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

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2024 р.

Дипломна робота

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

на тему: Блокчейн-технології для зберігання доказів в комп'ютерній криміналістиці

Виконав: здобувач вищої освіти **IV** курсу, групи ФБ-06
(шифр групи)

Вєрнікова Лілія Геннадіївна
(прізвище, ім'я, по батькові) (підпис)

Керівник Барановський Олексій Миколайович, к.т.н., доцент кафедри ІБ
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент Хмельницький Микола Олексійович, к.ф.-м.н., доцент кафедри ММЗІ
(посада, науковий ступінь, вчене звання, науковий ступінь, 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 – 2024 року

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

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

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Вєрнікова Лілія Геннадіївна
(прізвище, ім'я, по батькові)

1. Тема роботи Блокчейн-технології для зберігання доказів в комп'ютерній криміналістиці,
керівник роботи Барановський Олексій Миколайович, к.т.н, доцент кафедри ІБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 31 травня 2024 р. № 2251-с

2. Термін подання здобувачем вищої освіти роботи 14 червня 2024 р.

3. Вихідні дані до роботи: фреймворк, на основі блокчейну для систем зберігання цифрових доказів

4. Зміст роботи: огляд і аналіз традиційних методів обробки і зберігання цифрових доказів, пропозиція фреймворку, моделювання фреймворку в вигляді графу, приблизна оцінка вартості реалізації та зберігання.

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

6. Дата видачі завдання: 27 лютого 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання теми дипломної роботи, визначення мети і постановка задач	17.10.23 - 26.02.24	виконано
2	Узгодження теми дипломної з керівником	27.02.24 - 28.02.24	виконано
3	Огляд і аналіз літератури за тематикою дипломної роботи	28.02.24 - 15.04.24	виконано
4	Отримання завдання	16.04.24 - 17.04.24	виконано
5	Розробка концепції фреймворку для системи зберігання цифрових доказів	18.04.24 - 13.05.24	виконано
6	Визначення структури дипломної роботи	13.05.24 - 15.05.24	виконано
7	Дослідження області та поставка існуючих проблем	16.05.24 - 18.05.24	виконано
8	Аналіз готових рішень і прикладів на основі блокчейну	18.05.24 - 19.05.24	виконано
9	Деталізація і опис всіх процесів в рамках запропонованого фреймворку	20.05.24 - 22.05.24	виконано
10	Моделювання фреймворку в графовій базі даних	23.05.24 - 25.05.24	виконано
11	Розрахунки приблизної вартості реалізації і зберігання	26.05.24 - 27.05.24	виконано
12	Формулювання рекомендацій щодо впровадження фреймворку	28.05.24 - 29.05.24	виконано
13	Оформлення і подача дипломної роботи	30.05.24 - 11.06.24	виконано

Здобувач вищої освіти _____ Лілія ВЄРНІКОВА
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Олексій БАРАНОВСЬКИЙ
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Робота складається з 4 розділів, містить у собі 20 рисунків, 1 таблицю, 1 додаток, 27 посилань на джерела, обсяг роботи становить 58 сторінок.

В роботі наведено: теоретичні дані стосовно обробки і зберігання цифрових доказів в сфері комп’ютерної криміналістики, ланцюга зберігання цифрових доказів, основи блокчейн-технологій; детальний опис всіх процесів запропонованого фреймворку, процес моделювання в графовій системі управління базами даних, розрахунки приблизної вартості реалізації і зберігання записів, рекомендації щодо впровадження.

Об’єкт дослідження: традиційні методи зберігання і обробки цифрових доказів.

Предмет дослідження: інтеграція блокчейн-технологій в систему обробки і зберігання цифрових доказів для забезпечення цілісності даних і прозорості процесів.

Мета роботи: створення фреймворку для підвищення ефективності і рівню захисту систем пов’язаних з цифровими доказами.

Ключові слова: блокчейн, ланцюг зберігання, цифрові докази.

ABSTRACT

The work consists of four sections and includes 20 figures, 1 table, 1 appendix, and 27 references with a total length of 57 pages.

This paper presents: theoretical data on the processing and storage of digital evidence in the field of computer forensics, the chain of custody for digital evidence, and the fundamentals of blockchain technologies; a detailed description of all processes within the proposed framework, the process of modeling in a graph database management system, calculations of the approximate cost of implementation and storage of records, and recommendations for implementation.

Object of the study: traditional methods of storing and processing digital evidence.

Subject of study: integration of blockchain technologies into the system of processing and storing digital evidence to ensure data integrity and process transparency.

Purpose of the study: to create a framework to enhance the efficiency and security of systems related to digital evidence.

Keywords: blockchain, chain of custody, digital evidence.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CoC – Chain of Custody

БД – База Даних

ПЗ – Програмне Забезпечення

IoT – Internet of Things

ESA – European Space Agency

NFT – Non-fungible token

PoW – Proof of Work

PoS – Proof of Stake

DPoS – Delegated Proof of Stake

PoA – Proof of Authority

AES – Advanced Encryption Standard

MFA – Multi-factor authentication

FBI – Federal Bureau of Investigation

NIST – National Institute of Standards and Technology

INTERPOL – The International Criminal Police Organization

ЦП – Цифровий підпис

RBAC – Role-based access control

АЗ – Апаратне Забезпечення

ETH – криптовалюта на платформі Ethereum

Gwei – номінал ETH, зазвичай використовується для оплати газу для транзакції

ВСТУП

Наразі, ми спостерігачі і, одночасно, творці цифрової ери, епохи, коли інформаційні технології все більше і швидше проникають як і в повсякденне життя, так і різноманітні бізнес-процеси. Глобальна цифровізація, безсумнівно, стає передумовою для зростання кількості і серйозності кіберзлочинів, що стає передумовою для удосконалення існуючих політик безпеки і створення нових засобів для збереження цілісності, доступності і конфіденційності інформації; а також актуалізує питання зберігання цифрових доказів, під час розслідування і судових процесів. Цифрові докази можуть бути знищені або спотворені, що ставить під загрозу прозорість і надійність юридичних процесів, отже питання удосконалення існуючих механізмів захисту приймає високий пріоритет.

Впровадження блокчейн технології в протоколи Chain of Custody є досить перспективним та сучасним рішенням для покращення рівня безпеки даних. Технологія пропонує архітектуру що базується на децентралізації, незмінності записів, і все це без потреби посередника, що вкрай важливо в аспекті розслідування кіберзлочинів. До того ж, використання блокчейну покращить ефективність процесів верифікації, що важливо в системах, де швидкість обробки даних є критичною.

Мета роботи: розробити концепцію (фреймворк) ефективної системи зберігання цифрових доказів, за допомогою інтеграції блокчейну, щоб максимально забезпечити прозорість і цілісність даних.

Для досягнення мети, були поставлені певні завдання, а саме:

- Вивчення предметної області
- Огляд і аналіз існуючих методів зберігання доказів
- Розробка концепції фреймворку основаного на блокчейні для зберігання і використання цифрових доказів
- Моделювання фреймворку в графовій системі управління базами даних
- Розрахунок приблизної вартості реалізації і зберігання запису
- Формулювання висновків і рекомендації, на базі результатів аналізу

Об’єктом дослідження будуть сучасні методи зберігання і використання цифрових доказів в комп’ютерній криміналістиці CoC. Предмет дослідження: використання блокчейн-технологій для впровадження посиленого захисту цифрових доказів.

Методи дослідження які будуть застосовані під час роботи:

- Огляд літератури і наукових робіт в рамках обраної тематики
- Розробка фреймворку блокчейн-системи
- Порівняльний аналіз традиційних процесів і процесів в рамках фреймворку
- Використання графової системи управління базами даних для створення моделі

Наукова новизна обумовлена виявленням невідповідності традиційних методів обробки і зберігання цифрових доказів згідно визначеним вимогам.

Тезиси роботи були успішно представлені на XXII Всеукраїнській науково-практичній конференції «Теоретичні і прикладні проблеми фізики, математики та інформатики» та опубліковані в загальному збірнику.

1 ДОСЛІДЖЕННЯ ОБЛАСТІ ТА ПОСТАНОВКА ПРОБЛЕМИ

В розділі «Дослідження області та постановка проблеми» викладено аналіз сучасних методів зберігання цифрових доказів у цифровій криміналістиці, наведені основні проблеми традиційних методів, такі як недостатня підготовка персоналу, ненадійність аудиту, відсутність стандартизації, ризик втрат і пошкоджень даних. Також, розглянуто вимоги до зберігання цифрових доказів, включаючи цілісність, прозорість, доступність, захист та сумісність. Зроблено висновки, про необхідність розробки більш ефективних і безпечних систем зберігання цифрових доказів, що відповідатимуть сучасним вимогам правосуддя.

1.1 Огляд сучасних методів зберігання цифрових доказів

Цифрова криміналістика (англ. Digital Forensics) – галузь судово-медичної експертизи, що зосереджена на виявленні, зборі, аналізі та збереженні цифрових доказів, які можуть бути використані в судових процесах.

Цифрові докази охоплюють будь-яку інформацію, збережену або передану в електронній формі, включаючи дані з комп'ютерів, мобільних пристроїв, мережевих систем, а також інтернет-комунікацій [15].

Основною метою цифрової криміналістики [12] є забезпечення цілісності та достовірності доказів, щоб вони могли бути прийняті у суді. Це включає розробку та впровадження методів і технологій для безпечного зберігання, передачі та аналізу цифрових даних, а також захист від можливих загроз і маніпуляцій.

Традиційні методи зберігання цифрових доказів найчастіше полягають в зберіганні даних на фізичних носіях або на локальних системах. В якості фізичних носіїв інформації зазвичай використовують жорсткі диски, USB-накопичувачі тощо, які зберігаються у спеціально обладнаних, згідно стандартів, приміщеннях з обмеженням доступу задля забезпечення цілісності і конфіденційності цифрових доказів. Також, все більше розповсюджується практика зберігання даних в локальних системах, що знаходяться під контролем відповідних органів. Таке зберігання дозволяє пришвидшити доступ і використовувати не тільки фізичні методи захисту інформації, а використовувати новітнє ПЗ для зменшення ризиків компрометації.

Ключових аспект зберігання і життєвого циклу цифрових доказів – дотримання протоколу ланцюга зберігання [10] *Chain of Custody* (далі – CoC). Протоколи CoC в контексті цифрової криміналістики визначають і відстежують всі дії з цифровими доказами протягом їх життєвого циклу, тобто утворюють хронологічних цифровий слід. Основною метою CoC є зберігання цілісності

кожного доказу, який після обробки може стати вирішальним у веденні різного плану розслідувань.

Рисунок 1.1 – Процеси CoC

1.2 Проблеми існуючих систем зберігання і обробки цифрових доказів

В технологічному світі зазвичай головна вразливість будь-якої системи – людський фактор. Витоки інформації, несанкціонований доступ до інформації тощо, в більшості випадків є результатом некомпетентності і халатності персоналу.

Проблеми [11], які виникають під час використання традиційних методів протоколу CoC:

- *Недостатня підготовка та компетентність персоналу*: різноманітні особи, що контактують з цифровими доказами (служби швидкого реагування, судові експерти, жертви, свідки, правоохоронці і т.д.) не проходять обов'язковий інструктаж, щодо поводження з важливими даними, це може призвести до пошкодження або навмисного втручання.

- *Ненадійність традиційних методів аудиту*: традиційні методи часто включають у собі ведення паперових/електронних журналів для відстеження доступу до доказів, які мають вразливість до підробок і втрат.

- *Відсутність систематичної взаємодії між різними системами і інстанціями:*використання різної деталізації на різних етапах переміщення доказів, що ускладнює відстеження CoC.

- *Ризик втрати і пошкодження даних:* цифрові докази що зберігаються на фізичних носіях, що вразливі до втрат, пошкоджень або знищення (через випадковості, аварії, крадіжки, природні умови), а ті, які зберігаються в локальних системах, можуть стати об'єктами кібератак, зломів, або технічних збоїв.

- *Відсутність автоматизованих систем аудиту*: традиційні методи не забезпечують повну прозорість всіх операцій з доказами, що може ставити під питання їхню достовірність

- *Відсутність стандартизації*: в різних країнах і різних організаціях використовують різні методи зберігання і обробки доказів, що ускладнює процедури міжнародної співпраці і обмін доказами між різними правоохоронними органами.

- *Повільна швидкість доступу*: через використання інструментів, які не відповідають сучасним технологіям отримання доступу до цифрового доказу є складною і довгою процедурою.

1.3 Основні вимоги до зберігання цифрових доказів

Цифрові докази є цінною інформацією в судових процесах, і повинні відповідати строгим умовам щодо їх стану, а саме:

- *Цілісність* – необхідно гарантувати, що дані не можуть бути змінені або пошкоджені після їхнього збирання. Це досягається за допомогою криптографічних методів, таких як хешування, що дозволяє виявити зміни в даних.

- *Прозорість і відстежуваність* – кожна операція з цифровими доказами повинна бути задокументована і доступна для перевірки. Це включає зберігання детальної інформації про те, хто, коли і для чого мав доступ до доказів.

- *Доступність і захист даних* – необхідно забезпечити контроль доступу до даних, щоб тільки уповноважені особи могли мати до них доступ. Це включає використання багатофакторної аутентифікації, ролей і привілеїв.

- *Захист від втрат і пошкоджень* – дані повинні бути захищені від фізичних і цифрових загроз. Це включає використання резервного копіювання, шифрування та безпечного зберігання.

- *Сумісність і стандартизація* – системи зберігання цифрових доказів повинні відповідати міжнародним стандартам і бути сумісними з існуючими системами правосуддя. Це забезпечує можливість використання доказів у судових процесах різних юрисдикцій.

Висновки до розділу 1

Після аналізу поточної ситуації і проблем, які існують в області зберігання цифрових доказів, а також аналізу рекомендованих вимог для даних такого типу, можна зробити висновок, що сучасні системи не відповідають вимогам, отже потрібно розробити і впровадити більш ефективну і безпечну систему що буде відповідати *сучасним* вимогам для підтримання порядку.

2 ТЕОРЕТИЧНІ АСПЕКТИ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ТА ДОТРИМАННЯ ПРОТОКОЛУ CHAIN OF CUSTODY

В розділі «Теоретичні аспекти блокчейн-технологій та дотримання ланцюга зберігання цифрових доказів» було розглянуто особливості архітектури блокчейн-технологій, а саме архітектуру і перспективи використання з прикладами успішних реалізацій. Також, було ознайомлено з основними принципами дотримання протоколу CoC, існуючими методиками та правовими аспектами.

2.1 Архітектура та перспективи використання блокчейн-технологій

2.1.1 Визначення та принципи роботи

Блокчейн (англ. Blockchain, block – блок, chain – ланцюг) – це технологія яка будується на принципах розподіленої бази даних [14], функціонуюча в P2P системі, безпека якої базується на криптографічних алгоритмах. Простими словами, це сховище даних, що містить у собі інформацію про всі транзакції, які відбуваються в межах системи. В контексті безпеки, основну роль в забезпеченні цілісності даних грає використання хешування.

Отже, елементарна частинка блокчейну це блок, що в загальному випадку містить в собі: хеш попереднього блоку (H_{prev},), мітку часу (T), деталі транзакції (D), та число Nonce (N), що використовується для валідації нового блоку в алгоритмах консенсусу. Математично сформулювати структуру блоку можна наступним чином:

$$\text{Блок} = \{H_{prev}, T, D, N\} \tag{2.1}$$

Структуру блоку графічно зображено на рисунку 2.1.

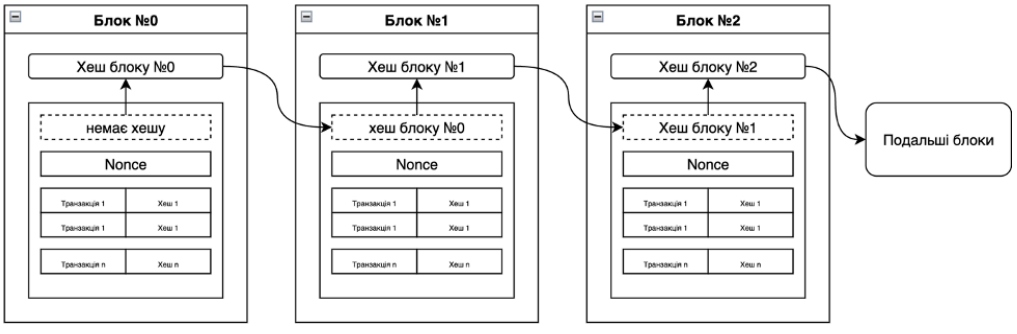

Рисунок 2.1 – Структура блоків

Завдяки такій структурі утворюється ланцюг залежності між ними і майже унеможливлює порушення цілісності даних.

2.1.2 Алгоритми консенсусу

Консенсусні алгоритми є основою функціонування будь-якої блокчейн-системи. Вони визначають процес, за допомогою якого всі учасники мережі приходять до узгодженого рішення щодо дійсного стану реєстру транзакцій. Основна мета консенсусного алгоритму полягає в забезпеченні узгодженості даних між усіма вузлами мережі, навіть якщо деякі з них можуть бути зловмисними або помилковими. Ці алгоритми гарантують, що всі учасники мають однаковий вигляд на поточний стан блокчейну, забезпечуючи таким чином цілісність і безпеку системи.

Деякі типи консенсуних алгоритмів:

- Proof of Work (PoW)

  Учасники мережі (майнери) виконують складні математичні задачі, щоб додати новий блок до блокчейну. Перший, хто вирішує задачу, отримує право додати блок і винагороду у вигляді криптовалюти. Зазвичай блокчейни на базі PoW є досить стійкими і безпечними, проте є енерговитратним та мають низьку пропускну здатність

- Proof of Stake (PoS)

  В фінансових системах власники криптовалюти можуть стати валідаторами, пропонуючи свої монети як заставу. Валідатори вибираються випадково для створення нових блоків.Така система має нижче енергоспоживання аніж PoW, але існує ризик централізації через накопичення монет в одного суб’єкта.

- Delegated Proof of Stake (DPoS)

  Користувачі голосують за делегатів, які будуть відповідальні за створення нових блоків. Делегати обираються на основі кількості голосів, отриманих від користувачів. Така система зазвичай має високу ефективність і швидкість обробки, проте як і в випадку PoS є ризик централізації.

- Proof of Authority (PoA)

  У PoA авторитетні вузли (вузли-авторитети) мають право створювати нові блоки. Вузли-авторитети обираються на основі їхньої репутації та довіри до них у мережі. Системи що використовують PoA в якості консенсусного алгоритму зазвичай мають високу пропускну здатність, швидке підтвердження транзакцій, низьке енергоспоживання порівняно з PoW, та здатність працювати в приватних блокчейнах, де довіра до вузлів є визначальною. Недолік використання PoA – ризик централізації, через обмеженість кількості авторитетних вузлів.

2.1.3 Приватні і публічні блокчейни

В загальному випадку блокчейн-системи за ступенем доступу до системи поділяють на три основні типи [3]: публічні, приватні, консорціумні. Вибір блокчейну зазвичай залежить від цілей і потреб використання. Основні відмінності різновидів блокчейн-систем наведені в таблиці 2.1

Таблиця 2.1 – Відмінності блокчейнів за ступенем доступу

	Тип блокчейну		
	Публічний	Приватний	Консорціумний
Інклюзивність	Так	Ні	Ні
Читання	Будь-який користувач	Лише підтверджені користувачі	В залежності від політики
Запис	Будь-який користувач	Лише підтверджені користувачі	Лише підтверджені користувачі
Право власності	Ніхто	Одна організація	Дві і більше організацій
Ідентифікація користувачів	Немає	Є	Є
Швидкість транзакції	Низька	Висока	Висока

2.1.4 Смарт-контракти

Смарт-контракт – це самовиконуваний контракт з умовами угоди, закодованими програмно. Смарт-контракти працюють на блокчейн-платформі, забезпечуючи автоматичне виконання умов контракту без необхідності залучення третьої сторони. Це дозволяє автоматизувати і спростити процеси, підвищуючи їх прозорість і ефективність.

Основні характеристики смарт-контрактів:

- Автоматизація: автоматичне виконання умов угоди після виконання заданих умов.
- Незмінність: після розгортання в блокчейні код і умови не можуть бути змінені.
- Децентралізація: виконання на децентралізованій мережі, що забезпечує прозорість і цілісність.
- Безпека: використання криптографічних методів захисту підвищує рівень безпеки

Використання смарт-контрактів може закрити суттєву кількість задач, що потребують автоматизації, тим самим підвищити швидкість взаємодії з системою, її ефективність та рівень безпеки. Також, одна з ключових особливостей – фіксація всіх дій, а отже ще досягається прозорість роботи системи, що є важливо і корисно для аудиту.

2.1.5 Перспективи використання блокчейн-технологій

Наразі, блокчейн-технології займають достатній обсяг на світовому ринку, адже їх можна використовувати як забезпечення надійності і цілісності обміну даних в багатьох сферах [1]: від IoT до сфери охорони здоров’я. Світова спільнота суцільно підтримує і визнає потенціал блокчейну.

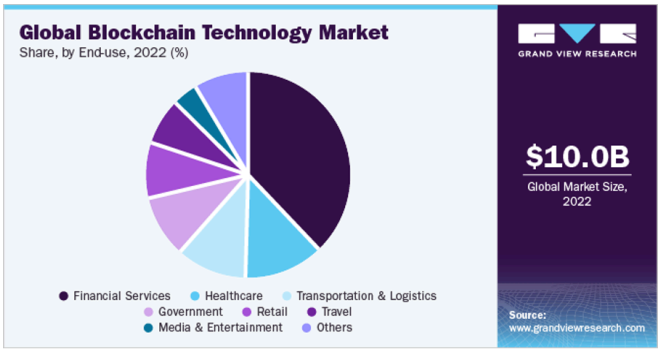

Рисунок 2.2 – Глобальний ринок блокчейн-технологій

Наприклад, типовими проблемами світової логістики є відсутність прозорості на багатоетапних процесах доставки грузів. Тож, останнім часом, тенденція інтеграції блокчейн-технологій в системи логістики тільки зростає [4] : корпорація IBM на базі IBM Blockchain [5] створила систему IBM Food Trust, основною задачею якої є забезпечення прозорості і аудит ланцюга постачання продуктів харчування. Сервіс зберігає реєстр даних про понад 1 млн. продуктів харчування, таких як: походження продуктів, інформація про статус транспортування, поточний стан і т.д. Важливо, IBM повідомили, що використання блокчейн-технологій в рамках їхньої платформи зменшило витрати в середньому на 80%, що підтверджує ефективність технології і в економічному плані. Блокчейн-технології також можуть широко використовуватись в сфері охорони здоров'я, де зберігання цілісності даних є життєво важливим процесом. Також, переваги блокчейна в області перевірки права власності на інформацію також забезпечують певні перспективи у цій сфері. Серед прикладів залучення технології в реаліях, можна виділити співпрацю уряду Естонії та технологічної компанії Guardtime, результат якої – розгортання загальнонаціональної платформи на основі блокчейну для підтвердження особистих даних пацієнтів та їх захисту. До речі, наразі їхня співпраця не тільки зберігається, а і розвивається в різноманітні напрямки, від створення проектів що перевіряють дані на предмет маніпуляції, до покращення можливостей кібербезпеки ESA [6].

2.2 Методика дотримання протоколу CoC

2.2.1 Суть дотримання протоколу CoC

Як було зазначено раніше, протокол Chain of Custody – це хронологічна документація, в якій фіксується весь життєвий цикл даних. Це важливий процес в комп'ютерній криміналістиці, що гарантує цілісність і надійність доказів:

Основні компоненти:

- **Збір**: процес починається з ідентифікації та збору всіх потенційних цифрових доказів з місця злочину. Це включає створення дублікатів оригінальних даних за допомогою судово-медичних інструментів, щоб уникнути їх зміни

- **Збереження**: важливо зберігати цілісність доказів. Це включає документування кожної дії, здійсненої над доказами, включаючи, хто з ними працював, коли і з якою метою.
- **Контроль та документування**: підтримання суворого контролю над тим, хто має доступ до доказів, і документування кожної передачі та дослідження забезпечує чіткий аудиторський слід..

В загальному випадку процедура виглядатиме як на рисунку 2.3.

Рисунок 2.3 – Дотримання протоколу CoC в загальному вигляді

При первинному контакті, перший реагуючий збирає докази, документує процес збору, включаючи дату, час і залучених осіб. Далі, докази транспортуються до судово-медичної лабораторії для аналізу. Дослідження і аналіз проводять судові аналітики, клон для розслідування [22], зберігаючи оригінал, цей процес також ретельно документується. Під кінець процедури, генерується комплексний звіт, що детально описує використані судово-медичні методи, проведений аналіз та результати. Цей звіт включає документацію CoC, щоб підтвердити цілісність доказів протягом всього їх життєвого циклу. Документація CoC має бути повною і безперервною для прийняття в суді. Будь-які невідповідності або нестача інформації можуть призвести до виклику доказів і їхнього можливого відхилення.

Дотримання таких процедур і принципів допоможе забезпечити *правову прийнятність* (якщо виявлено що протокол не дотримувався, суд може відхилити доказ і тим самим змінити результат судового процесу), *збереження довіри до доказів*, *захист від фальсифікацій*.

2.2.2 Технологічні інструменти та методи

Для забезпечення дотримання протоколу у сфері цифрової криміналістики зазвичай використовуються спеціалізовані технологічні інструменти та методи, які гарантують цілісність, автентичність і надійність цифрових доказів:

- Спеціалізоване програмне забезпечення для управління CoC

Програмні системи, такі як Forensic Toolkit (FTK) та EnCase [27], автоматизують процес документування всіх дій з цифровими доказами. Вони дозволяють відслідковувати кожну зміну, зберігаючи детальні журнали операцій, що забезпечує прозорість та підзвітність. Ці системи також підтримують створення хеш-кодів для кожного файлу, що дозволяє виявляти будь-які несанкціоновані зміни у даних.

- Методи хешування

  Використання хеш-функцій, таких як SHA-256 для генерації унікального коду для кожного файлу, який змінюється при будь-якій модифікації даних, що дозволяє виявляти та попереджати несанкціоновані втручання.

- Криптографія та шифрування

  Шифрування даних за допомогою алгоритмів, таких як AES, забезпечує захист цифрових доказів від несанкціонованого доступу. Шифрування гарантує, що дані можуть бути прочитані лише авторизованими користувачами, які мають відповідні ключі доступу. Використання MFA додає додатковий рівень безпеки, знижуючи ризики компрометації даних.

- Резервне копіювання та відновлення даних

  Регулярне створення резервних копій та збереження копій у різних географічних місцях, забезпечує додатковий захист. Процедури відновлення даних повинні бути чітко документовані та регулярно перевірятися для забезпечення їхньої ефективності у разі необхідності.

- Контроль доступу та аудиторський слід

  Використання систем контролю доступу, які обмежують можливість доступу до цифрових доказів лише уповноваженим особам. Це включає фізичні заходи безпеки, такі як захищені серверні кімнати, та логічні заходи, такі як управління правами доступу. Ведення аудиторських слідів дозволяє документувати всі дії з даними, що сприяє підтримці цілісності доказів та забезпечує можливість ретроспективного аналізу всіх операцій.

Застосування передових технологічних інструментів та методів є невід'ємною складовою успішного дотримання протоколу CoC у цифровій криміналістиці.

2.2.3 Правові аспекти і значення CoC

Правові аспекти та значення протоколу CoC у цифровій криміналістиці мають критичне значення для забезпечення прийнятності цифрових доказів у судових процесах:

- *Правові вимоги*: для того, щоб цифрові докази були прийнятними у суді, вони повинні відповідати встановленим правовим стандартам та протоколам. Протокол CoC забезпечує документування кожного етапу збору, зберігання, передачі та аналізу доказів, що є обов'язковим для підтвердження їхньої достовірності. Будь-яке порушення CoC може призвести до відхилення доказів у суді, що може значно вплинути на результат судового процесу.

- *Забезпечення цілісності та автентичності:* CoC включає методи, які гарантують, що зібрані дані залишаються незмінними від моменту їх збирання до представлення у суді. Це включає використання хешування та шифрування для підтвердження цілісності даних. Підтримка детальної документації всіх маніпуляцій з доказами допомагає забезпечити прозорість та можливість перевірки їхнього походження та обробки.

- *Правова прийнятність доказів*: судові органи вимагають чіткої документації всіх дій з доказами, щоб виключити можливість їх підробки або несанкціонованого доступу. У разі недотримання CoC, захист може оскаржити правомірність використання таких доказів, що може призвести до їх виключення з розгляду.

- *Міжнародні стандарти та співпраця*: міжнародні організації (детальніше розглянуто в пункті 2.2.4), розробляють стандарти та рекомендації для забезпечення єдиного підходу до зберігання та обробки цифрових доказів у різних країнах. Це сприяє міжнародній співпраці та обміну доказами між правоохоронними органами. Впровадження міжнародних стандартів допомагає узгоджувати процеси та підходи, що підвищує ефективність та правову захищеність цифрових доказів на глобальному рівні.

- *Значення CoC у судових процесах*: дотримання CoC є основою для забезпечення справедливості у судових процесах, оскільки воно гарантує, що ці файли можуть бути використані в якості доказів. Це особливо важливо

у випадках, де цифрові докази можуть бути вирішальними для винесення вироку. Судова практика показує, що ретельне дотримання CoC допомагає уникнути оскарження доказів та забезпечує їхнє прийняття у суді, що сприяє встановленню істини та справедливості.

Таким чином, правові аспекти та значення протоколу Chain of Custody є фундаментальними для забезпечення надійності та прийнятності цифрових доказів у судових процесах. Вони включають суворе дотримання документальних процедур, використання технологічних інструментів для захисту даних та узгодження з міжнародними стандартами.

2.2.4 Підходи до дотримання протоколів CoC

Дотримання протоколу CoC є глобальним стандартом, і базується на загальноприйнятих рекомендаціях міжнародних організацій та передових технологій. Ці підходи гарантують цілісність, автентичність та прийнятність цифрових доказів у судових процесах.

Рекомендації розроблені Федеральним Бюро Розслідувань США (FBI) :

- **Ідентифікація доказів**: кожен цифровий доказ повинен бути належним чином ідентифікований та задокументований з моменту його збору. Це включає опис об'єкта, умови та обставини його виявлення, а також хронологію подій з моменту його збору до передачі у суд.

- **Ведення повного журналу**: журналізація всіх дій з доказом є обов'язковою. Цей журнал повинен містити інформацію про те, коли і ким доказ був зібраний, збережений, переданий та аналізований. Це дозволяє відстежити історію доказу і гарантує його цілісність (FBI, Digital Evidence Policy, source).

- **Збереження цілісності**: для перевірки того, що цифрові дані не були змінені після їх збору, застосовуються методи хешування. Використання хеш-функцій, таких як SHA-256, дозволяє підтвердити незмінність даних.

- **Захист від несанкціонованого доступу**: використання заходів безпеки, таких як фізичне блокування місць зберігання та шифрування даних, для запобігання несанкціонованому доступу або маніпуляції з доказами. Це включає застосування багатоетапної автентифікації та контролю доступу.

Рекомендації від Національного інститут стандартів і технологій США (NIST):

- **Стандартизація процесів**: NIST розробляє та поширює стандарти та керівництва, що визначають найкращі практики для збору, зберігання та аналізу цифрових доказів. Це включає детальні протоколи для обробки та зберігання цифрових даних, що гарантують їх цілісність та автентичність [23].

- **Хешування та верифікація**: NIST рекомендує використовувати хеш-функції для верифікації цілісності цифрових доказів. Використання таких алгоритмів, як SHA-1, SHA-256, забезпечує точну перевірку незмінності даних з моменту їх збору до передачі у суд [21].

- **Ведення документації**: Подібно до рекомендацій FBI, NIST наголошує на важливості ведення детальної документації всіх дій з цифровими доказами. Це включає журналізацію всіх етапів роботи з доказами, від збору до аналізу та зберігання [23].

- **Захист від несанкціонованого доступу**: Впровадження заходів фізичної та логічної безпеки для захисту цифрових доказів. Це включає використання шифрування, багаторівневого контролю доступу та інших методів захисту даних [24].

Окрім рекомендацій FBI та NIST, існують й інші авторитетні підходи, що застосовуються у різних країнах та організаціях:

- Міжнародна організація кримінальної поліції (INTERPOL) надає глобальні керівництва для цифрових криміналістів. Це включає рекомендації щодо збору, зберігання та аналізу електронних доказів, а також встановлення та управління лабораторіями цифрової криміналістики [25].
- Європейське агентство правоохоронних органів (Europol) також розробляє керівництва та стандарти для збору та зберігання цифрових доказів. Їхні рекомендації спрямовані на забезпечення уніфікованого підходу до обробки цифрових доказів у всіх країнах-членах ЄС.

Світові підходи до дотримання протоколу Chain of Custody включають впровадження передових технологій, стандартизацію процесів, постійне навчання фахівців та використання спеціалізованого програмного забезпечення. Ці підходи,

базовані на рекомендаціях авторитетних організацій, таких як FBI, NIST, INTERPOL та Europol, допомагають забезпечити цілісність, автентичність та прийнятність цифрових доказів у судових процесах. Для детального ознайомлення рекомендується дослідити нормативні документи організацій щодо рекомендацій по обробці цифрових доказів і процесів комп’ютерної криміналістики.

Висновки до розділу 2

В цьому розділі, було детально розглянуто теоретичні аспекти функціонування блокчейну, приклади успішних реалізацій систем на основі блокчейн-технологій, що підтвердило перспективність напрямку. Також, було проведено ознайомлення з основними принципами дотримання протоколу CoC, а також розглянули питання правових аспектів, технологій, що використовуються для для дотримання протоколу та методиками, що рекомендують авторитетні міжнародні організації.

3 РОЗРОБКА ФРЕЙМВОРКУ СИСТЕМИ ЗБЕРІГАННЯ ЦИФРОВИХ ДОКАЗІВ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

В розділі «Розробка фреймворку системи зберігання цифрових доказів на основі блокчейн-технологій», на основі попереднього аналізу предметної області і висновків щодо потреби оновлення класичної системи зберігання і обробки цифрових доказів буде запропоновано новий фреймворк для забезпечення дотримання CoC. В цьому розділі описується архітектура запропонованого фреймворку, його особливості і процес моделювання в графовій базі даних.

3.1 Архітектура

3.1.1 Основні компоненти фреймворку

В рамках запропонованого фреймворку є основні компоненти, що є необхідними і достатніми:

- Приватний блокчейн на базі Ethereum

  Для основи, логічніше всього використовувати приватний блокчейн, так як через специфіку задачі нам необхідні затверджені вузли мережі. Приватний блокчейн дозволяє обмежити доступ до мережі від сторонніх користувачів, чим забезпечує бажаний рівень конфіденційності. Для реалізації бажано використовувати продукт Geth, що є клієнтом для налаштування приватної мережі від Ethereum

- Консенсусний алгоритм PoA

  Ефективним рішенням, в рамках фреймворку, буде використовувати алгоритм консенсусу PoA, особливостями якого є висока пропускна здатність (а швидкість обробки транзакції напряму впливає на швидкість отримання доступу або перевірки цілісності файлів), знижене енергоспоживання (економічно-вигідне рішення) та можливість надавати тільки авторитетним вузлам право валідації. Детальніше на схему роботи цього алгоритму можна ознайомитись на рисунку 3.1.

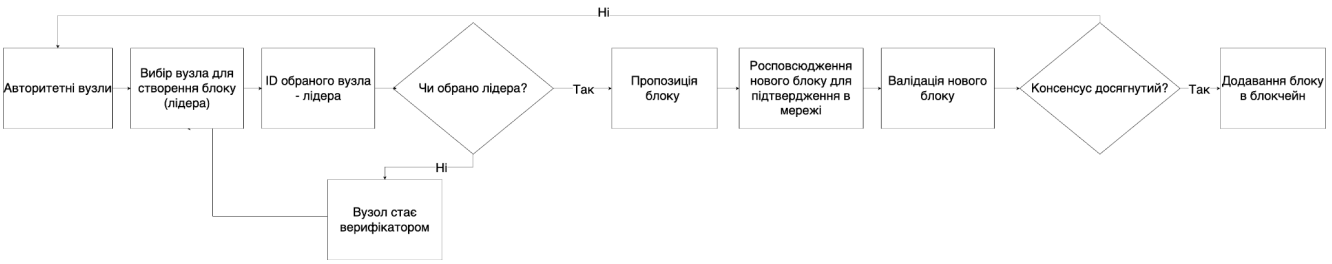

Рисунок 3.1 – Схема роботи консенсусного алгоритму PoA

- Смарт-контракти

  Вагома перевага використання Ethereum – смарт-контракти. Їх необхідно використовувати для автоматизації правами доступів, реєстрації, часових міток і зберігання хешів. Програмування смарт-контрактів відбувається на мові Solidity, зазвичай з використанням середовища Truffle для тестування і розробки.

- Децентралізоване сховище

  Так як використання блокчейну в якості сховища для великих за об’ємом даних, доцільно використовувати децентралізоване сховище поза межами системи, а блокчейн використовувати для збереження цілісності.

- Системи реєстрації і аутентифікації користувачів

  Необхідно використовувати сучасні і швидкі продукти для збору і трансформації в хеш біометричних даних.

- Інтерфейси користувача

  Також, необхідно інтегрувати сучасні та зручні веб-інтерфейси або мобільні додатки для взаємодії користувача з системою: реєстрація, отримання доступу, завантаження файлів, перевірка CoC тощо.

3.1.2 Взаємодія і залежності

Взаємодія і залежності між компонентами фреймворку забезпечують цілісність, безпеку та ефективність системи управління цифровими доказами. Приблизний опис цих взаємодій та залежностей нижче:

- Збір і аутентифікація даних

    - *Користувачі*: взаємодіють із системою через інтерфейси користувача для реєстрації та аутентифікації.
    - *Біометрична аутентифікація*: користувачі реєструються, використовуючи біометричні дані (такі як сітківка ока або відбитки пальців), які перетворюються в унікальні ID за допомогою криптографічно-стійкого алгоритму SHA-256 і зберігаються в блокчейні за допомогою запрограмованих раніше смарт-контрактів.
    - *Смарт-контракти*: автоматично перевіряють ID при кожній взаємодії користувача з системою

- Завантаження та обробка файлів

    - *Завантаження файлів*: користувач завантажує файл через інтерфейс, який автоматично передає його до децентралізованого сховища.
    - *Генерація хешу*: система генерує хеш файлу за допомогою криптографічного алгоритму SHA-256, фіксує час завантаження у вигляді часової мітки та зберігає ці дані разом з ID користувача у блокчейні через запрограмований смарт-контракт.
    - *Децентралізоване сховище*: забезпечує надійне *зберігання* файлів, зберігаючи посилання на файли в блокчейні для забезпечення їхньої цілісності.

- Управління правами доступу

    - *Смарт-контракти:* використовуються для визначення прав доступу до файлів, базуючись на раніше сформульованій політиці доступів.
    - *Моніторинг дій:* всі дії користувачів (читання, редагування, передача) фіксуються в блокчейні, забезпечуючи прозорість і відстежуваність.

- Аудит та моніторинг

    - *Система аудиту*: регулярно проводить перевірку цілісності даних та фіксує всі зміни, забезпечуючи безпеку і надійність системи.
    - *Контроль доступу*: Система аудиту також перевіряє відповідність доступу користувачів до файлів згідно з визначеними ролями та політиками безпеки.

Візуалізацію цих процесів зображена на спрощеній схемі, яка є на рисунку 3.2.

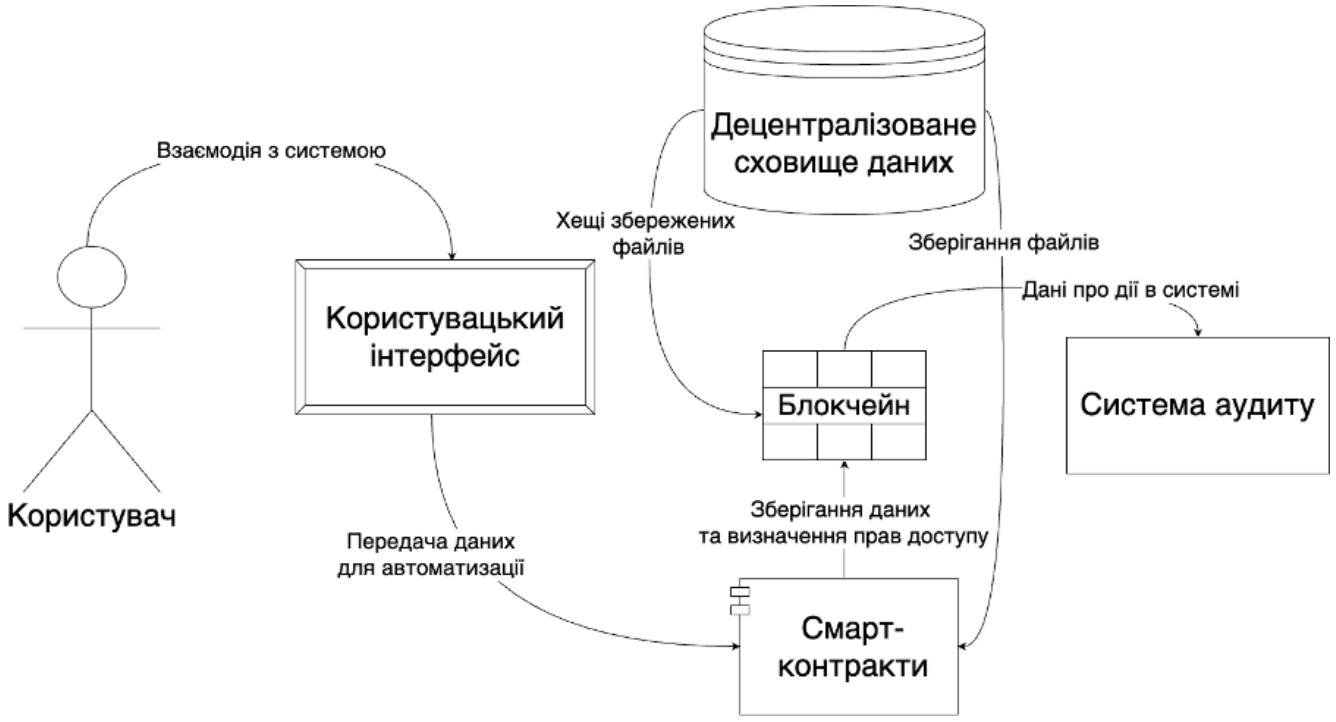

Рисунок 3.2 – Схема взаємодії в системі між компонентами

3.1.2 Розподіл доступу і структура мережі

Запропонований фреймворк доцільно використовувати в масштабі країни для правоохоронних інстанцій. Це включає централізовану координацію з боку адмініструючого вузла; регіональні вузли, що виступають «хабами» для місцевих правоохоронних органів і забезпечують зв’язок з адмініструючим вузлом і верифікують транзакції; місцеві вузли для збору даних і локальною початковою обробкою даних перед передачею до блокчейну.

В спрощеному вигляді процеси будуть виглядати так:

1) Слідчий на місцевому рівні збирає цифрові докази (наприклад, файли з камер спостереження) і завантажує їх у децентралізоване сховище через свій локальний вузол.
2) Хеші цих файлів автоматично створюються і зберігаються в блокчейні за допомогою смарт-контрактів. Ці смарт-контракти також записують часові мітки і ідентифікатори користувача.

3) Інші правоохоронні органи можуть отримати доступ до доказів, перевіряючи хеші через свої регіональні хаби. Доступ до цих даних контролюється за допомогою RBAC.
4) Дії з доказами записуються в блокчейні, забезпечуючи прозорість і можливість аудиту для перевірки дотримання протоколу Chain of Custody (CoC).

Така структура допомагає зберігати ключові аспекти безпеки цифрових доказів:

- *Прозорість*: всі дії з доказами записуються в блокчейні, що забезпечує високий рівень прозорості і довіри до системи.
- *Конфіденційність і цілісність*: використання сучасних криптографічних методів забезпечує високий рівень захисту даних.
- *Масштабованість*: архітектура системи дозволяє масштабувати мережу, додаючи нові вузли на регіональному та місцевому рівнях.
- *Ефективність*: автоматизація процесів за допомогою смарт-контрактів знижує ймовірність помилок і підвищує швидкість обробки даних.
- Швидкість доступу: структура дозволяє отримувати всю інформацію про дані в будь-яку частину мережі.

В приватних блокчейн-мережах, є можливість реалізувати динамічне управління доступом до транзакцій, наприклад за моделлю RBAC, що означає що можно самостійно встановлювати права доступу до транзакцій від конкретного вузла.

3.2 Процес реєстрації і аутентифікації користувачів

3.2.1 Методи ідентифікації

Для забезпечення надійної ідентифікації і реєстрації, найдоречніше буде використовувати сучасні методи збору і обробки ідентифікаційних даних користувачів. Основними джерелами можуть бути фізіологічні біометричні показники людини, такі як відбитки пальців, сітківка ока, скан обличчя на ін. Це буде знижувати ризики підробки або викрадення ідентифікаційних даних.

Так як, даний фреймворк пропонується для використання правоохоронними органами, проблема біометричної ідентифікації що полягає в потребі централізованої біометричної бази відпадає. Але, якщо використовувати в приватних інстанціях пропонується зібрати таку базу локально, користуючись даними суб’єктів, що будуть взаємодіяти з системою.

Наразі, є дебати щодо найбільш безпечної процедури ідентифікації шляхом використання біометричних показників, але розпізнавання райдужної оболонки ока, вважається, все ж одним з найкращим в цьому контексті. Райдужна оболонка ока унікальна, і відносно інших показників – стабільна.

3.2.2 Ідентифікація в рамках системи

Для забезпечення унікальності кожного користувача в системі, зібрані біометричні дані використовуються для генерації унікального ідентифікатора (ID) за допомогою криптографічного алгоритму SHA-256. Цей ідентифікатор є хешем від біометричних даних, що гарантує його унікальність та конфіденційність. За основу системи аутентифікації можна взяти таку [8] як на рисунку 3.3

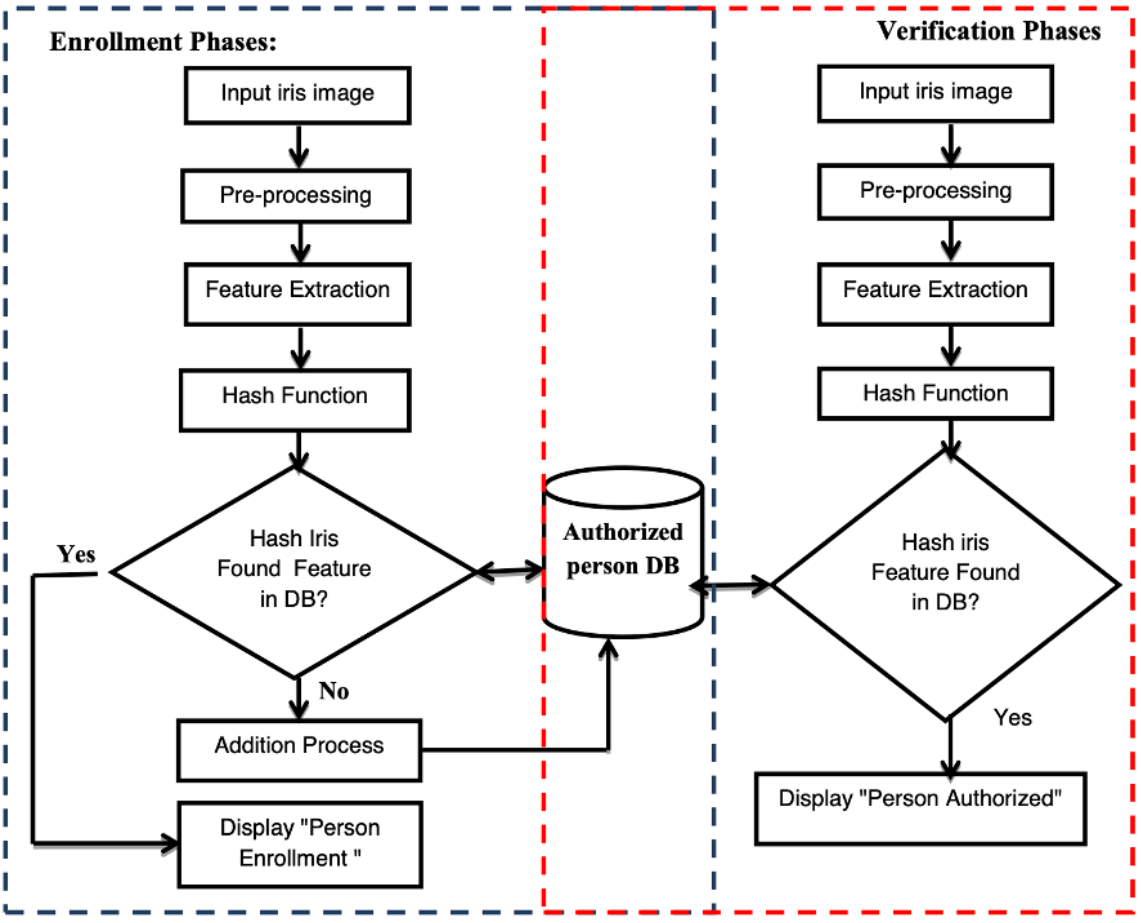

Рисунок 3.3 – Схема аутентифікаційної системи

Таким чином, ми отримуємо ідентифікатор, який використовується для всіх подальших користувача в рамках системи, включаючи доступ до файлів, підтвердження транзакцій та аудит дій. Це значення зберігається в блокчейні за

допомогою смарт-контракту, забезпечуючи незмінність та доступність ідентифікатора для подальшої верифікації користувача.

3.2.3 Смарт-контракти для автоматизованої реєстрації

Для автоматизації процесу реєстрації та забезпечення надійності даних використовуються смарт-контракти, розроблені на платформі Ethereum. Смарт-контракти дозволяють автоматизувати перевірку (рис 3.5) і збереження ідентифікаційних даних, а також управління правами доступу користувачів.

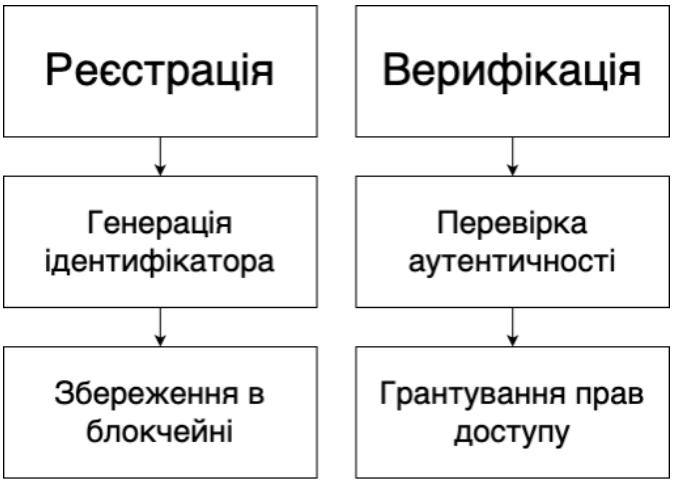

Рисунок 3.4 – Автоматизація процесів пов’язаних з реєстрацією і верифікацією

Перевагами такого підходу до реєстрації та ідентифікації користувачів є висока безпека та конфіденційність завдяки використанню біометричних даних і криптографічного хешування, що забезпечує надійний захист ідентифікаційних даних від підробки та викрадення.

Автоматизація процесів реєстрації та верифікації, за допомогою смарт-контрактів, дозволяє значно спростити управління користувачами, знижуючи ризик помилок і підвищуючи ефективність системи, відповідно блокчейн забезпечує незмінність та доступність ідентифікаційних даних, а також прозорість та можливість аудиту всіх дій користувачів, що підвищує довіру до системи та її надійність.

3.3 Процес завантаження і обробки файлів

Етап завантаження і обробки файлів можна назвати ключовим в рамках роботи, адже процеси, які відбуваються в рамках цього етапу, суттєво відрізняються від традиційних систем зберігання і обробки цифрових доказів, і допомагають виконувати протоколи CoC в належній мірі, зберігаючи головні характеристики цифрових доказів – цілісність і прозорість.

3.3.1 Процесс завантаження

Процес завантаження файлів відбувається поетапно:

1) Ідентифікація користувача за допомогою інтегрованої системи збору і хешування біометричних даних.

2) Надання доступу шляхом порівняння хешу, з тим який зберігається в блокчейні смарт-контрактом

3) Отримання доступу до завантаження

4) Передача файлу

3.3.2 Генерація хешу

Генерація хешу файлу є важливим етапом для забезпечення його цілісності та автентичності. Хешування здійснюється двічі: локально перед завантаженням у децентралізоване сховище та безпосередньо у сховищі.

Локальне обчислення хешу використовується для первинної перевірки цілісності цифрового доказу. Після завантаження у сховище, генерується ідентифікатор вмісту файлу в *сховищі*. Після отримання двох хешів відбувається перевірка на відповідність, яка підтвердить цілісність цифрового доказу.

Для хешування рекомендовано використовувати алгоритм хешування SHA256

3.3.3 Структура блоку

Для забезпечення точного відстеження CoC, потрібно, щоб вміст блоків в мережі був необхідним і достатнім, а саме містити в собі: часову мітку, ідентифікатор вмісту файлу, ідентифікатор користувача, ідентифікатор файлу в сховищі. Блоки формуються автоматично за допомогою смарт-контракту, який до кожного запису проставляє мітку часу.

Тобто, на виході ми маємо блок даних наступного вигляду:

$$Block = \{H_{\text{local}}, ID, H_{\text{storage}}\} \tag{3.1}$$

де H – хеш, ID – ідентифікатор.

Після утворення блоку формується транзакція, під транзакцією мається на увазі запис в блокчейні, який пов'язує блок даних з певною дією (завантаження файлу). Далі, з використанням ЦП транзакція підписується приватним ключем системи, і тим самим гарантує що дані не були змінені після підпису. Підписана транзакція надалі надходить до блокчейну для подальшої валідації, шляхом виклику спеціальних функцій що передають її до мережі вузлів. Далі, відбувається валідація транзакції авторитетними вузлами мережі, що використовують алгоритм PoA (деталі описані в пункті 3.2.1): вузли виконують криптографічну перевірку підпису транзакції за допомогою публічного ключа та відповідність даних в блоці. Після успішної валідації блок, що включає хеш попереднього блоку (виконання зв'язності і незмінності ланцюга) додається до блокчейну разом з часовою міткою, що автоматично фіксується в цей момент (рис. 3.5).

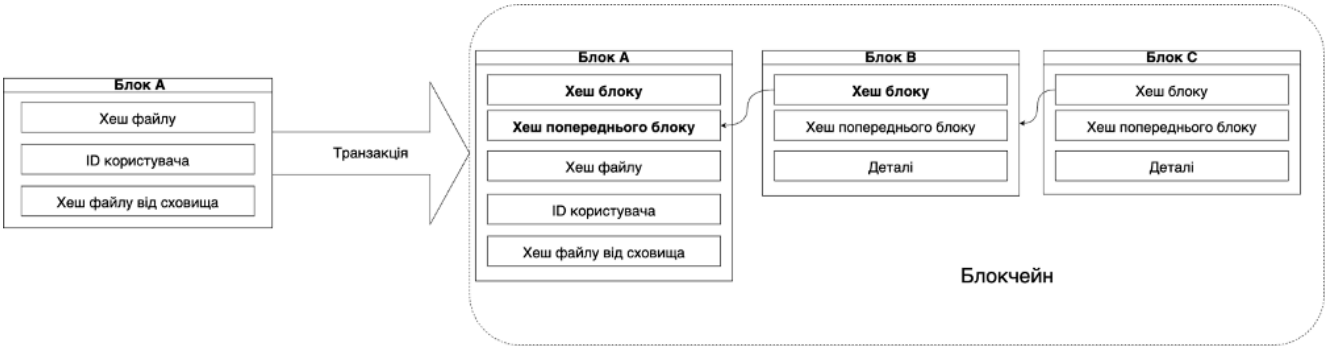

Рисунок 3.5 – Вміст і відправка блоку до блокчейну

Така послідовність дій і використання даних алгоритмів, допомагає зберегти цілісність завантажених файлів, в нашому випадку – цифрових доказів.

3.4 Використання децентралізованого сховища

Використання блокчейну як *сховища* для зберігання самих файлів (що, вірогідно, мають великі об’єми) не є ефективним, оскільки основне призначення блокчейн-технологій – децентралізоване зберігання невеликих обсягів даних, таких як транзакції і різного роду метадані. Кожен блок має обмежений розмір, який є непридатним для великих файлів. Також, зберігання великої кількості даних у блокчейні, очевидно, буде ресурсозатратно через вартість транзакцій, яка залежить від складності обчислень і даних, що передаються, а отже це – економічно не вигідно для організації. І наостанок, використання блокчейн-технологій в такому призначенні має проблеми з масштабованістю, адже кожен вузол мережі зберігає повну копію блокчейну, а це призводить до значного збільшення вимог щодо дискового простору і обчислювальної потужності, ставлячи під питання продуктивність системи.

Найдоречніше в цьому випадку буде використовувати децентралізовані сховища на кшталт IPFS, Storj, Sia і т.д. По-перше, воно використовує розподілену мережу вузлів для зберігання даних, що забезпечує високу стійкість до відмов. Дані розподіляються між багатьма вузлами, і навіть у випадку виходу з ладу одного або кількох вузлів дані залишаються доступними, що значно підвищує надійність і доступність системи. По-друге, дані в децентралізованих сховищах зазвичай шифруються перед зберіганням, що забезпечує їх захист від несанкціонованого доступу. Крім того, розподіл даних між багатьма вузлами ускладнює їх компрометацію, оскільки зловмиснику потрібно було б атакувати багато вузлів одночасно, щоб отримати доступ до повного набору даних. Третє, використання контентно-адресованого зберігання забезпечує цілісність даних, оскільки кожен файл отримує унікальний ідентифікатор, заснований на його вмісті, що дозволяє легко виявляти маніпуляції з даними. Нарешті, децентралізовані сховища можуть ефективно обробляти великі обсяги даних і легко масштабуються, додаючи нові вузли до мережі, що дозволяє системам зберігати великі обсяги даних без значного впливу на продуктивність.

Однак, в рамках роботи, цей компонент можна вважати як Black box, вхідними параметрами є цифрові докази, а вихідними – їхнє безпечне збереження.

Тому, припустимо використовувати не тільки централізовані сховища, а і традиційні, якщо це аргументовано.

3.5 Процеси управління і надання прав доступу

3.5.1 RBAC

RBAC –модель контролю доступу, що надає права доступу на основі ролей користувачів у системі. Вона дозволяє централізовано управляти доступом, призначаючи користувачам певні ролі, а потім надаючи доступ, на основі цих ролей. Це забезпечує високий рівень безпеки та гнучкості, оскільки дозволяє легко змінювати права доступу користувачів, змінюючи їхні ролі, без необхідності перепризначення доступу кожному користувачу окремо. Компоненти моделі включають у собі такі сутності: Ролі, Користувачі, Привілеї, Зв’язки. Існує думка [9], що саме політика на основі RBAC є найефективнішою стратегією підтримки дотримання федеральних, державних та місцевих законів і правил. Її структура полегшує управління доступом до конфіденційних даних та їх використання відповідно до нормативних та законодавчих вимог.

Рольове управління доступом має декілька ключових перевau. По-перше, його використання покращує рівень безпеки, значно знижуючи вплив людського фактору. По-друге, це спрощує дотримання стандартів, запобігаючи некоректний доступ. По-третє, зменшується об’єм роботи для адміністраторів системи, дозволяючи швидко змінювати привілеї для окремих суб’єктів. Проте, існують і недоліки. Адміністратор повинен мати глибоке бачення і розуміння операційної діяльності організації, що займає багато часу. Крім цього, така модель може бути не гнучка, у випадках непередбачених потреб у доступі за рамками встановленої політики.

Необхідно зауважити, що при впровадженні схожої моделі доступів, один з найголовніших етапів це чітке визначення ролей в рамках інстанції.

Розглянемо тривіальний приклад застосування RBAC в сфері криміналістики. Нехай у нас визначені ролі: Адміністратор (повний доступ до всіх ресурсів і управління ролями), Слідчий (доступ до завантаження і перегляду файлів), Аналітик (доступ до аналізу файлів, немає доступу до редагування і завантаження), Оперативник (має обмежений доступ до певних типів файлів). Тоді, взаємодія в рамках RBAC буде приблизно такого вигляду: Адміністратор

призначає ролі користувачам на основі посадових обов’язків (наприклад, за допомогою смарт-контрактів), кожна роль має чітко визначені права доступу. При спробі отримання доступу до певного ресурсу, система перевіряє його роль і визначає чи є необхідні права для отримання доступу, якщо користувач має необхідні права – система надає доступ, в протилежному випадку – відмова.

Рекомендовані кроки [9], яких треба дотримуватись при впровадженні на практиці наведені нижче:

1) Визначення даних і ресурсів що потребують контрольованого доступу;

2) Аналіз штабу, визначення функцій і обов’язків для формування ролей;

3) Зіставлення ролей з вимогами доступу;

4) Тренінги персоналу за тематикою принципів і заходів безпеки для RBAC.

Виконання цих етапів забезпечує коректне функціонування політики безпеки і стане ефективним рішенням для поточних обставин.

3.5.2 Смарт-контракти для управління і грантування доступів

В межах процесів отримання доступів в системі, програмування смарт-контрактів повинно буде чітко побудованим процесом з раніше визначеними вимогам таким як: безпека, прозорість, автоматизація; або деталізованим специфічним вимогам згідно політики безпеки.

Процес управління доступом з використанням смарт-контрактів (рис 3.7):

- Створення і налаштування смарт-контрактів

  На початковому етапі необхідно запрограмувати смарт-контракти, які будуть містити в собі всі ролі, права доступу і правила визначення ролей. Це все розгортається в блокчейні, забезпечуючи їхню незмінність і доступність для всіх учасників системи.

- Призначення ролей

  При реєстрації користувача в системі, йому призачається відповідна роль. Це може бути виконано вручну адміністратором, або автоматично, на основі заздалегідь визначених правил згідно вимогам організації. Інформація про призначену роль повинна зберігатись в смарт-контракті.

- Запит на доступ

  При спробі отримання доступу до певного ресурса або виконання деякої дії, надсилається запит до смарт-контракту. Запит містить ідентифікатор користувача та системний ідентифікатор запитуваного ресурсу.

- Перевірка прав доступу

  Смарт-контракт перевіряє користувача, що надіслав доступ, на існування необхідних прав для цього.

- Надання доступу

  Якщо умови доступу задовольняються, користувачу надається доступ (це може включати доступ на перегляд, завантаження, редагування та ін.).

- Логування

  Всі дії, що пов’язані з доступом, автоматично логуються в блокчейні. Це дозволяє відслідкувати всі дії і зміни, забезпечуючи можливість аудиту і проводження розслідування у випадку виникнення інцидентів.

Рисунок 3.6 – Процес управління доступом смарт-контрактами

Смарт-контракти дозволяють централізовано управляти ролями та правами доступу користувачів, автоматично перевіряти і надавати доступ до ресурсів на основі визначених правил. Це робить систему більш ефективною і надійною, що є важливим для збереження цілісності цифрових доказів у правоохоронних органах.

3.5.3 Отримання прав доступу

Підсумовуючи з попередніх пунктів опису управління і отримання доступу, цей процес ґрунтується на призначенні ролей відповідно RBAC і використанням смарт-контрактів для автоматизації і взаємодії з блокчейном. Високорівневі етапи взаємодії системи і користувача щодо отримання прав доступу в системі до певного ресурсу або дії зображені на діаграмі на рисунку 3.7.

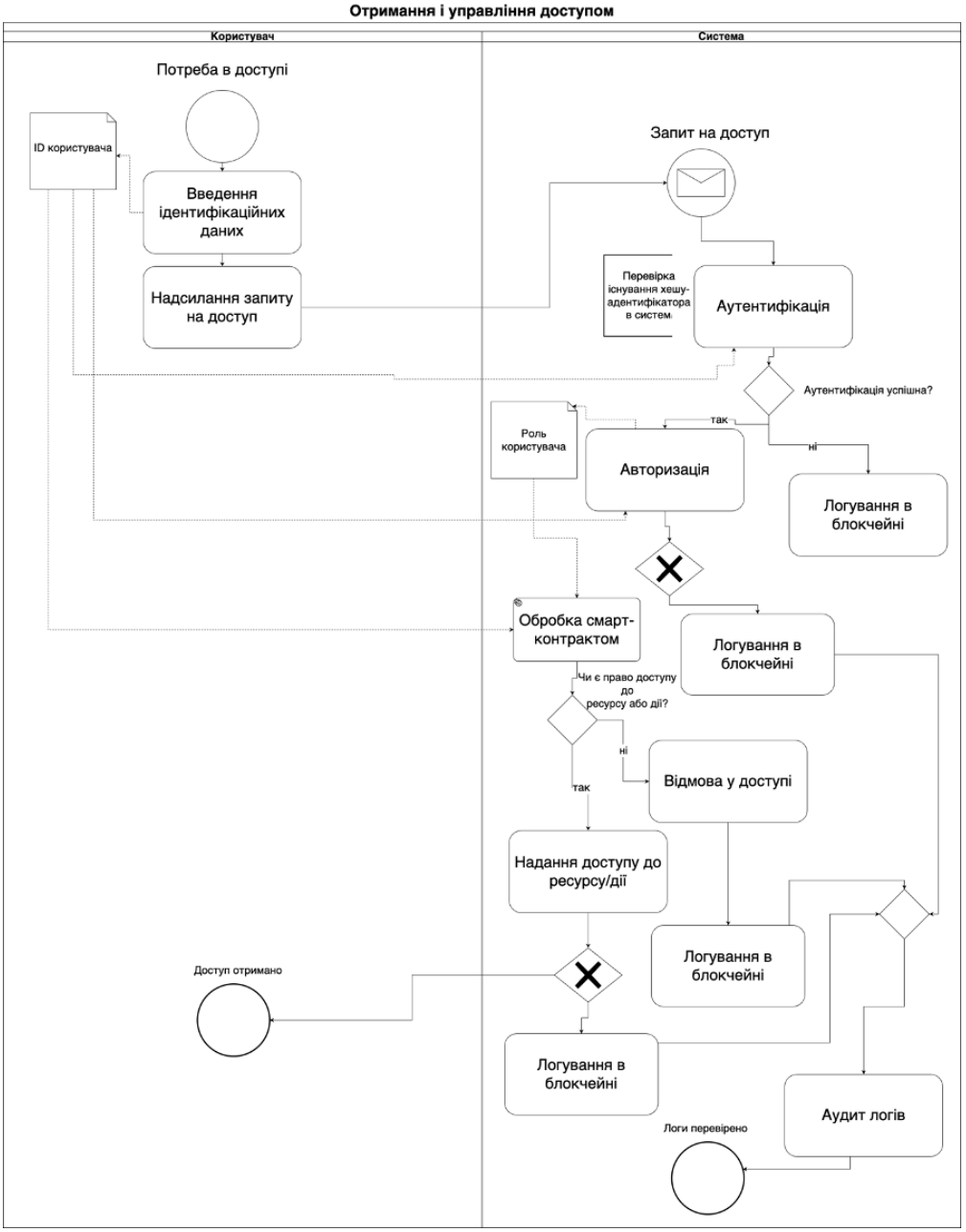

Рисунок 3.7 – Діаграма отримання доступу

3.6 Можливості аудиту в рамках міжнародних стандартів

Так як, управління цифровими доказами є критичним аспектом сучасної криміналістики, необхідно, щоб створена система забезпечувала цілісність, аутентичність і прозорість обробки цифрових доказів при дотриманні правових і етичних вже встановлених норм. В запропонованому фреймворку забезпечується надійний механізм аудиту в перспективі.

Аудит в контексті CoC дає можливість ретроспективного аналізу всіх операцій по обробці цифрових доказів, що включає реєстрацію, зберігання, доступ і т.д. Всі дії повинні бути прозорими і доступними для перевірки відповідним органам для гарантії, що дані не піддавались компрометаціям. Основний компонент архітектури фреймворку – блокчейн-технології, і саме тут логуються всі дії, що пов’язані з обробкою доказів, а завдяки особливостям концепту блокчейн – всі записи залишаються незмінними і прозорими для слідкування. В більшості документації стандартів і відомих практик існують настанови щодо збору, ідентифікації і обробки цифрових доказів; наприклад ISO/IEC 27037:2012, FBI Digital Evidence Policy, NIST Special Publication 800-86; основні критерії стосуються саме прозорості і відслідковуваності, що означає що ідея запропонованої системи повністю цьому відповідає. Наступною перевагою використання такої системи в контексті аудиту, є майже повна автоматизація процесів за допомогою смарт-контрактів, що знижує рівень ризику людських помилок, що є одним з основних ризиків після огляду проблем традиційних методів.

Ініціація аудиту відбувається за участі уповноваженої особи через інтерфейс системи. Система збирає всі лог-файли, що були записані в блокчейні, які відносяться до запитуваних доказів. Аудитор проводить аналіз записів згідно встановленого регламенту: це може бути перевірка часових місток, ідентифікатори користувачів що пов’язані з доказами, деталі проведених і спроб проведення операцій для виявлення аномалій або спроби маніпуляції. На завершенні створюється відповідний звіт з висновками і рекомендаціями по роботі з цифровими доказами для майбутнього покращення ефективності системи. Зауважимо, що аудити – це превентивний захід, практикувати який потрібно регулярно задля виявлення проблем роботи системи і потреби оновлення.

3.7 Моделювання фреймворку в графовій базі даних

3.7.1 Створення моделі

Для моделювання будемо використовувати сервіс графової системи управління БД з відкритим сурс-кодом базований на Java – Neo4j. Такий сервіс підходить для даних взаємопов’язаних елементів, таких як користувачі, файли, доступи і т.д. Графова структура допоможе візуалізувати ці структури, що дасть глибше розуміння будови системи.

Для створення *прикладу* моделі ми будемо використовувати декларативну мову запитів Cipher, що надасть зручну взаємодію з сервісом. Наш граф буде містити кілька типів вузлів та зв'язків, кожен з яких відповідає конкретним сутностям і взаємодіям у системі.

Типи вузлів:

- *User* (користувач) з властивостями: id (ідентифікатор), name (ім’я), role (роль користувача в системі), accessRights (права доступу).
- *File* (файл) з властивостями: id (ідентифікатор), hash (хеш файлу), uploadTimestamp (часова мітка), type (тип), description (опис),storageHash (хеш сховища).
- *Blockchain* (блокчейн) з властивостями: id (ідентифікатор), description (опис).
- *Block* (блок) з властивостями: id (ідентифікатор), prevHash (хеш попереднього блоку), hash (хеш блоку), fileHash (хеш файлу або дії що логується), userId (id користувача), storageHash (хеш файлу в схвоищі), timestamp (часова мітка).
- *Smart-contract* (смарт-контракт) з властивостями: id (ідентифікатор), code (код), role (роль).
- *DecentralizedStorage* (децентралізоване сховище) з властивостями: id (ідентифікатор), location (локація), description (опис).
- *UserInterface* (інтерфейс користувача) з властивостями: id (ідентифікатор), type (тип інтерфейсу), description (опис).

Типи зв’язків:

- *USES* (використовує): користувач взаємодіє з інтерфейсом користувача для доступу до системи.

- *CALLS* (викликається): інтерфейс користувача викликає смарт-контракт для виконання певних дій (наприклад, реєстрація або завантаження файлів).
- *REGISTERS* (реєструється): смарт-контракт реєструє нового користувача в системі.
- *CREATES* (створює): смарт-контракт створює новий блок, який містить інформацію про певну дію (наприклад, реєстрація користувача або завантаження файлу).
- *STORED_IN* (зберігається в): блок зберігається в блокчейні або файл зберігається у децентралізованому сховищі.
- *UPLOADS_VIA* (завантажує через): користувач завантажує файл через смарт-контракт, який обробляє завантаження.
- *CONTAINS* (містить): блок містить посилання на файл, забезпечуючи відстеження файлів у блокчейні.
- *HAS_ACCESS* (має доступ): користувач має доступ до певного файлу, що визначає його права на перегляд або зміну файлу.
- *EXECUTES* (виконує): користувач виконує смарт-контракт для виконання певних дій у системі (наприклад, реєстрація або завантаження файлів)

Визначивши основні компоненти графу, і написавши відповідні запити для обробки Neo4j (код прикладений в додатку А) ми отримуємо граф, який зображено на рисунку 3.8.

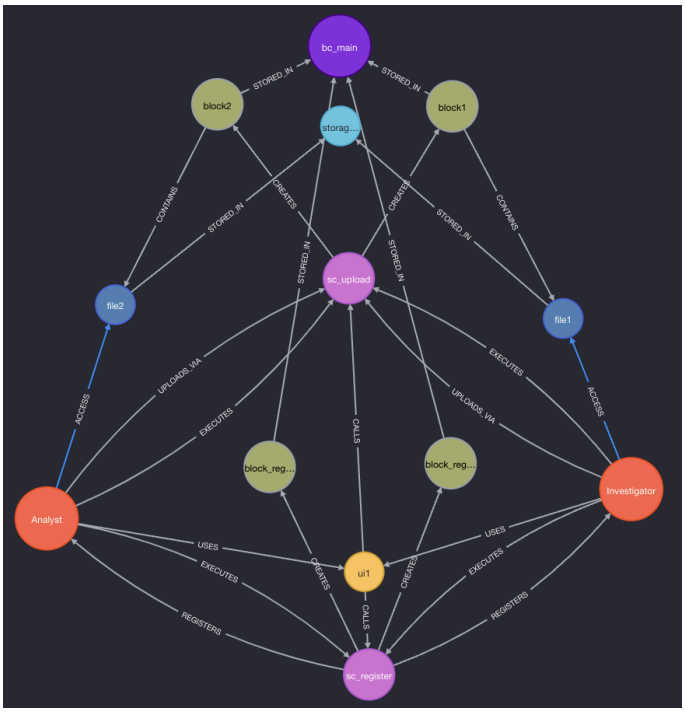

Рисунок 3.8 – Приклад фреймворку у вигляді графу

Виходячи з того що бачимо на графі, ми отримали модель спрощеної структури взаємодії між різними компонентами фреймворку для зберігання цифрових доказів на основі блокчейн-технологій. Ми бачимо взаємодію між різними компонентами системи, включаючи користувачів, інтерфейс користувача, смарт-контракти, файли, децентралізоване сховище та блокчейн.

- Користувачі (Investigator і Analyst): представлені червоними вузлами, вони взаємодіють з інтерфейсом користувача (USES), викликають смарт-контракти (EXECUTES), завантажують файл через смарт-контракт завантаження (UPLOADS_VIA) та мають доступ до свого файлу (HAS_ACCESS).
- Файли (file1 і file2): сині вузли представляють файли, які були завантажені користувачами. Кожен файл зберігається в децентралізованому сховищі (STORED_IN) та міститься в блоці блокчейну (CONTAINS)
- Блоки (block_register1, block_register2, block1, block2): зелені вузли представляють блоки блокчейну. Вони містять інформацію про реєстрацію користувачів та завантаження файлів і зберігаються в головному блокчейні (STORED_IN).
- Децентралізоване сховище (storage1): блакитний вузол представляє децентралізоване сховище (IPFS), де зберігаються файли (STORED_IN)
- Смарт-контракти (sc_register і sc_upload): фіолетові вузли представляють смарт-контракти, які виконуються користувачами (EXECUTES). Смарт-контракт реєстрації (sc_register) викликається інтерфейсом користувача (CALLS) для реєстрації нових користувачів та створює блоки реєстрації (CREATES). Смарт-контракт завантаження (sc_upload) викликається інтерфейсом користувача (CALLS) для завантаження файлів, створює блоки завантаження (CREATES) та зберігає їх в блокчейні (STORED_IN).
- Користувацькі інтерфейс (ui1): жовтий вузол представляє веб-інтерфейс, який використовується користувачами (USES) для взаємодії з системою та викликає смарт-контракти (CALLS)
- Блокчейн (Blockchain): фіолетовий вузол представляє головний блокчейн, де зберігаються всі блоки з інформацією про дії користувачів (STORED_IN)

На графі чітко відслідковується, як кожен компонент взаємодіє з іншими, що відображає структуру і функціональність фреймворку для зберігання цифрових доказів.

Висновки до розділу 3

Запропонований фреймворк для зберігання та обробки цифрових доказів на основі блокчейн-технологій забезпечує високий рівень безпеки, цілісності, прозорості та автоматизації процесів. Використання приватного блокчейну на базі Ethereum з алгоритмом консенсусу PoA дозволяє досягти високої пропускної здатності, зниженого енергоспоживання та конфіденційності. Смарт-контракти автоматизують процеси реєстрації, аутентифікації, управління правами доступу та аудиту, що значно знижує ризик людських помилок і забезпечує прозорість всіх операцій. Децентралізоване сховище даних забезпечує надійне зберігання великих обсягів даних, зберігаючи посилання на файли в блокчейні для перевірки цілісності. Використання біометричної аутентифікації підвищує рівень безпеки ідентифікаційних даних, а рольове управління доступом (RBAC) дозволяє гнучко керувати правами користувачів відповідно до їхніх обов’язків. Регулярні аудити, що проводяться за допомогою системи, гарантують відповідність встановленим стандартам та виявлення можливих аномалій або спроб маніпуляцій з цифровими доказами.

Таким чином, розроблений фреймворк забезпечує надійне, ефективне та безпечне управління цифровими доказами, що є критично важливим для правоохоронних органів і відповідає сучасним вимогам до зберігання та обробки конфіденційної інформації. Використання платформи Neo4j дозволило ефективно та лаконічно візуалізувати взаємодію між різними компонентами фреймворку, що дало змогу наочно проаналізувати структуру системи і функціонал.

4 ІМПЛЕМЕНТАЦІЯ

В розділі «Імплементація» показано результати взаємодії з графовим представленням фреймворку, описаного і змодельованого в попередніх розділах, а також розрахунок приблизної вартості реалізації і збереження запису враховуючи особливості системи. На завершення, додано загальні рекомендації щодо реалізації подібної системи.

4.1 Тестове застосування запропонованої моделі системи

Для демонстрації роботи, напишемо пару запитів для отримання деякої інформації. Результати виконання стандартних запитів зображені на рисунках 4.1 – 4.5.

Рисунок 4.1 – Блоки що зберігають інформацію про реєстрацію користувачів

Рисунок 4.2 – Перегляд блоків збережених в блокчейні

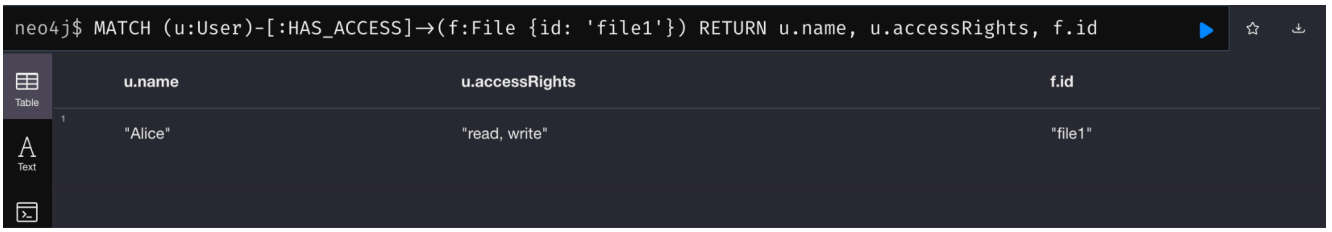

Рисунок 4.3 – Користувачі і їх доступ до файлів

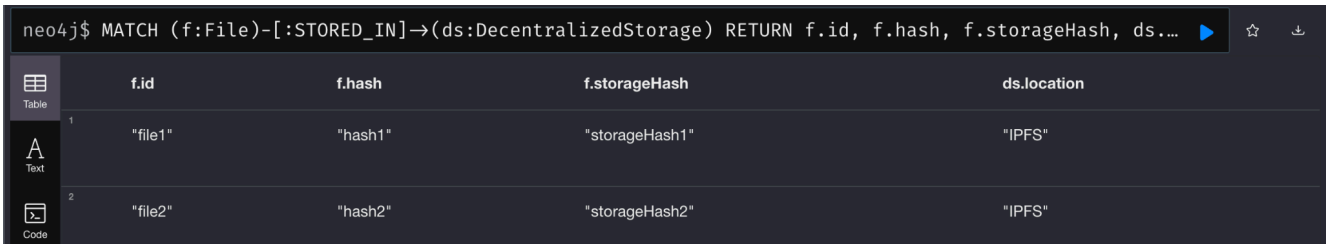

Рисунок 4.4 – Перегляд файлів збережених в сховищі

Рисунок 4.5 – Всі дії певного користувача

Для виконання запитів для демонстрації дій, пов’язаних з аудитом додамо певні зв’язки і вузли для збільшення інформативності:

- Вузол File:
  - id: 'file3', hash: 'anomaly', uploadTimestamp, type: 'document', description: 'Anomalous file'

    - id: 'file4', hash: 'hash4', uploadTimestamp, type: 'image', description: 'Regular file'
- Вузол Block:
    - id: 'block3', prevHash: 'blockHash2', hash: 'blockHash3', fileHash: 'anomaly', userId: 'hashAlice', storageHash: 'storageHash3', timestamp: 1685644800000
    - id: 'block4', prevHash: 'blockHash3', hash: 'blockHash4', fileHash: 'hash4', userId: 'hashBob', storageHash: 'storageHash4', timestamp: 1688133600000
- Зв’язок CONTAINS:
    - між блоком block3 та файлом file3
    - між блоком block4 та файлом file4
- Зв’язок VALIDATES:
    - між валідаційним вузлом validator1 та блоком block3
    - між валідаційним вузлом validator2 та блоком block4

Тепер відправимо запити щодо аудиту і безпеки. Результати зображені на рисунках 4.6. і 4.7.

Рисунок 4.6 – Перевірка цілісності за хешами

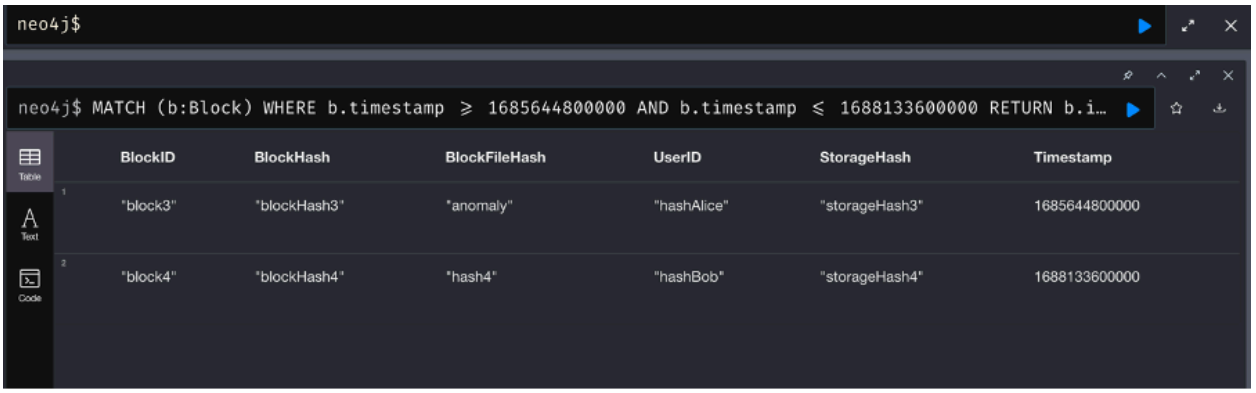

Рисунок 4.7 – Аудит дій користувачів за певний період

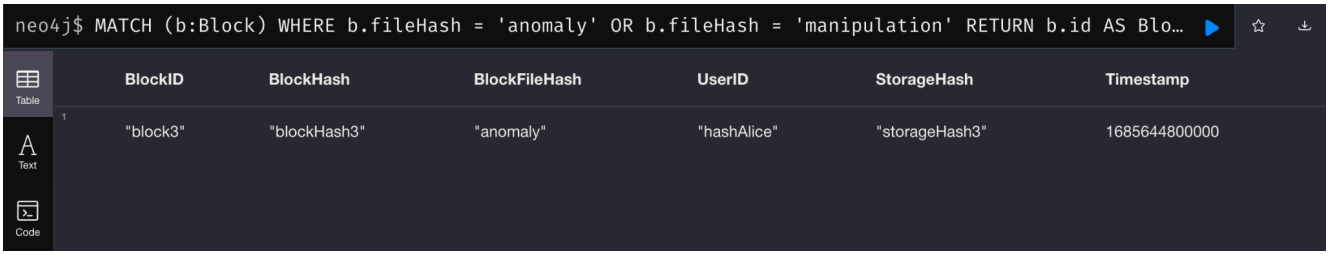

Рисунок 4.8 – Виявлення аномалій або спроб маніпуляцій за хешем.

В результаті спрощеного моделювання фреймворку для зберігання цифрових доказів на основі блокчейн-технологій у графовій базі даних Neo4j, ми можемо зробити певні висновки. Використання Neo4j дозволило ефективно візуалізувати складні взаємодії між користувачами, файлами, блоками, смарт-контрактами та децентралізованими сховищами, забезпечуючи глибше розуміння структури системи. Запити для перевірки хешів та аудиту дій за певний період продемонстрували можливість виявлення аномалій та маніпуляцій, що є критично важливим для підтримання надійності та безпеки системи.

4.2 Розрахунок вартості реалізації і зберігання

4.2.1 Вартість реалізації

Розрахувати точну вартість реалізації запропонованого фреймворку майже неможливо без вхідних даних. Проте, *загальну* формулу можна описати, виходячи з приблизних цін ринку і знання компонент. Розглянемо основні компоненти для виведення формули приблизної вартості реалізації (в формульному вигляді: C – вартість, T – час, V – об’єм):

- Інфраструктура блокчейну: розгортання приватного блокчейну на базі Ethereum і врахування інвестицій для АЗ для вузлів і відповідно ПЗ для обслуговування

$$C_{servers} + C_{config} + C_{support} \tag{4.1}$$

- Розробка ПЗ: включає розробку смарт-контрактів на Solidity, тестування і деплоймент; використання сучасних методів збору біометричних даних; розробка інтерфейсів

$$C_{dev} \times T_{dev} + C_{software} \tag{4.2}$$

- Децентралізоване сховище: передбачення плати за зберігання файлів великих об'ємів

$$C_{storing} \times V_{data} \tag{4.3}$$

- Адміністрування і підтримка: використання RBAC, розробка систем аудиту

$$C_{staff} \times T_{hours} \tag{4.4}$$

- Безпека: використання криптографічних алгоритмів

$$C_{cryptography} \tag{4.5}$$

- Навчання і підготовка персоналу

$$C_{training} \tag{4.6}$$

Тобто, грубо розрахована вартість елементарної реалізації буде становити суму всіх цих компонент, що наведені в формулах (4.1 - 4.6) відповідно:

$$C_{total} = (C_{servers} + C_{config} + C_{support}) + (C_{dev} \times T_{dev} + C_{software}) + (C_{storing} \times V_{data}) + (C_{staff} \times T_{hours}) + C_{cryptography} + C_{trainings} \tag{4.7}$$

Використання даної формули (4.7) допоможе зрозуміти, які основні витрати будуть враховані для реалізації.

Розраховувати на реальних даних наразі не буде інформативно, через варіативність цін в різних точках світу і певних особливостей ринку.

4.2.2 Вартість зберігання записів і транзакцій в межах блокчейну

Вартість зберігання запису – аспект, який необхідно враховувати при плануванні впровадження системи, так як це напряму впливає на економічну ефективність і продуктивність функціонування. Дані, що зберігаються в блоці, дублюються і поширюються на всі вузли в рамках мережі. Витрати на зберігання включають у собі обчислювальні ресурси для обробки і валідації транзакції, простір для зберігання даних на кожному вузлі мережі. У публічних блокчейнах, наприклад, Ethereum, вартість зберігання порівняно висока, адже, в такому випадку, існує необхідність підтримки дуже великої кількості вузлів і високу конкуренцію за ресурси. В нашому випадку, через те, що ми використовуємо блокчейн приватного типу – адміністрація може налаштувати параметри зберігання так, щоб була максимальна оптимізація витрат. Це дозволяє зберігати дані при мінімальних витратах.

Вартість самої транзакції в приватних блокчейнах встановлюється адміністратором мережі з урахуванням: налаштованої мінімальної вартості газу, кількості газу для кожної транзакції або смарт-контракту. В такій архітектурі надається налаштування параметрів газу для підвищення пропускної здатності і досягнення стабільності.

Приблизну вартість транзакції в блокчейні можна обчислити за формулою 4.8.

$$C_{transaction} = G \times P \tag{4.8}$$

де G – кількість газу, P – ціна за одиницю газу.

В якості прикладу, використаємо кількість газу 50 000, а ціну за одиницю мінімальну (що дозволяє приватний блокчейн) – 1 Gwei, переведемо в ETH і отримавши поточний курс ETH до USD отримаємо ціну в USD.

Тоді, при таких вхідних даних вартість транзакції буде становити:

$$C_{transaction} = 50\,000 \times 1 = 50\,000\,(\text{Gwei})$$

$$C_{transaction} = \frac{50\,000}{10^{-9}} = 0.00005\,(\text{ETH})$$

$$C_{transaction} = 0.00005 \times 3500 \approx 0.175\,(\text{USD})$$

На прикладі можна побачити, що завдяки правильно обраним компонентам під час моделюванні фреймворку ми отримуємо економічне вигідне рішення для потреб організації.

Отже, правильне налаштування параметрів зберігання і вартості транзакції забезпечить ефективне керування ресурсами і зменшить витрати на обслуговування.

4.3 Рекомендації щодо впровадження запропонованого фреймворку

Для правильного впровадження запропонованого фреймворку в реальну системи, є деякі загальні рекомендації:

- Оцінка потреб та вимог

  Перш ніж впроваджувати фреймворк, важливо провести детальний аналіз існуючих вимог організації (визначення основних цілей, ресурсів та очікувань від системи, специфічні вимог щодо безпеки, прозорості та масштабованості)

- Пілотний проект

  Реалізація пілотного проекту дозволить протестувати фреймворк в меншому масштабі і відразу виявити можливі труднощі, та знайти шляхи їх уникнення до повного розгортання.

- Вибір технологій та інструментів

  Для успішного впровадження важливо обрати відповідні технології та інструменти. В нашому випадку це буде Ethereum для реалізації блокчейну, PoA як консенсусний алгоритм, а також середовище для смарт-контрактів (наприклад, Truffle) [16].

- Безпека та захист даних

  Необхідно забезпечити захист даних на всіх етапах: від збирання та зберігання біометричних даних до збереження файлів у децентралізованому сховищі та записів у блокчейні [17][18]. Використання сучасних криптографічних методів, таких як хешування та цифрові підписи, є обов'язковим.

- Навчання персоналу

  Важливо провести навчання для всіх користувачів та адміністраторів системи. Персонал має розуміти принципи роботи фреймворку, вимоги безпеки та правильні процедури роботи з цифровими доказами. Це допоможе ще більше мінімізувати ризики, пов'язані з людським фактором.

- Моніторинг та аудит

  Після впровадження необхідно налагодити регулярний моніторинг та аудит системи. Це допоможе виявляти та виправляти потенційні проблеми, а також забезпечити відповідність встановленим стандартам та політикам безпеки [18]. Рекомендовано використовувати автоматизовані системи для збору та аналізу логів, що повністю відповідає концепту фреймворку.

- Підтримка та оновлення

  Після впровадження системи дуже важливо забезпечити її підтримку та регулярні оновлення.

- Документація та стандартизація

  Створення детальної документації є необхідним для успішного впровадження та подальшої експлуатації системи. Документація повинна включати опис архітектури, процесів, політик безпеки, а також інструкції для користувачів та адміністраторів. Важливо також дотримуватися міжнародних стандартів, таких як ISO/IEC 27037:2012, що забезпечують сумісність та узгодженість системи.

- Взаємодія з іншими системами

  Для забезпечення ефективного обміну даними та інтеграції з іншими системами, необхідно забезпечити сумісність фреймворку з існуючими системами правосуддя та правоохоронних органів. Це дозволить використовувати цифрові докази в судових процесах різних юрисдикцій.

- Оцінка економічної ефективності

  Це включає аналіз витрат на впровадження, підтримку та оновлення системи, а також оцінку економічної вигоди від покращення безпеки та ефективності обробки цифрових доказів.

Дотримання цих загальних рекомендацій допоможе ефективно імплементувати фреймворк в систему. Процес впровадження фреймворку починається з оцінки потреб та вимог організації, що включає визначення основних цілей, ресурсів та очікувань від системи. Проведення пілотного проекту дозволяє протестувати фреймворк на меншому масштабі, виявити можливі труднощі та адаптувати систему перед повним розгортанням. Вибір відповідних технологій та інструментів, таких як Ethereum для блокчейну, IPFS для децентралізованого зберігання даних та сучасних криптографічних методів для захисту даних, забезпечує надійність і ефективність системи. Захист даних на всіх етапах, від збору та зберігання біометричних даних до збереження файлів у децентралізованому сховищі та записів у блокчейні, є ключовим аспектом запропонованого фреймворку. Використання хешування та цифрових підписів гарантує високий рівень безпеки, запобігаючи несанкціонованому доступу та маніпуляціям з даними. Навчання персоналу щодо принципів роботи фреймворку, вимог безпеки та правильних процедур роботи з цифровими доказами допомагає мінімізувати ризики, пов'язані з людським фактором. Регулярний моніторинг та аудит системи забезпечують своєчасне виявлення та усунення потенційних проблем, а також підтримують відповідність встановленим стандартам та політикам безпеки. Використання автоматизованих систем для збору та аналізу логів сприяє прозорості та ефективності роботи фреймворку. Підтримка та регулярні оновлення системи є необхідними для забезпечення її актуальності та відповідності новим викликам і загрозам. Створення детальної документації, що включає опис архітектури, процесів, політик безпеки та інструкцій для користувачів та адміністраторів, є критично важливим для успішного впровадження та подальшої експлуатації системи. Дотримання міжнародних стандартів, таких як ISO/IEC 27037:2012 та NIST Special Publication 800-86, забезпечує сумісність та узгодженість фреймворку з існуючими системами правосуддя та правоохоронних органів, що дозволяє ефективно використовувати цифрові докази у судових процесах різних юрисдикцій. Оцінка економічної ефективності фреймворку включає аналіз витрат на впровадження, підтримку та оновлення системи, а також оцінку економічної вигоди від покращення безпеки та ефективності обробки цифрових доказів. Впровадження цього фреймворку сприятиме значному підвищенню безпеки, прозорості та економічної ефективності у зберіганні та обробці цифрових доказів, що є критично важливим для сучасної цифрової криміналістики.

Висновки до розділу 4

Заключний розділ роботи був присвячений моделюванню і імплементації фреймворку. Використання платформи Neo4j дозволило ефективно та лаконічно візуалізувати взаємодію між різними компонентами фреймворку, що дало змогу наочно проаналізувати структуру системи і функціонал. Приблизна вартості в зберігання показала що основна процесс що утворює економічної вигоду в використанні фреймворка – правильно налаштування всіх параметрів приватного блокчейну, адже це напряму впливає на використання ресурсів. Також були надані загальні рекомендації щодо впровадження фреймворку в реальну систему.

ВИСНОВКИ

В рамках роботи, було проведено аналіз предметної області та існуючих загроз компрометації цифрових доказів при використанні традиційних методів обробки і зберігання в комп'ютерній криміналістиці. Було виявлено, що основна вразливість систем збереження цілісності цифрових доказів і випадки порушення протоколу CoC – особи, що приймають участь в процесах обробки і аналізу даних і недосконаліть методів захисту; таким чином виникає необхідність в проведенні аналізу і тестів для нових інтеграцій для знаходження рішення і покращення глобального рівня кібербезпеки. Виходячи з зазначеного вище, випливає потреба в пропозиції варіанту покращення процесів існуючих алгоритмів дотримання протоколу CoC, які можуть призводити до неправильних судових вироків, що ставить під загрозу правосуддя і життя людей, шляхом використання нових технологій і практик.

В результаті проведеної роботи було отримано і змодельовано, у вигляді графу, концепт фреймворку на основі блокчейну, що може бути інтегрований в поточні системи зберігання і обробки цифрових доказів для збереження цілісності даних, дотримання протоколів CoC, прозорості всіх операцій, автоматизації і покращення можливостей аудиту. Були наведені детальні описи компонент фреймворку і їх зв'язок між собою, що дало зрозуміти ідеї і перспективи використання технології блокчейн в сфері криміналістики і судових процесів, де цілісність і відстеження є ключовими вимогами для доказів, щоб вважати їх дійсними. Для прикладу і покращення розуміння було створено спрощену модель концепції у вигляді графу, і відтворені запити, що показують можливості взаємодії з системою. Також, в результаті приблизної оцінки вартості реалізації і зберігання одного запису було зроблено висновки, що така реалізація такої системи може бути економічно вигідніше, порівняно з стандартними системи зберігання і обробки цифрових доказів, через використання приватного типу блокчейну і автоматизації більшості процесів. Також, були наведені загальні рекомендації щодо імплементації фреймворку.

ПЕРЕЛІК ДЖЕРЕЛ І ПОСИЛАНЬ

[1] Blockchain Technology Market Size, Share & Trends Analysis Report By Type, By Component, By Application, By Enterprise Size, By End-use, By Offering, By Region, And Segment Forecasts, 2024 - 2030: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

[2] Wikipedia: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B0_%D0%B3%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%8F

[4] DigitalForest: https://digiforest.io/blog/blockchain-in-logistics

[5] IBM: https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust

[6] InvestEstonia: https://investinestonia.com/how-the-worlds-leading-blockchain-company-guardtime-turns-trust-into-digital-truth-from-its-tallinn-office/

[8] Biometric Authentication Based on Hash Iris Features by Dalal N. Hammod https://www.slideshare.net/slideshow/biometric-authentication-based-on-hash-iris-features/239546728

[9] What is Role-Based Access Control: https://www.fortinet.com/resources/cyberglossary/role-based-access-control

[10] Chain of Custody https://www.geeksforgeeks.org/chain-of-custody-digital-forensics/

[11] Chain of custody and life cycle of digital evidence https://www.researchgate.net/publication/279175015_Chain_of_custody_and_life_cycle_of_digital_evidence

[12] Computer forensic https://www.cisa.gov/sites/default/files/publications/forensics.pdf

[14] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends

[15] Handbook of Forensic Services

https://www.fbi.gov/file-repository/handbook-of-forensic-services-pdf.pdf/view

[16] Truffle https://archive.trufflesuite.com/docs/

[17] ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.

[18] NIST Special Publication 800-86 – Guide to Integrating Forensic Techniques into Incident Response https://csrc.nist.gov/publications/detail/sp/800-86/final

[19] INTERPOL, Guidelines for Digital Forensics First Responders

[20] INTERPOL, Global Guidelines for Digital Forensics Laboratories

[21] NIST, Digital Evidence Preservation

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf

[22] Ensuring Digital Forensics Integrity: The Significance of Chain of Custody Cyber Security https://www.salvationdata.com/work-tips/chain-of-custody-cyber-security/

[23] NIST, Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[24] NIST, Guidelines on Mobile Device Forensics

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[25] INTERPOL, Global Guidelines for Digital Forensics Laboratories

[26] Europol, Digital Evidence and Forensics

[27] Garfinkel, S. (2010). Digital Forensics: Digital Evidence in Criminal Investigations. Springer.

ДОДАТОК А

Код, результат якого наведений в пункті 3.7:

```
// Створення двох користувачів
CREATE (u1:User {id: 'hashAlice', name: 'Alice', role: 'Investigator', accessRights: 'read, write'})
CREATE (u2:User {id: 'hashBob', name: 'Bob', role: 'Analyst', accessRights: 'read'})

// Створення одного інтерфейсу користувача
CREATE (ui:UserInterface {id: 'ui1', type: 'web', description: 'Web Interface for File Management'})

// Створення смарт-контрактів для реєстрації та завантаження файлів
CREATE (sc_register:SmartContract {id: 'sc_register', code: 'registration_code_here', role: 'admin'})
CREATE (sc_upload:SmartContract {id: 'sc_upload', code: 'upload_code_here', role: 'admin'})

// Створення децентралізованого сховища
CREATE (ds:DecentralizedStorage {id: 'storage1', location: 'IPFS', description: 'InterPlanetary File
System for image storage'})

// Створення блокчейн вузла для зберігання записів
CREATE (bc:Blockchain {id: 'bc_main', description: 'Main blockchain for storing system actions'})

// Зв'язки між користувачами та інтерфейсом
CREATE (u1)-[:USES]->(ui)
CREATE (u2)-[:USES]->(ui)

// Реєстрація користувачів за допомогою смарт-контракту через інтерфейс
CREATE (ui)-[:CALLS]->(sc_register)
CREATE (sc_register)-[:REGISTERS]->(u1)
CREATE (sc_register)-[:REGISTERS]->(u2)

// Запис про реєстрацію в блокчейні
CREATE (b_register1:Block {id: 'block_register1', prevHash: '0x0', hash: 'blockRegisterHash1', action:
'register', userId: 'hashAlice', timestamp: timestamp()})
CREATE (b_register2:Block {id: 'block_register2', prevHash: 'blockRegisterHash1', hash:
'blockRegisterHash2', action: 'register', userId: 'hashBob', timestamp: timestamp()})
CREATE (sc_register)-[:CREATES]->(b_register1)
CREATE (sc_register)-[:CREATES]->(b_register2)
CREATE (b_register1)-[:STORED_IN]->(bc)
CREATE (b_register2)-[:STORED_IN]->(bc)

// Завантаження файлів користувачами через інтерфейс за допомогою смарт-контракту
CREATE (ui)-[:CALLS]->(sc_upload)
CREATE (u1)-[:UPLOADS_VIA {timestamp: timestamp()}]->(sc_upload)
CREATE (u2)-[:UPLOADS_VIA {timestamp: timestamp()}]->(sc_upload)

// Створення файлів
CREATE (f1:File {id: 'file1', hash: 'hash1', uploadTimestamp: timestamp(), type: 'image', description:
'Evidence image from crime scene'})
```

```
CREATE (f2:File {id: 'file2', hash: 'hash2', uploadTimestamp: timestamp(), type: 'document',
description: 'Witness statement'})

// Зберігання файлів у децентралізованому сховищі
CREATE (f1)-[:STORED_IN]->(ds)
CREATE (f2)-[:STORED_IN]->(ds)

// Отримання хешів файлів зі сховища
SET f1.storageHash = 'storageHash1'
SET f2.storageHash = 'storageHash2'

// Створення блоків за допомогою смарт-контракту
CREATE (sc_upload)-[:CREATES]->(b1:Block {id: 'block1', prevHash: 'blockRegisterHash2', hash:
'blockHash1', fileHash: 'hash1', storageHash: 'storageHash1', userId: 'hashAlice', timestamp:
timestamp()})
CREATE (sc_upload)-[:CREATES]->(b2:Block {id: 'block2', prevHash: 'blockHash1', hash:
'blockHash2', fileHash: 'hash2', storageHash: 'storageHash2', userId: 'hashBob', timestamp:
timestamp()})

// Створення зв'язків між блоками та файлами
CREATE (b1)-[:CONTAINS]->(f1)
CREATE (b2)-[:CONTAINS]->(f2)

// Збереження блоків в блокчейні
CREATE (b1)-[:STORED_IN]->(bc)
CREATE (b2)-[:STORED_IN]->(bc)

// Зв'язки для доступу до файлів
CREATE (u1)-[:HAS_ACCESS]->(f1)
CREATE (u2)-[:HAS_ACCESS]->(f2)

// Зв'язки між користувачами та смарт-контрактами
CREATE (u1)-[:EXECUTES]->(sc_register)
CREATE (u2)-[:EXECUTES]->(sc_register)
CREATE (u1)-[:EXECUTES]->(sc_upload)
CREATE (u2)-[:EXECUTES]->(sc_upload)
```