейну.

Завдяки відкритості для будь-якого внеску, популярні публічні блокчейни, такі як Bitcoin або Ethereum, складаються з тисяч вузлів, які сприяють підтримці цих блокчейнів. Це утворює глобальну та децентралізовану мережу незалежних вузлів, в якій кожен вузол взаємодіє та перевіряє роботу інших вузлів, на відміну від централізованих систем, де єдина особа або установа повністю контролює всю систему.

Стати нодою (англ. node, вузол) у приватному блокчейні (наприклад, Hyperledger та / або R3 Corda) можливо лише для корситувачів, яким заздалегідь був наданий доступ. Обмеження доступу до приватного блокчейну можна досягти за допомогою різних методів, таких як аутентифікація або експлуатація блокчейну в ізольованій мережі.

Незважаючи на те, що термінологія у галузі блокчейнів все ще розвивається і не є уніфікованою та узгодженою, приватні блокчейни також прийнято називати «дозволені блокчейни» (англ. permissioned), тоді як публічні блокчейни часто називають «блокчейнами без дозволу» (англ. permissionless). «Дозволеними» блокчейнами керують заздалегіть обрані особи. Це означає, що учасники приватних блокчейнів відомі, а тому можна з легкістю перевірити, чи діють ці учасники добросовісно. Оскільки всі учасники відомі, за неналежну поведінку, таку як підроблення транзакції, може бути покарано (наприклад, покарання може бути у формі попередньо визначеного та узгодженого штрафу).

Оскільки будь-хто може приєднатися до «блокчейну без дозволу», його учасники завжди є анонімними (це одна з переваг публічного блокчейну) та їх стимулом є шанс заробити локальну валюту цього блокчейна, як нагороду за майнінг блоків. У блокчейнах, що базуються на Proof-of-Stake, таких як Tezos чи Ethereum, учасники також можуть втратити частину своїх монет, якщо вони не дотримуються правил протоколу і їх звинувачує інший учасник блокчейну, який називається «обвинувачем». Обвинувач заробляє цю частку за виконану перевірочну роботу. Кожен блокчейн, приватний чи загальнодоступний, потребує системи контролю, щоб забезпечити правильну поведінку учасників відповідно до протоколу та правил блокчейну.

1.1.5 Час на створення блоку

У блокчейні транзакції транслюються негайно, але їм не довіряють, доки вони не стануть частиною блоку. Наприклад, надіславши транзакцію одразу після створення попереднього блоку доведеться чекати до створення наступного блоку, для того щоб цю транзакцію побачили інші користувачі (як приклад, у найвідомішому блокчейні Bitcoin генерація нового блоку триває від 10 до 60 хвилин). Саме з цієї причини важливий низький час додавання блоків до реєстру. Але цей критерій є важливим не у всіх системах на базі блокчейну. Якщо це не банківська сфера, та не обмін криптовалютою, а наприклад блокчейн – як сховище не критичних даних або історії взаємодії системи і користувачів, то затримка у 10 хвилин не буде критичною.

1.1.6 TPS

Цей показник тісно пов’язаний з попереднім, бо TPS - це теоретичне число, яке показує кількість транзакцій, яку мережа здатна обробляти кожну секунду і розраховується як відношення кількості транзакцій у блоці до часу блоку. TPS – це гарний показник пропускної здатності мережі. Як і у випадку з часом на генерацію блоків, важливо розуміти, що більше – не завжди значить краще. Буває безліч ситуацій, коли кількість транзакцій у блоці не буде великою, а тому і показник TPS може бути малим. Прикладом подібної системи якраз є сховище індикаторів компрометації про що буде детальніше розказано у розділі 3.

1.1.7 Смарт контракти

Smart Contract - це програма, що самостійно виконується, яка зберігається у блокчейні, і може бути виконана розподіленим та децентралізованим способом.

Зазвичай смарт контракти використовуються як форма угоди між постачальником та споживачем . Смарт контракти відповідають за перевірку, активацію або примусове виконання дій у системах блокчейну. Існують дві широко використовувані мови програмування для написання розумних контрактів Ethereum - Solidity та Serpent. Solidity - це мова програмування високого рівня, яка використовується для реалізації інтелектуальних контрактів на платформі блокчейну Ethereum. Вона дозволяє розробникам блокчейнів перевіряти програму під час виконання, а не під час компіляції.

Традиційно, коли дві сторони укладають договір, вони використовують послуги довіреної третьої сторони для виконання угоди. Так робили впродовж століть. Однак впровадження розумних контрактів та пов'язаних з ними технологій автоматизує цей процес. Розглянемо деякі ключові переваги смарт-контрактів перед традиційними контрактами:

- Уникнення посередників;
- Автоматизація та економія часу;
- Безпека;
- Точність та прозорість;
- Ціна;

Як бачимо, смарт-контракти – це дуже потужна технологія, яка має багато переваг і надає змогу чітко та надійно врегулювати відносини між учасниками мережі блокчейн.

1.1.8 dApp

Децентралізований додаток (англ. dApp) - це розподілене ПЗ з відкритим кодом, яке працює в мережі P2P і підтримується розподіленим реєстром

блокчейну. Дані програми та записи про роботу зашифровані, і для доступу до програми потрібен криптографічний маркер. Головною перевагою dApps є те, що вони завжди доступні і не мають жодної точки відмови .

dApps в чомусь схожі на звичайні програми та використовують ту саму технологію для відтворення веб-сторінки. Однак важливою відмінністю є те, що звичайний застосунок працює з централізованою базою даних, dApp працює з смарт-контрактами, які належать блокчейну. Оскільки смарт контракт по своїй суті просто програмний код і часто є лише невеликою частиною всього dApp, створення децентралізованого додатка на базі смарт контрактів потребує поєднання цих самих смарт контрактів з сторонніми система для реалізації інтерфейсу системи.

В даний час найпопулярнішою платформою для розробників dApp є Ethereum, але інші платформи блокчейну, такі як Cardano, Lisk, QTUM та NEO, також використовуються для розробки dApp.

1.1.9 Decentralized Cloud Storage

DCS або Decentralized Cloud Storage – це децентралізоване хмарне зберігання даних. Взагалі кажучи, запис великих файлів безпосередньо в блокчейн - погана практика. Ми використовуємо Google Drive, Dropbox та інші інструменти щодня, але існують дійсні випадки використання розподіленого зберігання даних. DCS працює майже так само, як мережі P2P та Bittorent, де файли, або їх частини, передаються клієнтам, які потім їх надсилають по запиту. За такої організації розподіленого зберігання файлів мають місце наступні твердження:

- Жоден центральний орган не може видаляти або змінювати ваші дані;

- Дані розподіляються між кількома незалежними вузлами мережі;
- Можна завантажувати фрагменти файлів з декількох вузлів;
- Децентралізоване сховище зберігає історію версій кожного файлу;
- Завдяки DCS зменшеншується навантаження на мережу та втрата даних.

1.2 Порівняння алгоритмів консенсусу

Децентралізація включає системи, які потребують моделей управління або механізмів консенсусу (див. підрозділ 1.1.2). Існує ряд таких моделей управління, кожна з яких має переваги та недоліки, а деякі є більш практичними, ніж інші. Ці моделі управління є одним з найважливіших факторів платформи, бо вони регулюють затримку та пропускну здатність мережі.

В залежності від потреб системи той чи інший механізм консенсусу буде кращим, чи гіршим. У цьому підрозділі пропонується розглянути відмінності найбільш популярних у блокчейнах алгоритмів консенсусу PoW, PoS та DPoS.

1.2.1 Доказ роботи (PoW)

Концепція алгоритму доказу праці була представлена в 1993 році, а сам термін «Доказ роботи» був введений в 1999 році Маркусом Якобссоном та Арі Джуелс. Основною причиною застосування моделі PoW є стримування DoS атак (відмови в обслуговуванні), вимагаючи від запитувачів певної послуги виконання роботи, а у випадку блокчейну - обчислювальної роботи перед додаванням блоку до ланцюга.

Багато платформ використали цей консенсус таким чином, що для видобутку певної цифрової валюти їм доводиться витрачати величезну кількість

обчислювальної енергії. Майнерам доводиться вирішувати важкі односторонні функції, а саме знаходження потрібного хешу, які потребують багато енергії. Майнер, який першим знайшов потрібний хеш, отримує винагороди у вигляді цифрової валюти цієї платформи. Класичний приклад використання PoW це Bitcoin.

Доказ роботи також вирішує проблему подвійних витрат у криптовалютах. Світ намагається споживаючи менше енергії та придумує все більше способів видобутку енергії. Обчислювальна потужність, необхідна для майнінгу, що відбуваються у всьому світі - величезна. У цьому полягає значна проблема з PoW.

Іншим недоліком роботи алгоритму є його затримка та пропускна здатність мережі. Із-за складності знаходження рішення, пропускна здатністьє дуже маленькою (в Bitcoin це приблизно 7 TPS), що є недостатнім порівняно з попитом на цю мережу. Це підводить нас до альтернативної моделі управління, яку використовували багато розробників блокчейн платформа, механізму консенсусу Proof of Stake.

1.2.1 Proof of Stake

Підтвердження частки є більш логічним варіантом для тих, хто хоче уникнути недоліків PoW. Різниця між цими двома методами консенсусу полягає в тому, що PoS вимагає від майнера володіння та утримання цифрової валюти. Кількість криптовалюти певної платформи, що належить одному майнеру, є показником частки, яку майнер має для цієї конкретної платформи.

Працює механізм консенсусу PoS на двох факторах. Перший фактор полягає у встановленні високих вимог для проведення атаки на мережу. Для ініціювання атаки потрібно 51 відсоток усіх криптовалют у цій мережі. Одному джерелу важко мати такий величезний відсоток всіх грошей системи.

Другий фактор – низький стимул для проведення атаки. Навіть, якщо комусь вдасться зібрати 51% всіх активів мережі, то у разі нападу і компрометації системи зловмисник втратить свої гроші. Цей механізм стримує зловмисників, тому що втрата у разі успішної атаки для зловмисника буде значно більшою ніж те, що він отримує

Більше користувачів блокчейну зараз більш схильні до PoS алгоритму, оскільки він надає «перевагу більшості» порівняно з PoW. Чудовим прикладом того, чому перевагу надають PoS, є біткойн. Зараз біткойн використовує PoW, через це майнерам доводиться шукати встановлювати потужне обладнання, яке є дуже дорогим та більш того потребляє велику кількість ресурсів. Порівнюючи це платформами, які працюють за алгоритмом PoS, то їх майнерам потрібне лише володіння деякою часткою цифрової валюти мережі та підключення до Інтернету.

«Доказ частки» сам по собі не є досконалим. Він має певні недоліки, які можна легко використати. Від власників великих відсотків криптовалют залежить напрямок розвитку криптовалюти та платформи. Атака на мережу також впливає на модель управління PoS більше, ніж на PoW. При злому системи майнер втрачає не лише свою криптовалюту, він також втрачає свою репутацію і статус у платформі. На відміну від PoW, де майнери втрачають лише свою криптовалюту. Ці недоліки призвели до розробки Делегованого підтвердження ставки (DPoS).

1.2.3 Delegated Proof of Stake (DPoS)

Делеговане підтвердження частки (DPoS) надає вирішення проблем, з якими стикаються як PoW, так і PoS. Його функції подібні до функцій PoS, але він відрізняється тим, що має більш демократичні особливості порівняно з PoS. В даний час більшість нових платформ обирають саме цю модель управління, оскільки вона забезпечує більш цілісний підхід

У DPoS вводяться делеговані свідки. Ці свідки мають право голосувати від імені тих, хто їх обрав. Свідок функціонує подібно до майнерів на платформах, що використовують PoS. У DPoS свідок, який не виконує свої обов'язки або не представляє думки своїх виборців, могли може бути з легкістю замінений на іншого.

Частка активів в платформі в DPoS подібна до PoS, оскільки зацікавлені сторони мають вплив, пропорційний кількості криптовалют, якими вони володіють. У DPoS поріг для того щоб стати майнером знижений до рівня активів більшості користувачів системи, на відміну від PoS. Таким чином, делеговане підтвердження частки вводить демократію в мережу. Ті, кто були обрані свідками, диктують напрямок розвитку та роботи платформи

Вдале використання алгоритму DPoS спостерігається на таких платформах, як LISK або EOS, які стала відомими у всьому світі. Алгоритм також допомагає підтримати децентралізацію на платформах, в яких він використовується. Крім того, DPoS позбавлений недоліків як PoW, так і PoS, при цьому зберігаючи їх переваги. Це призвело до створення більш надійних платформ (EOS, LISK) з чудовою продуктивністю.

1.3 Принцип роботи технології «блокчейн»

Базуючись на інформації представленій в підрозділах 1.1 та 1.2 розглянемо як працює технологія блокчейн, а саме яким чином транзакції додаються до розподіленого реєстру та стають дійсними. Даний процес зображено на рисунку 1.2.

Рисунок 1.2 – Додавання транзакції до блокчейну

Процес додавання транзакцію до спільного ланцюга блоків можна описати в п’ять етапів:

1) Вузол починає транзакцію, спочатку створюючи, а потім підписуючи її своїм приватним ключем (створеним за допомогою криптографічних механізмів). Транзакція може представляти будь-яку дію в блокчейні. Для фінансових систем це може бути передавання криптовалюти, для нашою системи це буде запис індикатора компрометації у блокчейн. Структура даних транзакції, як правило, містить деякі допоміжні дані, наприклад при переведенні коштів це адреси відправника та отримувача, а при збереженні IoC – це ідентифікатор постачальника даних.
2) Транзакція розповсюджується до інших користувачів, які перевіряють транзакцію на основі заданих критеріїв. Зазвичай для перевірки транзакції потрібно більше одного вузла.

3) Після перевірки транзакції вона включається в блок, який потім розповсюджується по мережі. На даному етапі транзакція вважається підтвердженою.
4) Щойно створений блок стає частиною реєстру, він криптографічно зв'язується з хешем попереднього блоку, а так як попередній блок також зв’язаний з попереднім до нього, то буде вірним сказати що новий блок криптографічно пов’язується з усіма попередніми блоками. На цьому етапі транзакція отримує друге підтвердження, а блок - перше підтвердження.
5) Потім транзакції підтверджуються кожного разу, коли створюється новий блок. Зазвичай для розгляду остаточної транзакції потрібно шість підтверджень у мережі.

Загалом, технологія блокчейн може революціонізувати кілька галузей, від банківської сфери до розподілу енергії. Його основна сила полягає в децентралізованому зберіганні інформації та забезпеченні надійного механізму довіри. Використання блокчейну означає, що кожна людина має достовірну, публічну інформацію про те, що будь-яка конкретна компанія чи особа вже зробила. Іншими словами, блокчейн забезпечує довіру завдяки прозорості історії взаємодії з системою.

1.4 Індикатори компрометації

Оскільки цифрові технології продовжують активно розвиватися майже в кожному бізнесі сьогодні, аналіз TI (Threat Intelligence) даних привертає велику увагу, допомагаючи компаніям приймати обґрунтовані рішення щодо своєї мережевої безпеки. Аналітики TI покладаються на точні дані, які називаються IoC

(Indicators of Compromise), щоб ефективно виконувати свої ролі та обов'язки в системі безпеки.

Threat Intelligence є вигідною інвестицією для забезпечення безпеки системи або компанії, оскільки TI дозволяє ідентифікувати та зупиняти атаки. Основна мета TI - надати вичерпний огляд кіберзагроз, які можуть стати великим ризиком для витоку або компрометації чутливих даних та допомогти захистити систему. IoC – є результатом аналізу TI даних.

Індикатор компроментації (Indicator of Compromise) в комп'ютерній криміналістиці - це артефакт, який спостерігається в мережі або в операційній системі, що з високою ймовірністю свідчить про вторгнення до комп'ютера[6].

Відстежуючи IoC, експрети з безпеки організації можуть виявляти кібератаки та швидко протидіяти їм, щоб запобігти порушенням безпеки, зменшити збитки до мінімуму та вдало впроваджувати нові політики безпеки.

Індикатори компрометації виступають як червоні прапори, які можуть допомогти експерту з безпеки вчасно виявити підозрілу активність. Вони можуть вказувати на потенційних зловмисників, які намагаються атакувати систему, або виявляти незавершені атаки, які можуть призвести до порушення даних, вбо ж виявляти програми-вимогачі та інші види шкідливого ПЗ.

Стає зрозуміло, що IoC – це дуже важливі дані, які використовуються для виявлення, протидії та знешкодження кібернетичних атак. Пропонується розгялнути приклади IoCs для кращого розуміння того, що з себе представляють типові IoC:

1) Незвичайний вихідний мережевий трафік: системним адміністраторам та професіоналам мережевої безпеки не важко виявити великі обсяги незвичного вихідного трафіку. Це може бути шпигунське програмне забезпечення, що спілкується зі своїми командно-адміністративними

серверами, або атака на викрадення конфіденційних даних. Індикатори вихідного трафіку та ПЗ для виявлення вторгнень у мережу можуть видавати попередження у разі виявлення незвичного рівня трафіку.

2) Географічні порушення: незвичайний трафік не повинен бути обмежений обсягом використовуваної смуги пропускання або регіоном, з якого походить трафік.
3) Аномалії в діяльності привілейованих облікових записів користувачів: атаки на ескалацію привілеїв, а також соціальною інженерія, така як фішинг, можуть призвести до того, що зловмисні актори отримують несанкціонований доступ до привілейованих облікових записів користувачів. Для організацій, які не використовують вдосконалену стратегію захисту з контролем доступу, який дотримується принципу найменших привілеїв, будь-яка компрометація облікового запису може призвести до доступу до приватних облікових записів користувачів.
4) Кількість спроб входу в акаунт: системні адміністратори можуть виявити, що в обліковому записі привілейованого користувача було кілька невдалих спроб входу, можливо, що вказує на атаку bruteforce.
5) Розміри відповідей HTML: SQL ін’єкції, що використовуються для вилучення конфіденційних даних із веб-програми, зазвичай мають більший розмір відповіді HTML, ніж звичайні запити.
6) Загальна кількість запитів на один і той самий файл: може знадобитися багато спроб і помилок, щоб знайти вектор атаки або вразливість, яка працює, можливим показником такого сценарія є користувач, який робить кілька запитів до одного й того ж файлу.
7) Невідповідний трафік з конкретних портів: зловмисники часто користуються перевагами не широковживаних портів, щоб обійти фільтри.

8) Підозрілі зміни реєстру або системних файлів: зловмисне програмне забезпечення часто вносить зміни до реєстру, саме тому створення базової лінії є важливою частиною боротьби із зараженням шкідливим програмним забезпеченням.
9) Аномалії запитів системи доменних імен: запити DNS і трафік до серверів управління часто дотримуються стандартного шаблону, який може слугувати хорошим показником підозрілої діяльності.
10) Веб-трафік з підозрілою поведінкою: слід дослідити веб-трафік, який не схожий на звичайну поведінку користувачів.
11) Викриті облікові дані: облікові дані для входу використовуються для запуску додаткових кібератак і можуть вказувати на те, що ваша організація була скомпрометована.
12) Ознаки атак DDoS з розподіленою відмовою в обслуговуванні: DDoS-атаки, що працюють від ботнетів, часто використовуються для відволікання від вторинних атак на конфіденційність або цілісність ваших систем.

Наведені вище приклади IoC це лише мала частка індикаторів, які можуть вказувати на компрометацію системи. Зрозуміло, що в залежності від об’єкту атаки індикатори компрометації будуть різними і в кожній сфері діяльності існує безліч вже відомих IoC та їх список постійно поповнюється.

Висновки до розділу 1

В першому розділі було розглянуте основне теоритичне підґрунтя, необхідне для розуміння побудови архітектури розподіленою системи обміну загрозами. На базі термінів, розглянутих у підрозділі 1.1, буде зроблено порівняльну характеристики блокчейн платформ, а проаналізувавши відмінність

алгоритмів консенсусу підрозділу 1.2 буде обрано блокчейн платформу з найбільш підходящим алгоритмом для запропонованої системи. Підрозділ 1.3 надає більш широке розуміння того, як блокчейн працює в цілому. А підрозділ 1.4 надає розуміння того, що таке індикатори компрометації, які вони бувають та чому вони є такими важливими у цифровому просторі.

2 КОНЦЕПТ ТА ПЕРЕВАГИ СИСТЕМИ

2.1 Платформа Threat Intelligence

Система CTI або TIP (Cyber Threat Intelligence, Threat Intelligence Platform) - це система виявлення та протидії загрозам, що базується на фактичних даних [7]. Кінцевою метою CTI є можливість превентивної реакції на кіберзагрози, такі як розширена стійка загроза (APT) та атаки нульового дня, а також створення образів та критеріїв для виявлення зловмисників та груп зловмисників. Система CTI збирає дані, пов'язані із загрозами, з різних каналів, аналізує та передає інформацію іншим системам. Система CTI аналізує мережеві журнали, системні журнали, журнали брандмауера, трафік, інформацію про репутацію мережевих ресурсів та інформацію, зібрану SIEM системами. Система CTI виокремлює таку інформацію, як моделі атак, IoC, ідентифікатори шкідливого ПЗ, моделі зловмисників та тактико-технічні процедури (TTP) з різних типів даних, і виражає їх як сутності для аналізу зв'язку між ними. Структурований вираз інформації про загрози (STIX) [8] є найбільш часто використовуваною мовою вираження даних CTI, а TAXII - протокол передачі даних для обміну даними у STIX форматі. Проаналізовані дані CTI виражаються мовою STIX, а потім обмінюються за допомогою протоколу TAXII [8]. Швидкий та ефективний обмін даними необхідний для активного нівелювання кіберзагроз. Якщо спостерігається поведінка зловмисника, система CTI генерує інформацію, пов’язану з кіберзагрозами, об’єднуючи зібрану та заздалегідь визначену інформацію. Ця інформація включає тип нападу і порядок дій зловмисника. Поширюючи цю інформацію з іншими вузлами, які беруть участь у системі CTI, інформація про кіберзагрозу швидко стає відомою всім вузлам. Кожен вузол встановлює та оновлює свою політику безпеки, використовуючи цю інформацію. Система CTI

також виконує профілювання зловмисників та груп зловмисників, щоб запобігти атакам нульового дня. Шляхом стереотипного моделювання поведінки зловмисників та шкідливих програм система може прогнозувати майбутні моделі атак та швидко встановлювати заходи протидії.

Із визначення та функціональних вимог до TIP стає зрозуміло, що розробка розподіленої системи, яка буде зберігати та обмінюватися IoC з іншими системи, також є Threat Intelligence Platform.

2.2 Платформа обміну зловмисною інформацією

Платформа обміну зловмисною інформацією або MISP (англ. Malware Information Sharing Platform) - це безкоштовне програмне забезпечення з відкритим вихідним кодом, яке допомагає обмінюватися інформацією про загрози, включаючи індикатори кібербезпеки [9].

MISP використовують для збору, обміну, зберігання та співвіднесення індикаторів компрометації (IoC) цілеспрямованих атак, розвідувальних даних про загрози, інформації про фінансові шахрайства, інформації про вразливість чи навіть інформацію про боротьбу з тероризмом [9].

MISP - це платформа розвідки загроз, що використовується понад 6000 організаціями по всьому світу та служить платформою для обміну загрозами, спільнота, якої автоматично надсилає на платформу IoC, зібрані за дпомогою IDS (Система виявлення вторгнень) або SIEM систем приватних організацій[10].

Стає зрозуміло, що MISP є платформою Threat Intelligence (TPI), а тому є прямим конкурентом та аналогом до запропонованою системи на базі блокчейну. В підрозділі 2.3, буде розглянуто які переваги запропонована система має у порівнянні з успішною та широковживаною TIP MISP.

2.3 Переваги системи на основі блокчейну

Як буде розглянуто у розділі 3 запропонована система буде використовуватись не тільки для зберігання та обміну IoC, а також для визначення рівня репутації постачальників даних, яким можуть бути великі організації такі, як OSINT, SIEM та інші TIP та індивідуальні користувачі. Інформація про довіру до конкретних фідів є цінною для системи, тому що на базі репутації можна фільтрувати трафік або надавати більше привілеїв постачальникам даних з високим рівнем довіри і для користувачів даної системи, тому що, отримавши список репутації всіх вендорів даних, можна налаштувати політики безпеки в своїх організаціях для того, щоб уникнути взаємодії з ненадійними організаціями. Так як інформація про коефіцієнти довіри буде зберігатись у Trusted History Blockchain, то користувачі зможуть бути впевненими в цілісності та достовірності цих даних, завдяки тому, що історія зміни репутації до конкретних організацій буде повністю прозорою для користувачів системи. Це досягається завдяки децентралізації даних та неможливості змінювати та видаляти транзакції, які було додано до блокчейну.

Як бачимо, першою вагомою перевагою запропонованої системи над MISPом є оцінка довіри до всіх постачальників даних. Важливо сказати, що в нашій країні поки що не існує систем з подібним функціоналом, хоча просто системи обміну загрозами існують.

Інші переваги системи досягаються за допомогою методів оцінки та зберігання інформації у блокчейні. За допомогою основних переваг блокчейну таких, як децентралізація даних, цілісність даних та прозора історія роботи з реєстром, досягається надійність зберігання інформації та неможливість бути скомпрометованою з моменту, коли вона була додана до спільного реєстру. Крім

того, оцінка дійсності даних та учасників системи може здійснюватися за допомогою смарт-контрактів блокчейну, а результати можуть прозоро розповсюджуватися серед інших учасників за допомогою тих же смарт-контрактів. Завдяки методам оцінки вхідних даних (див. розділ 3) можна гарантувати, що вилучені з сирих даних IoC є надійними та вірними.

Отож, переваги запропонованої моделі можна сформулювати наступним чином:

(1) Навіть якщо надійний канал даних надсилає неправильну інформацію, система може запобігти обробку та зберігання невірної інформації, оскільки до вилучення IoC, з первинного джерела даних, першим чином система перевіряє дійсність отриманої інформації.

(2) Система може ефективно обробляти великі обсяги інформації та забезпечити безпечне середовище для зберігання синтезованої інформації.

(3) Система управляє розподіленим реєстром на основі технології блокчейн, яка в свою чергу гарантує цілісність та достовірність інформації про IoC, які потрапили в розподілений реєстр, та винагороду постачальника відповідно до його внеску.

(4) За допомогою надійності технології блокчейн проводиться оцінка довіри до всіх постачальників даних, на базі якої можна обмежити спілкування з ненадійними постачальниками. Ця інформація також може бути надана всім користувачам системи.

Висновки до розділу 2

В другому розділі було розглянуто такі поняття, як TIP та її існуюча реалізація MISP та надано переваги запропонованої системи зберігання індикаторів компрометації у блокчейні.

3 РОЗРОБКА АРХІТЕКТУРИ

В цьому розділі буде запропоновано архітектуру розподіленої системи з блокчейн сховищем для індикаторів компрометації. Архітектура системи – це опис елементів цієї системи і обґрунтування вибору інструментів та технологій для реалізації цих елементів, а також опис взаємодії цих елементів. Буде розглянуто архітектурний концепт, описано кожен елемент архітектури та проведено порівняльні характеристики, в контексті даної теми, технологій для реалізації цих елементів. Також буде розглянута покрокова взаємодія елементів системи.

3.1 Архітектурний концепт системи

Архітектурний концепт системи – це схематичне пов’язання компонентів системи та демонстрація зв’язків між ними. Архітектурний концепт системи зображено на рис. 3.1. У цьому розділі буде поверхово розглянуто кожен рівень архітектури системи, зображеної на рис 3.1. Для кращого розуміння рисунку основні архітектурні рівні системи позначені різними кольорами. Синій колір – це рівень постачальників даних, помаранчевий – рівень блоку аналітики та зеленим кольором позначені основні сховища даних: база даних для зберігання вхідної інформації, довірене сховище історії комунікацій та репутації вендорів системи та блокчейн сховище індикаторів компрометації.

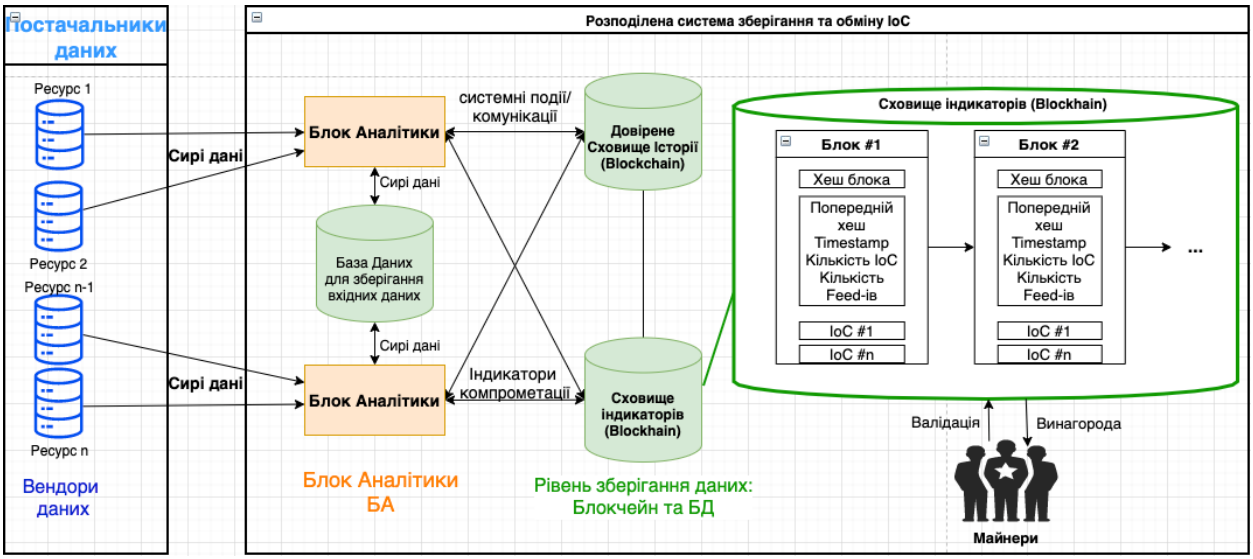

Рисунок 3.1 - Архітектурний концепт системи.

Запропонована система використовується для виокремлення, зберігання та обміну IoC на основі блокчейн сховища. Система розподіляється на три основні рівні, як зображено на рисунку 3.1:

- Фіди (feeds) – тобто постачальники даних;
- Блок аналітики (AB, Analyze data&information Block);
- Сховища даних у вигляді централізованої БД та двох блокчейнів: (1) Довірене Сховище Історії (THB, Trusted History Blockchain) та (2) Сховище Індикаторів компрометації (IoC Storage);

Рівень постачальників даних (feeds) - це рівень, представлений різноманітними організаціями та приватними користувачами, які незалежно збирають, валідують, оцінюють дані у межах своїх систем (це можуть бути інші CTI, SIEM, IDS, OSINT або ж звичайні користувачі мережі Інтернет тощо). Після внутрішніх циклів обробки даних (якщо вони є, пакети можуть бути вислані в систему і без цього кроку) вони надсилають сирі дані, тобто пакети, в яких потенційно зберігається інформація про загрози, до нашої системи. Для

заохочення сторонніх організацій надсилати дані до нашої системи пропонується винагороджувати фідів у разі надання корисних даних. Кожен постачальник має власний коефіцієнт довіри, яке залежить від кількості та якості даних надісланих до системи.

Блок аналітики (Analyze info Block, AB) – основний модуль системи, який повинен відповідати чітким функціональним вимогам (див. підрозділ 3.4). Блок аналітики відповідає за перевірку на валідність та унікальність вхідних даних, а також виокремлює IoC та додає їх до блокчейну. До того ж AB відповідає за збереження історії спілкування між системою та зовнішніми акторами. AB є центральним елементом архітектури, який реалізує складну логіку та пов’язує зовнішніх користувачів з системою.

Рівень сховищ даних (Blockchains/DB) – складаєть з трьох основних сховищ даних різного характеру. Перше сховище - централізована база даних, в якій зберігаються першоджерела даних, які поступають у систему від фідів. Інші два сховища – це децентралізовані сховища, тобто блокчейни, для зберігання індикаторів компрометації та історії взаємодії системи з фідами та користувачами.

Майнери блоків блокчейнів - використовуючи механізм консенсусу обраного блокчейну, майнери валідують блоки, які містять IoC, транзакції надсилання та запиту даних, репутацію конкретних фідів, та транзакції переказу коштів за внески корисних даних у систему від фідів та запити даних від користувачів. У рамках системи криптовалюта, видобута майнерами, може використовуватись для переведення у грошовий еквівалент та для здійснення операцій всередені системи, а тому майнери можуть також бути внутрішніми користувачами системи. Користувачі витрачають криптовалюту для отримання

інформації від CTI. Кожна вартість за запитом даних та винагорода за внесок даних має різну суму залежно від важливості даних та репутації вендора.

3.2 Обґрунтування багаторівневої архітектури

Згідно рисунку 3.1 дана архітектура є багаторівневою, бо має наступні рівні:

- Блок аналітики, який сам по собі є багатокомпонентною структурою (див. підрозділ 3.3);
- Централізована БД для зберігання сирої інформації, яка надходить до системи;
- THB (Довірене Сховище Історії) для зберігання репутації вендорів даних та транзакцій, які відбуваються в системі;
- IoC Storage (Сховище Індикаторів Компрометації) для зберігання індикаторів компрометації та інформації щодо вендора, який надав дані, з яких був отриманий даний IoC;

Розглянемо необхідність та користь, яку надають ці чотири елементи.

1) AB (блок аналітики) є обов'язковим та головним структурним елементом системи, без якого всі інші елементи не мали б сенсу, бо він відповідає за обробку даних та взаємодію всіх інших компонентів системи. Тому, не може виникнути сумнівів, що AB є необхідним компонентом даної системи.

2) Централізована база даних. Механізм роботи блоку аналітики такий, що з первинної інформації, надісланої фідом, виокремлюється IoC та зберігається в блокчейн. Але що буде, якщо в системі виникне колізія чи невірно сформується або нормалізується індикатор компрометації і це буде виявлено вже після додавання в блокчейн?

В такому випадку доведеться провести розслідування чому саме виникла критична ситуація і тут у нагоді стануть першоджерела даних, які дадуть повне розуміння того на якому етапі була допущена помилка. Завдяки цьому розслідуванню можна бути покращити та оптимізувати роботу одного з компонентів блоку аналітики, результат дії якого привів до такої ситуації. Також можуть виникнути ситуації коли через невірно визначені IoC результат зміни довіри до фіда був хибним, і однаково важливим є чи ця зміна була в позитивну чи в негативну сторону. В цьому випадку також необхідно буде звернутись до першоджерел та з'ясувати причини та адекватність тієї чи іншої поведінки системи.

З вищенаведених аргументів стає зрозуміло, що сирі дані зберігати потрібно, але неможна зберігати ці дані децентралізовано, тобто у блокчейні. По перше, блокчейни мають обмеження на максимальний розмір блоків, а первинної інформації до системи буде надходити значно більше ніж виявлятися індикаторів компрометації. По друге, це не є ефективним, тому що кожен вузол децентралізованої системи повинен буде зберігати всю інформацію, яка знаходиться в блокчейні, а надмірність і дуже велика кількість інформації буде використовувати більшу кількість ресурсів локальних систем користувачів, тому такий підхід не є бажаним для нашої системи.

Відповідно, ми повинні зберігати першоджерела даних в централізованій БД (в підрозділі 3.4 з'ясовується яка сама БД підходить для задач нашої системи), з яких блок аналітики буде ідентифікувати ІК і потім їх вже записувати в надійну децентралізовану систему.

3) THB та IoC Storage є блокчейнами, тому що за допомогою даної технології досягається цілісність даних, прозора історія додавання даних до блоку (так як блокчейн дозволяє тільки операції читання та запису і не дозволяє операції оновлення даних та їх видалення) та розподілене зберігання даних серед

внутрішніх користувачів системи. В випадку ТНВ ми зберігаємо в ньому не тільки транзакції системи, але ще і коефіцієнти довіри до конкретних вендорів, а тому користувачі можуть бути впевнені, що дані отримані з ТНВ будуть надійними, бо механізми довіри реалізуються як раз за допомогою технології блокчейн (відбувається поступовий запис інформації о коефіцієнтах довіри до кожного фіда до блоків зі збереженням всієї історії змін цих коефіцієнтів). Важливим моментом є те, що всі записи до блокчейнів повинні мати мітку часу, щоб історія додавання інформації була зрозумілою і прозорою.

Отже, необхідність всіх компонентів системи доведена і можна приступити до вибору інструментів та опису функціональних вимог.

3.3 Функціональні вимоги до блоку аналітики

В систему надходить велика кількість даних від різних постачальників інформації. Перш за все ці дані необхідно обробити та виявити їх корисність – це задача блоку аналітики (AB, Analyze information Block). AB – є вхідною точкою для всіх зовнішніх запитів до системи. Схематично блок аналітики зображено на рис. 3.2. Детальний опис взаємодії зі сховищами даних буде надано у підрозділі 3.6 (про взаємодію компонентів системи):

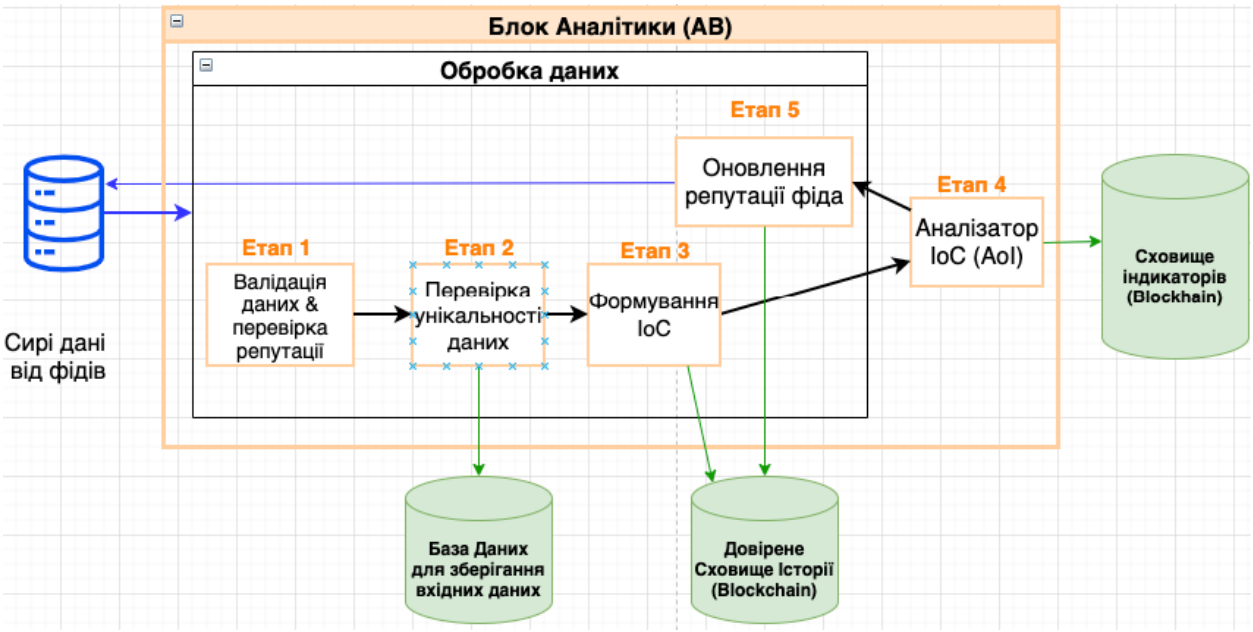

Рисунок 3.2 - Блок аналітики

АВ повинен відповідати ряду функціональних вимог, які перераховано нижче:

- Обробка та парсинг вхідних даних та обробка інформації стосовно постачальників цих даних;
- Верифікація даних отриманих від фідів (БА має впевнитися, що отримані дані не є зловмисними або недостовірними, а також є корисними для системи);
- Збереження першоджерела та інформації про вендора в базу даних;
- Перевірка унікальності даних (якщо IoC, відповідний конкретним даним вже існує в системі, потрібно розширити інформацію стосовно цього IoC або ж проігнорувати цей запит);
- Виокремлення IoC з валідних та унікальних даних (створення уніфікованого об’єкта IoC з сирих даних, який в подальшому буде додано AoI);

- Додавання IoC до Аналізатора Індикаторів Компрометації (AoI, Analyzer of Indicators). Елемент AoI є чергою, котра зберігає та оброблює IoC від різних фідів в межах одного циклу генерації блоку;
- Збереження знайдених IoC до IoC Storage;
- Визначення та коригування репутації feedів в залежності від якості наданих даних;
- Запис даних про репутацію вендора та його запити до ТНВ;

На основі описаних функціональних вимог до АВ можна зробити висновки, що АВ відповідає за парсинг, валідацію, дедуплікацію та нормалізацію даних отриманих із зовнішніх джерел. А також розширення існуючої інформації про IoC та визначення рівня репутації постачальників даних.

3.4 Вибір централізованої БД для зберігання вхідних даних

У цьому розділі буде порівняно SQL та NoSQL бази даних в контексті задач даної системи та обрана БД для зберігання першоджерел IoC.

Для отримання IoC спершу необхідно обробити вхідну інформацію в блоці аналітики. Після цього, якщо інформація валідна та корисна, з неї буде виокремлено IoC та додано до черги AoI. Однак, як було зазначено в підрозділі 3.2 є необхідність в тому щоб зберігати вхідні дані надані вендорами. Але зберігання всіх даних, які присилають в систему, не є ефективним, бо, по перше, ці дані можуть бути зловмисними, а по друге вони можуть бути надлишковими для системи, тобто вже інувати в БД. Тому буде доречним запропонувати зберігати першоджерела тільки тих даних, котрі пройшли перший та другий етап (відповідно «Валідація даних & перевірка репутації вендора» та «Перевірка унікальності даних») в циклі блоку аналітики (див. рисунок 3.2).

Тепер, коли ми визначились с етапом запису сирих даних до БД, слід обрати конкретну БД для реалізації поставлених задач. Спершу слід визначити використовувати SQL чи NoSQL базу даних, тому порівняємо переваги та недоліки цих видів баз даних для даної системи:

1) Бази даних SQL є реляційними, NoSQL - нереляційними.

Розробка та підтримка структури реляційної БД – це досить трудомістка та важка робота і в нашому випадку вона не принесе достатньо переваг. Легше і зручніше зберігати першоджерела у тому вигляді, в якому вони надійшли до нашої системи, щоб при їх подальшому використанні не було втрачено частину даних через нормалізацію чи обробку даних. Якщо дані будуть зберігатися в первинному вигляді, вони будуть давати більше інформації при зверненні до них, аніж вже оброблені дані. Для зберігання вхідних пакетів даних краще підійде нереляційна БД.

2) Бази даних SQL використовують структуровану мову запитів і мають заздалегідь визначену схему. Навідміну, NoSQL бази даних мають динамічні схеми для неструктурованих даних.

Зробивши висновки с попереднього пункту, зрозуміло, що дані, які потрібно зберігати в БД не будуть структурованими і, більш того, можуть бути надані в різному вигляді в залежності від постачальника.

3) Бази даних SQL є вертикально масштабованими, а NoSQL БД є горизонтально масштабованими.

Бази даних SQL масштабуються вертикально, а це означає, що для збільшення навантаження на один сервер, потрібно покращити його технісні характеристики, такі як кількість ядер процесору чи кількість оперативної пам’яті. Бази даних NoSQL, навпаки, є горизонтально масштабованими. Це

означає, що можна обробити більше трафіку шляхом шардінгу або додавання більшої кількості серверів для NoSQL БД. Взагалі, горизонтальна масштабованість є більш потужною, що робить бази даних NoSQL кращим вибором для великих або неструктурованих наборів даних, а це саме те що необхідно в нашій системі.

4) Бази даних SQL краще для багаторядкових транзакцій, а NoSQL - для неструктурованих даних, таких як документи або графіки.

Бази даних NoSQL мають динамічні схеми для неструктурованих даних, і дані можуть зберігаються різними способами: вони можуть бути орієнтованими на стовпці, орієнтовані на документи, на основі графіків або організовані як сховище ключ-значення. Ця гнучкість дає багато переваг порівняно з SQL базою даних. В нашому випадку буде доречно зберігати дані парами ключ-значення, де ключем буде мітка часу та IP вендора, а значенням буде пакет даних.

З усього вищезазначеного стає зрозумілим, що по всім параметрам, кращим варіантом для даною системи буде обрати NoSQL базу даних.

Особливими вимогами для бази даних запропонованої системи будуть наступні: швидкий запис та читання даних, масштабованість, високий час безвідмовної роботи. Слід зазначити, що час на видалення та оновлення даних не є важливим згідно наших задач, так як такі випадки будуть траплятись вкрай рідко. Було б плюсом, якби БД мала підтримку SQL синтаксису, аби спростити запити на отримання даних.

Задачі, які поставлені в нашому випадку до бази даних досить прості: записувати неструктуровану інформацію та інколи читати її, і зовсім рідко вносити зміни до БД. Виходячи з цього можна обрати будь-яку відому базу даних, бо всі вони гарно впораються зі своєю задачею. Наприклад “MongoDB”, “Apache Cassandra”, “Google Cloud BigTable” або “Apache HBase”.

3.5 Вибір та порівняльна характеристика блокчейн платформ

В цьому підрозділі пропонується розглянути порівняння провідних блокчейн платформ та обрати найкращу для реалізації розподіленої системи обміну загрози на основі блокчейн сховища.

Мною була опублікована стаття «Порівняння провідних блокчейн платформ» в науковому журналі [2]. В цій статті були порівняні найбільш відомі блокчейн платформи (Bitcoin, Ethereum, XRPL (Ripple), Stellar, R3 Corda, Hyperledger Fabric, Quorum, OpenChain, EOS, Cosmos, LISK.) на основі десяти порівняльних характеристик, таких як галузь використання, покоління блокчейну[11], тип блокчейну, наявність смарт контрактів та dApps, час генерації блоку, TPS, DCS та управляюча організація. Ґрунтуючись на порівняльній таблиці та на потребах запропонованої системи було обрано блокчейн платформу для реалізації структури блокчейн-сховища для IoC.

На основі розглянутих в статті критеріїв була сформована наступна порівняльна таблиця (рис. 1). Для кращого розуміння порівняльних критеріїв дивись теоретичний матеріал розділу 1.

	Bitcoin	**Ethereum**	**XRPL (Ripple)**	**Stellar**	**R3 Corda**	**Hyperledger Fabric**	**Quorum**	**OpenChain**	**EOS**	**Cosmos**	**LISK**
Галузь	Фін. послуги	Міжгалузева	Фін. послуги	Фін. послуги	Фін. послуги	Міжгалузева	Міжгалузева	Цифрове управління активами	Міжгалузева	Міжгалузева	Міжгалузева
Покоління	1st	2nd	1st	1st	1st	2nd	2nd	2nd	2nd	3rd	2nd
Тип блокчейну	Публічний	Публічний	Приватний	Обидва	Приватний	Приватний	Приватний	Приватний	Приватний	Обидва	Приватний
Алгоритм консенсусу	PoW	PoS(before PoW)	RPCA	SCP	Pluggable Framework	PBFT	Majority Voting	Partionned Consensus	DPoS	BPoS	DPoS
Смарт контракти	Так	Так	Ні	Так	Так	Так	Ні	Так	Так	Так	Так
dApps	Ні	Так	Ні	Так	Ні	Так	Ні	Так	Так	Так	Так
Час блоку	10-60хв	3-5хв	4с	5с	2с	1с	0.5с	5с	1.5с	2с	10с
TPS	7	25	1500	1000	600	750	180	100	4000	10000	25
DCS	Ні	Так	Ні	Ні	Ні	Так	Так	Ні	Так	Так	Так
Управляючий орган	Bitcoin	Ethereum Developers	Ripple Labs	Stellar Development Foundation	R3 Consortium	Linux Foundation	Ethereum Developers and JP Morgan Chase	CoinPrism	EOSIO Core Arbitration Forum(ECAF)	The Cosmos GWG	The Lisk Foundation

Рисунок 3.3 - Порівняльна характеристика блокчейн платформ

Розглянемо необхідні критерії для запропонованої системи та виберемо підходящі платформи згідно порівняльної таблиці (рисунок 3.3). В таблиці зображеній на рис. 3.3 клітинки зафарбовані різними кольорами: червоним, жовтим та зеленим. Червоний колір означає, що характеристика даної платформи зовсім не підходить для нашої системи, жовтий – означає що дане рішення можливо застосувати, але є невеликі нюанси, а зелений колір означає, що поточна характеристика даної платформи є повність підходящою для потреб нашої системи.

Для запропонованої системи, потрібна блокчейн платформа, яка є міжгалузевою, так як наша система не є виключно фінансовою і основна мета застосування технології це зберігання даних, таких як IoC та транзакції спілкування між системою та клієнтами, та доступ до них.

Наступним критерієм є алгоритм консенсусу, який у нашому випадку повинен бути відносно простим та ефективним алгоритм консенсусу. Гарними алгоритмами для даної системи будуть PoS, DPoS, PBFT, бо вони ефективні та широковживані. Алгоритм PoW буде поганим вибором для нашої системи, так як для майнінга блоків в цьому алгоритмі потрібно використати гігантську кількість обчислювальної потужності, а це є дуже коштовним і за для уникнення зайвих трат, цей алгоритм краще не використовувати. Жовтим позначені алгоритми, які не є часто вживаними, а тому є менш протестованими в реальних умовах і інформації щодо їх викорситання значно менше ніж для алгоритмів, позначених зеленим кольором.

Також платформа повинна мати можливість створення смарт контрактів, бо за допомогою смарт контрактів будуть регулюватися відносини між постачальниками даних, користувачами та системою, мати блокчейн 2.0 або 3.0 покоління(не бажано, тому більшість функцій та переваг цього покоління є

непотрібними для нашої системи) і бути приватною, так як блокчейн повинен бути доступним для обмеженого кола користувачів або для використання внутрішніми аналітичними сервісами.

До того ж із-за специфіки нашої системи TPS і час на створення блоку не є важливими критеріями для IoC Storage, тому що відносно невелика кількість записів буде додаватися до блоку кожного циклу, а час генерування самого циклу немає сенсу робити менше ніж п'ять хвилин із-за специфіки даної системи. Але критерій TPS є важливим для THB, тому що кількість транзакцій про запити користувачів і довіру до вендорів значно більша ніж кількість записів про IoC і тим не менш швидкості обробки 25 транзакцій на секунду (величина платформи LISK) буде цілком достатньо для задовільнення потреб системи.

Згідно рис. 3.3 та обговорених вище критеріїв для нашої цілі підходять декілька блокчейн-платформ. Це EOS, Hyperledger Fabric та LISK, так як вони повністю задовольняють критеріям запропонованої системи та використовують зрозумілий і ефективний механізм консенсусу і, до того ж, є досить популярним з поміж інших існуючих платформ, а це означає що для ці платформи гарно документовані та існує велика кількість інформації щодо використання платформ, а також великі ком’юніті, досвід учасників яких може бути корисним в процесі імплементації системи.

3.6 Взаємодія компонентів системи

В цьому підрозділі буде пояснена детальна робота системи починаючи з отримання сирих даних від постачальників та закінчуючи оновленням репутації постачальника та збереженні її у блокчейн. Слід зазначити, що суть системи в тому, що дані зберігається в централізованій БД, а інформація в блокчейнах. Інформація – це дані, які пройшли всі етапи обробки з АВ і є корисними для

фінальних користувачів системи чи для системи в цілому. Розглянемо покрокову роботу системи (див. рисунок 3.4).

Технологія блокчейн має різноманітні властивості, включаючи цілісність даних, децентралізацію та прозорість створення та додавання цих даних до блоків. Більш того, за допомогою блокчейну можна перевіряти внески каналів, які надають велику кількість корисних даних, щоб нагородити ці канали відповідно їх внеску та мотивувати для подальшої співпраці. Фіди можуть зробити свій внесок двома способами: шляхом надання ексклюзивної інформації та надання інформації, яка вже була надана іншим фідом (в межах одного циклу генерації блоку).

На рис. 3.4 наведено діаграму послідовностей для кращого розуміння процесу обробки інформації та додавання IoC до блокчейну.

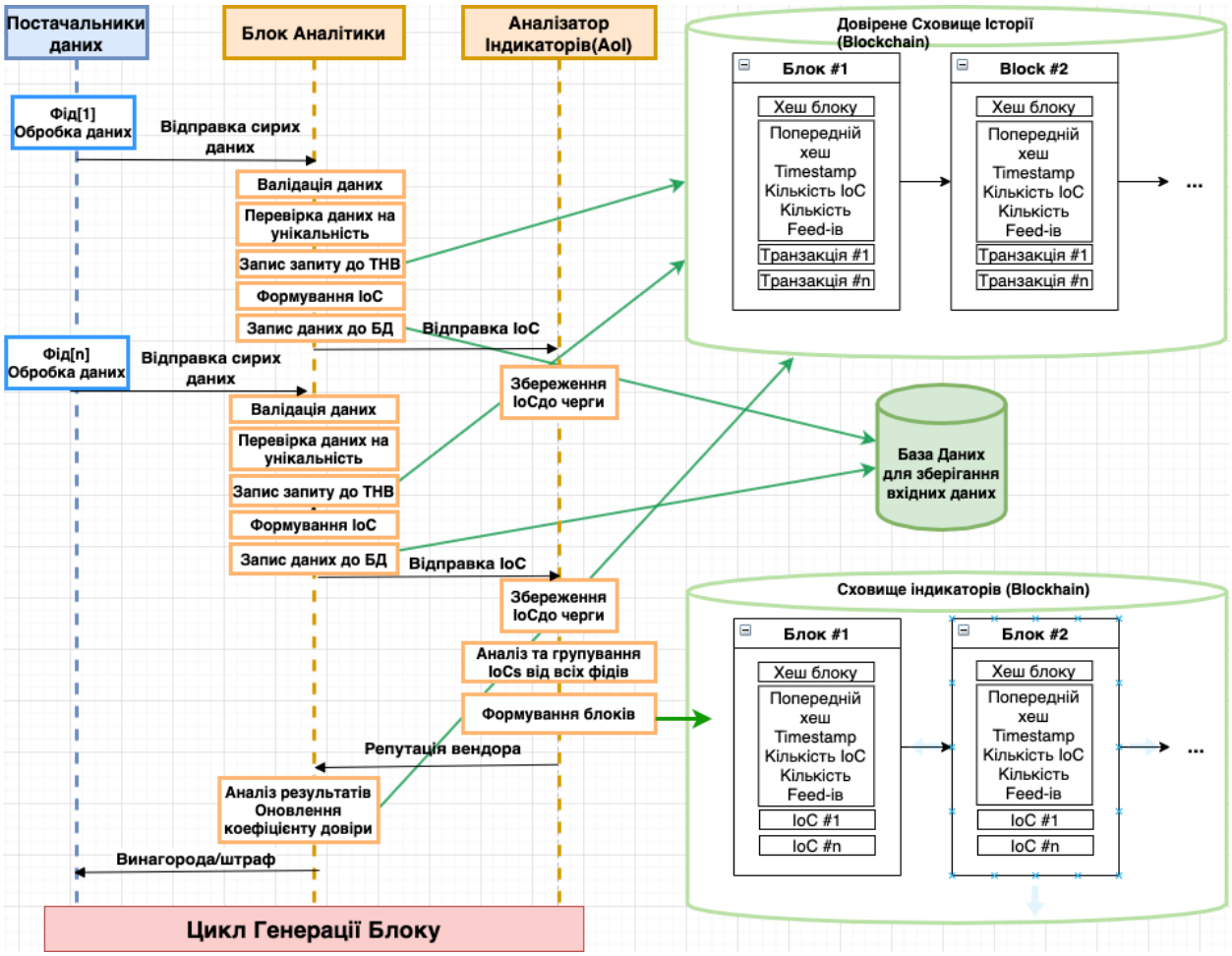

Рисунок 3.4 - Діаграма послідовностей процесів системи

Згідно з рисунком 3.4, процес роботи системи можна пояснити у п’ять етапів (підрозділи 3.6.1 – 3.6.5).

3.6.1 Збір даних

Перший етап це збір даних, він позначений на рисунку 3.4 синім кольором (на рисунку показано лише дві ітерації, але в реальних умовах їх може бути скільки завгодно в межах одного циклу генерації блоку). Вхідні дані можуть надходити з різних джерел, таких як звичайні користувачі мережі Інтернет або ж

організації і платформи, наприклад, інші CTI, OSINT, MISP, IDS, ISACs (information sharing and analysis centers), SIEM системи та інше. Інформація щодо надходження даних, тобто комунікація між нашою та зовнішньою системами записується до THB, це потрібно для того щоб система мала доступ до історії взаємодії конкретного фіда з блоком аналітики і базуючись на цій історії можна було б побудувати коефіцієнт довіри до цього фіда. На основі коефіцієнта довіри можна спростити механізми оцінки даних, які надходять від цього постачальника, збільшувати рівень винагороди за корисні дані та надати інформацію користувачам щодо порядності цього вендора. Але для участі в процесі обміну даними, фід спочатку повинен надіслати запит на додавання до блокчейну THB. Це потрібно для того, щоб, по перше, створити ID цього фіда в системі та надати йому рівень довіри за замовчуванням, а, по друге, для того щоб в подальшому цей фід мав змогу отримувати винагороду за надання корисних даних. Цей підхід також має дуже вагому перевагу для майбуніх контриб'юторів. Оскільки постачальник даних є учасником приватного блокчейну THB, то він має доступ до інформації щодо репутації інших вендорів. Регулярно аналізуючи цю інформацію, вендор може налаштовувати свою мережеві екрани та інші засоби захисту таким чином щоб обмежувати трафік від інших стовідсотково ненадійних систем чи платформ. Як вже зазначалось раніше зберігати пакети даних повністю у блокчейні не є ефективним, тому що це перевантажить систему гігантською кількістю інформації, тому спочатку вхідні пакети потрібно обробити.

3.6.2 Обробка даних

Після збору даних настає наступна стадія – обробка даних (відповідно етапи 1 – 3 з рисунку 3.2). Спочатку дані, отримані від вендора, проходять валідацію (етап 1, рисунок 3.2). Гонг та ін. [12] запропонував модель, яка може

проаналізувати надійність та достовірність даних, використовуючи порівняльний аналіз даних CTI, щоб перевірити надійність інформації OSINT.

Після цього дані проходять перевірку на унікальність (етап 2, рисунок 3.2), тобто перевіряється, що система не має ідентичних даних для уникнення дуплікації. В разі виявлення дуплікації, АВ перевіряє чи можна розширити інформацію про існуючі IoC, якщо так, то цей пакет проходить подальшу обробку, якщо ні – ігнорується. Такий підхід позбавляє від необхідності збирати непотрібні, зловмисні та повторювані дані.

Одразу після валідації та перевірки даних на унікальність, запит користувача додається до THB. В цій транзакції зазначається час звернення до системи, тип звернення (надання пакету з потенційно корисною для системи інформацією, чи запит іншого характеру, наприклад, надсилання пакету даних на аналіз наявності IoC в ньому) та результат оцінки наданих даних. У разі, якщо вендор надав злочинні данні, до THB додається транзакція зменшення рівня репутації цього фіда, а у разі надання невалідних чи вже існуючих у системі даних репутація вендора залишається незмінною. А в разі надання корисних даних, з яких пізніше буде сформовано IoC, репутація вендори збільшиться пропорційно його вкладу в систему після генерації блоку IoC (див. підрозділ 3.6.5).

В разі успіху на етапах 1 і 2 блоку аналітики, наступним кроком процесу обробки даних є формування IoC (етап 3, рисунок 3.2). Для виявлення кіберзагроз та IoC за даними, можна використати [13],в якому запропоновано метод аналізу загроз на основі сирих даних.

Сформований IoC в купі з ID вендора цього індикатора передаються до блоку AoI, а вхідний пакет разом з IP-адресою відправника(або ж його ID з блокчейну THB) записується у централізовану БД, для того щоб пізніше, у разі необхідності, можна було з’ясувати походження того чи іншого IoC. Важливо зазначити, що запис сирих даних у БД буде відбуватись тільки в разу успішного

формування IoC (див. рисунок 3.4), у іншому разі це не буде мати ніякого сенсу, бо якщо IoC не буде сформовано, до цього пакету ніколи не звернуться в майбутньому, тобто цей запис буде «мертвим» в БД.

Процес обробки даних передає в AoI лише інформацію про IoC, яка є критично важливою, та інформацію про ID фіда, який надав вхідний пакет даних. Таким чином розподіляються і зберігаються ресурси системи, бо кожен окремий вузол АВ відповідає за свою задачу, тобто архітектура АВ є мікросервісною, а не монолітною.

3.6.3 Обробка IoC в AoI

Після виявлення IoC та збереження його першоджерела в БД, індикатор компрометації надсилається до блоку Аналізатора Індикаторів (етап 4, рисунок 3.2, та третій стовпчик на рисунку 3.4). Аналізатор IoC (AoI, Analyzer of Indicators) з черги - це незалежна система, яка є частиною блоку аналітики, та яка обробляє IoC отримані на етапі обробки інформації. Аналізатор IoC може забезпечити прозорість за допомогою відкритого коду (логіка цього блоку є доступною для користувачів системи). До того ж AoI частково вирішує проблеми великого навантаження на систему та оптимізації простору для зберігання даних (обмеження на розмір блоків). Перша проблема вирішується завдяки тому, що АВ має мікросервісну архітектуру, а не монолітну. Значить AoI буде працювати незалежно від інших блоків АВ, а це в свою чергу зменшує навантаження на мережу завдяки розподіленню ресурсів та обробці в AoI лише IoC. Друга проблема вирішується за рахунок групування IoC від різних вендорів. Отож, вузол AoI є частиною АВ та має дві основні функції: групування та оцінку IoC (циклічний процес, який починається спочатку щойно згенеровано новий блок IoC Storage) та генерація блоків.

Оскільки AoI додає всі IoC до черги, як тільки вони поступають в даний блок, то по завершенню однієї ітерації генерування блоку, він може може проаналізувати зібрані IoC. AoI перевіряє чергу раз в n хвилин, де n – це константний проміжок часу. Аналіз IoC полягає в тому, що AoI перевіряє, чи існують в черзі однакові IoC, надіслані з різних каналів. В випадку коли декілька різних постачальників надіслали дані, з яких було отримано одні й ті самі IoC, AoI групує їх в один IoC (важливо, що IoC можуть бути схожими та доповнювати один одного) та формує одну транзакцію і, відповідно, збільшує коефіцієнти довіри до вендорів.

Для накопичення репутації вендорами, пропонується наступна модель. Внесок унікальних та оригінальних даних дає x балів каналу, який надав цю інформацію. Якщо ж фід надав інформацію, з якої було вилучено такий самий індикатор компрометації, який вже є у черзі, або IoC, який доповнює інший IoC, доданий до черги раніше (тобто фід надав неунікальну інформацію в межах ітерації тим самим підтвердивши інформацію іншого вендора), то він отримує y балів репутації. Цілком зрозуміло, що x > y, але коефіцієнт відношення (k = x/y) цих двох величин краще встановити експериментальним шляхом. Отже, якщо внесок унікальних IoC фіда дорівнює u і r – внесок неунькальних IoC (ті що підтверджують інші), то загальний зріст репутації цього постачальника за один цикл буде дорівнювати:

$$\text{Внесок} = \frac{ku+r}{\text{Загальний вклад всіх фідів за цикл}} * 100\% \qquad (3.1)$$

Вважається, що чим більше інформації передається з каналу і чим вищий рівень довіри до цього каналу, тим надійнішими є дані.

3.6.4 Генерація блоку(зберігання IoC у блокчейн)

Генерація блоків IoC Storage є важливою функцією, за яку також відповідає AoI (етап 4, рисунок 3.2). Формування блоків у AoI, а не в блоці обробки даних (підрозділ 3.6.2), пов’язано з ефективністю зменшення навантаження на систему, спричиненою обробкою великої кількості зібраних даних в блоці обробки, а також розподіленням ресурсів системи.

Блокчейн IoC Stroage використовується для захисту IoC. Реалізація блокчейну, на відміну від використання загальнодоступних блокчейнів, вимагає створення блоків в централізованій установі для підвищення ефективності системи, в якій відбувається обмін великими даними. AoI генерує блоки з згрупованих індикаторів компрометації (підрозділ 3.6.3), ID записів першоджерел бази даних для цих індикаторів та ідентифікаторів фідів, кожний константний проміжок часу (припустимо кожні 10 хвилин), тобто блоки генеруються з надійного та валідного набору даних.

У таблиці 3.1 наведені компоненти, які зберігає блок. Блокчейн забезпечує цілісність даних, з'єднуючи усі попередні значення хешу блоку зі значенням хешу поточного блоку.

Блок містить мета інформацію, таку як: номер блоку, хеш блоку, хеш попереднього блоку, час створення, кількість збережених індикаторів та кількість вкладників. Блок-хеш - це хеш усієї інформації в блоці. Кількість IoC представляє кількість індикаторів збережених в блок, а кількість фідів - кількість постачальників даних, з яких було сформовано IoC поточного циклу.

Дані блоку містять транзакції, які складаються з IoC, ID першоджерел та ID фіда в системі. ID фіда представлений унікальним ідентифікаційним номером, виданим під час реєстрації у приватному блокчейні THB.

Таблиця 3.1 – Схематичний вигляд блоку IoC Storage

Номер блоку	2456
Хеш блоку	4a859de867b6f963a1baa2dac5447938c0be7c763656831bb1e883b9d6c13375
Попередній хеш	7ec43b37a805aa35fdbb7aa7ba8e3e1da3a8c2bd021fea85f96518a51b3fa526
Час створення	21/May/2021:11:43:14
Кількість IoC	300
Кількість фідів	57
Дані	#1/Feed#76/ 0bb705f69588bcbaef440f729228911321ed4f47491335047349e67f01d0c1b1 #1/Feed#23/ 01d0bbddc2fbe25bfaa0f4ca92ddefb765cd953a5626fe6d85a7f7059ce9c38d … #300/Feed#76/ 0ffe40b16aa45c5af2a321171d207ebcb5b87f50aee86bc253d3c0d6cfe0c774

Після закічення циклу генерації блоку AoI видаляє всю інформацію з черги та починається новий цикл (підрозділи 3.6.1 – 3.6.4).

3.6.5 Інформування постачальників щодо результату обробки, надісланих даних

Щойно всі попередні процеси завершені (тобто кожні n хвилин) потрібно відправити винагороду та повідомити про змінення коефіцієнту довіри всіх фідів приймаючих участь у циклі генерації блоку. Нагадаємо, що коефіцієнт довіри було зменшено на третьому етапі, якщо дані були зловмисними. Якщо ж дані, надані фідом, стали першоджерелами для IoC то його коефіцієнт довіри зросте на величину, яка вираховується за формулою 3.1. Після обчислення нового значення коефіцієнту довіри до постачальника даних, цей коефіцієнт буде записано як нова транзакція до THB. Такий підхід надає прозору історію щодо змінення репутації з самої першої взаємодії з системою, тому що транзакція, яка потрапила в THB вже залишиться там назавжди. Щоб змінити значення довіри потрібно записати нову транзакцію. Таким чином, можна отримати ланцюжок транзакій з коефіцієнтами довіри відносно конкретного фіда і простежити зміну рівня довіри до нього.

Якщо фід надав корисні дані до системи протягом одного циклу, тобто його репутація всередині системи виросла, він отримає винагороду у вигляді локальної валюти THB, ця винагорода буде базуватись на двох фактори: кількість наданих корисних даних та загальний рівень довіри (чим він вище, тим більше винагорода). Також буде доречним розглянути ідею стягувати штраф з гаманців THB, якщо репутація фіда за цикл впала із-за надання зловмисних даних. Це зробить невигідним вкладання в систему зловмисних даних для зловмисників. Також, окрім винагороди, всі фіди отримають повідомлення про змінення рівня довіри до них.

Важливо зазначити, що аналіз результатів поточного циклу, передається назад до первинного обробника даних в блок «Оновлення репутації фіда»(див.

рис 4.2, етап 5). Це зроблено для того, щоб розділити рівні взаємодії системи зі сховищами даних. Обробник даних взаємодіє з ТНВ та БД, а Аналізатор Індикаторів взаємодіє з IoC Storage.

На даному етапі система може збирати та обробляти дані, а також інформувати користувача щодо результатів обробки. У наступному розділі розглянемо способи використання системи.

3.7 Способи використання системи

Побудована архітектура (див. підрозділи 3.1-3.6) надає змогу обробляти вхідні дані, дедуплікувати інформацію, виокремлювати з них IoC та зберігати їх у надійному сховищі. Запропоновано механізми для обчислення рівня репутації для постачальників даних та методи винагороди за вклад корисної інформації. Крім того система має повну та цілісну історію взаємодії з користувачами та фідами, за допомогою якої можна простежувати зміну рівнів довіри до постачальників даних. Враховуючи ці переваги можна придумати досить багато шляхів ефективного використання системи. В даній роботі запропоновано два основні напрямки використання даної системи: (1) використання однією організацією або групою організацій зі спільними інтересами та (2) із залученням зовнішніх користувачів для отримання прибутку за продаж інформації.

3.7.1 Використання системи внутрішніми користувачами

Використання системи внутрішніми користувачами схематично зображено на рисунку 3.5.

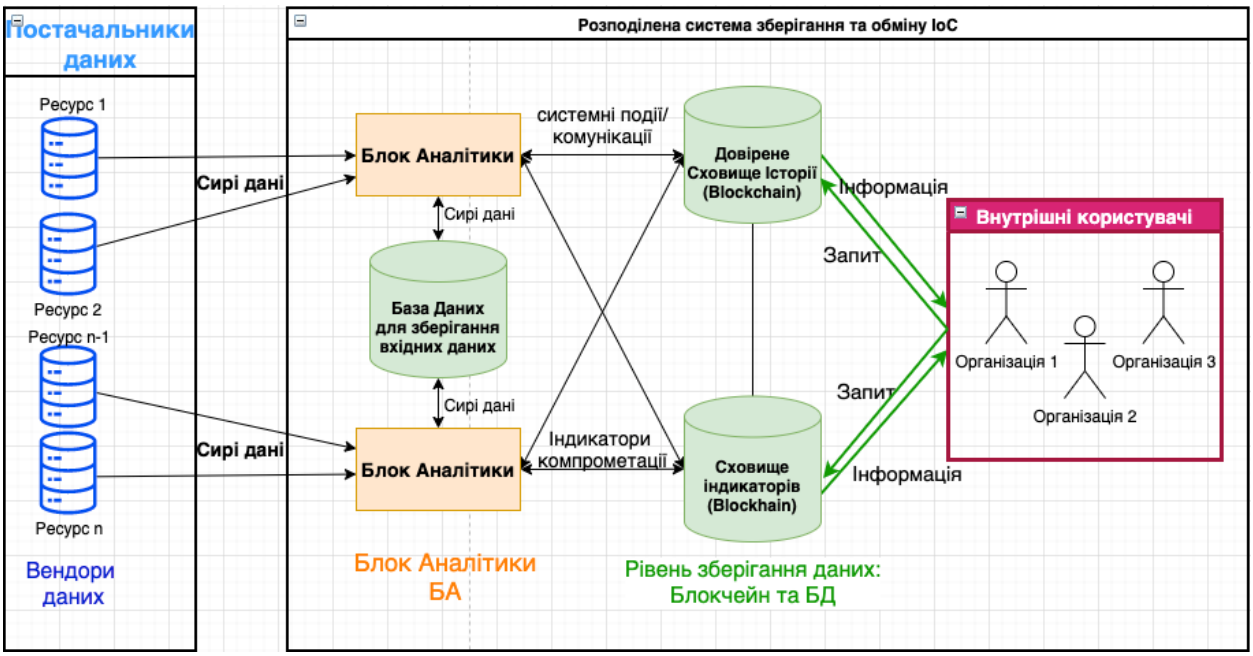

Рисунок 3.5 – Використання системи внутрішніми користувачами

Внутрішні користувачі мають повний доступ до цієї системи, тобто вони повністю регулюють роботу системи. Користувачем може буди як одна приватна організація, яка використовує систему для збору IoC та будування політик безпеки, так і декілька спільних організацій, які мають спільні інтереси (наприклад, уряд однієї країни чи всі Європейські атомні станції).

Суть даної моделі в тому, що збір та аналіз даних полягає виключно на організації, яка ці дані буде використовувати. До того ж важливим фактором є те, що орагнізації необхідно платити кошти фідам, у разі надання корисних даних для того щоб заохочувати їх робити подальші внески до системи.

3.7.2 Використання системи зовнішніми користувачами

Використання системи зовнішніми користувачами схематично зображено на рисунку 3.6.

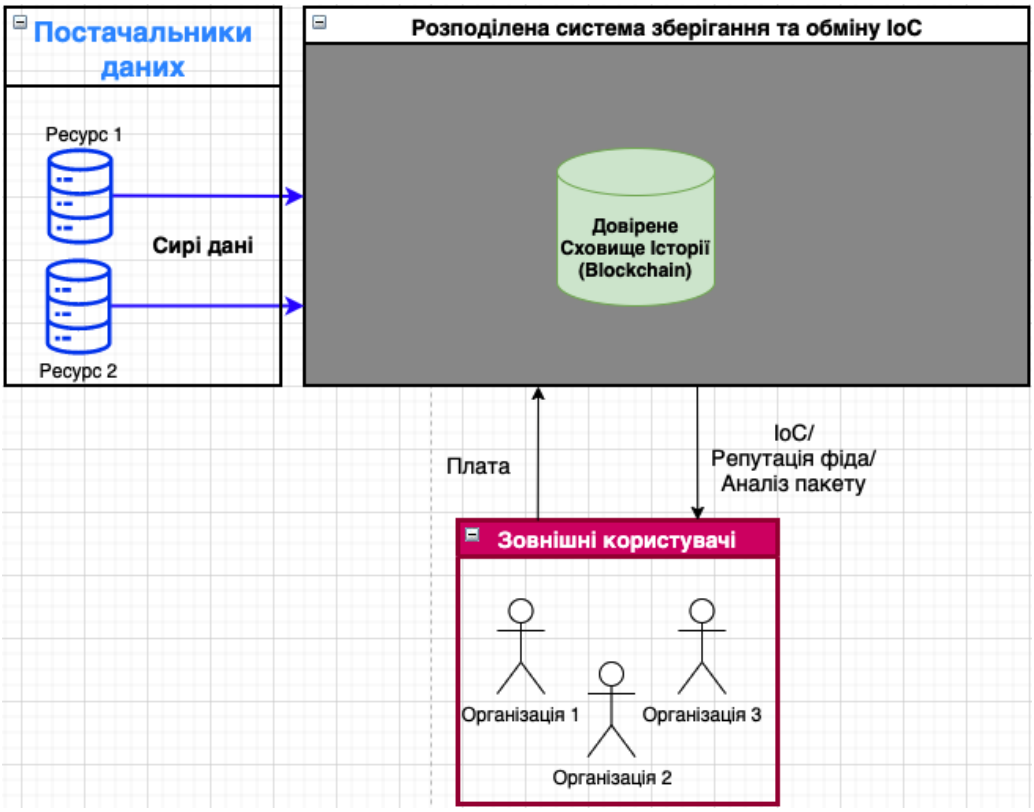

Рисунок 3.6 – Використання системи внутрішніми користувачами

Зовнішні користувачі не знають, яким чином побудована внутрішня архітектура системи. Але вони є учасниками Trusted History Blockchain. Завдяки THB, користувачі можуть обмінювати локальну валюту блокчейну на корисну для них інформацію. Використання системи зовнішніми користувачами може відбуватись в два шляхи.

1) Перший шлях – це надання надійної інформації користувачу за певну плату та її подальший аналіз користувачем. Це є ситуація, коли споживач інформації, який потребує нову CTI інформацію або хоче узнати чи можна довіряти тій чи іншій організації, отримує цю інформацію від нашої системи. В даному випадку споживачем інформації може бути індивідуальна особа або експерт з питань безпеки будь-якої організації.

2) Другий шлях - дана модель може використовуватись для аналізу пакету даних, надісланого користувачем, за наступним сценарієм: зовнішній актор надсилає плату за послугу та пакети даних, які він хоче перевірити на наявність кіберзагроз, система в свою чергу аналізує прийняті пакети даних на основі IoC Storge і відправляє результат аналізу користувачу.

Суть даної моделі в тому, що збір та аналіз даних полягає на власнику даної системи. Це робиться для того, щоб в подальшому отримувати кошти за продаж надійної інформації або аналіз даних користувача.

Висновки до розділу 3

В розділі 3 було запропоновано архітектуру розподіленої системи для зберігання індикаторів компрометації. У ході роботи було проведено порівняльну характеристику блокчейн платформ за багатьма характеристиками та обрано платформу для реалізації блокчейну в даній системі згідно задач, які вона повинна виконувати. Також було обрано централізовану базу даних для даної системи. Опис взаємодії компонентів системи дає повне розуміння того, як запропонована системи буде функціонувати. Крім розробки архітектури, були наведені два основні напрямки використання даною системи: використання системи внутрішніми та зовнішніми користувачами.

Як результат роботи отримали архітектуру, готову для імплементації та подальшого використання системи перевагами якої будуть: ефективна обробка даних та надійні механізми отримання та зберігання IoC, методи для оцінки репутації фідів та доступ до прозорої історії додавання і розширення IoC до блокчейну, комунікації користувачів з системою та зміни репутації постачальників даних.

ВИСНОВКИ

В першому розділі даної роботи було розглянуто технологію блокчейн та основні супутні терміни, порівняно найбільш популярні алгоритми досягнення консенсусу.

В другому розділі було описано концепт запропонованої системи та надано переваги, які вона має.

В третьому розділі була створена архітектура для розподіленою системи обміну індикаторами компрометації, описано архітектурний концепт системи, порівняно провідні блокчейн платформи за багатьма характеристиками, порівняно та обрано базу даних для даної системи та проведено детальний опис взаємодії всіх елементів системи, а також надано подальші шляхи використання даної системи.

У роботі було створено архітектуру CTI системи на основі блокчейну. За допомогою використання технології блокчейн досягається децентралізація, консистентність та достовірність даних, а також неможливість скомпрометувати IoC, які вже потрапили до блоків. За допомогою запропонованої складної логіки блоку аналітики та розподілення обчислень досягається ефективна обробка вхідних даних та виокремлення достовірних IoC. Користувачі такої приватної блокчейн мережі можуть створювати стратегії реагування на IoC, як тільки вони були додані до розподіленого реєстру, і бути впевненими, що ці IoC не були і не будуть скомпрометовані. Це дозволить, зокрема для об'єктів критичної інфраструктури, якщо ми говоримо про локальний сектор (наприклад, уряд однієї країни) швидко реагувати на потенційні загрози і зробити свої системи в цілому більш захищеними. Також була запропонована модель оцінки довіри до постачальників даних. За допомогою запропонованої системи можна визначити

вектор атак: куди і на які об’єкти будуть спрямовані атаки, якого типу атаки, та які IoC було використано для ідентифікації атаки.

Внаслідок роботи отримуємо систему, яка по суті є сховищем, з одного боку фактичних загроз, тобто IoC, з другого боку потенційних загроз і чим раніше ці потенційні загрози будуть виявлені, тим більш захищеною ми робимо всю систему, та системи користувачів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) IBM Corporation. Three ways blockchain Explorers chart a new direction [Електронний ресурс] // IBM Corporation. – 2017. – Режим доступу до ресурсу: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03835USEN&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US.
2) Порівняння провідних блокчейн платформ. // Інновації науки XXI століття. – 2021. – №66. – С. 73–79.
3) Colomo-Palacios R. A critical review on blockchain assessment initiatives: A technology evolution viewpoint [Електронний ресурс] / R. Colomo-Palacios, M. Sánchez-Gordón, D. Arias-Aranda // Journal of Software: Evolution and Process. – 2020. – Режим доступу до ресурсу: https://onlinelibrary.wiley.com/doi/full/10.1002/smr.2272.
4) Imran B. Mastering Blockchain / Bashir Imran., 2018. – (Second Edition).
5) Yaga, D. Blockchain Technology Overview [Електронний ресурс] / D. Yaga, P. Mell // Cornel University. — 2019. — Режим доступу до ресурсу: https://arxiv.org/abs/1906.11078.
6) Gragido W. "Understanding Indicators of Compromise (IoC) Part I [Електронний ресурс] / Will Gragido // blogs.rsa.com. – 2012. – Режим доступу до ресурсу: https://web.archive.org/web/20170914034202/https://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/.
7) Burger, E.W.; Goodman, M.D.; Kampanakis, P.; Zhu, K.A. Taxonomy model for cyber threat intelligence information exchange technologies. In Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, Scottsdale, AZ, USA, 3 November 2014.

8) Barnum, S. Standardizing cyber threat intelligence information with the structured threat information expression (STIX). Mitre Corp. 2012, 11, 1–22.
9) MISP Project [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.misp-project.org/communities/.
10) Wagner, C.; Dulaunoy, A.; Wagener, G.; Iklody, A. Misp: The design and implementation of a collaborative threat intelligence sharing platform. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, Vienna, Austria, 24 October 2016
11) Colomo-Palacios, R. A critical review on blockchain assessment initiatives: A technology evolution viewpoint [Електронний ресурс] / R. Colomo-Palacios, M. Sánchez-Gordón, D. Arias-Aranda // Journal of Software: Evolution and Process. — 2020. — Режим доступу до ресурсу: https://onlinelibrary.wiley.com/doi/full/10.1002/smr.2272.
12) Gong S. A Reliability Comparison Method for OSINT Validity Analysis [Електронний ресурс] / S. Gong, J. Cho, C. Lee // IEEE Xplore. – 2018. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8412560.
13) Qamar, S.; Anwar, Z.; Rahman, M.A.; Al-Shaer, E.; Chu, B.T. Data-driven analytics for cyber-threat intelligence and information sharing [Електронний ресурс] / S. Qamar, Z. Anwar, M.A. Rahman, E. Al-Shaer, B.T. Chu // Comput. Secur. – 2017. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0167404817300287?via%3Dihub.
14) BlockChain Technology: Beyond Bitcoin / M. Crosby [et al.] // Applied Innovation Review. — 2016. — № 2. — P. 8. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. Appl. Innov. 2(6–10), 71 (2016).

15) N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis and S. Shiaeles, “On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection,” 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019.
16) L. Lamport, R. Shostak, and M. Pease, “The byzantine generals prob-lem,” ACM Transactions on Programming Languages and Systems(TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.
17) Riesco R. Cybersecurity threat intelligence knowledge exchange based on blockchain [Електронний ресурс] / R. Riesco, X. Larriva-Novo, V. Villagra // Springer Link. – 2019. – Режим доступу до ресурсу: https://link.springer.com/article/10.1007/s11235-019-00613-4.
18) Shiel I. A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology [Електронний ресурс] / I. Shiel, D. Homan // 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/334485083_A_New_Network_Model_for_Cyber_Threat_Intelligence_Sharing_using_Blockchain_Technology.
19) Wagner C. MISP -The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform [Електронний ресурс] / C. Wagner, A. Dulaunoy, G. Wagener // 3rd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2016). – 2016. – Режим доступу до ресурсу: https://www.researchgate.net/publication/309413369_MISP_-The_Design_and_Implementation_of_a_Collaborative_Threat_Intelligence_Sharing_Platform.