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

ПОМОГАЄВ Сергій Олександрович

Алгоритми безпечного зберігання медичних записів за допомогою Blockchain / Secure Medical Record Storage Algorithms Using Blockchain

спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -22
С.О. Помогаєв

Науковий керівник
д.т.н., професор В.В.Яцків

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ **В.В.Яцків**

ТЕРНОПІЛЬ - 2023

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

ЗАТВЕРДЖУЮ
Завідувач кафедри

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ПОМОГАЄВ СЕРГІЙ ОЛЕКСАНДРОВИЧ
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми безпечного зберігання медичних записів за допомогою Blockchain / Secure Medical Record Storage Algorithms Using Blockchain
керівник роботи д.т.н., професор В.В. Яцків
затверджені наказом по університету від 1 грудня 2022 року № 491

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

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

4. Основні питання, які потрібно розробити:
– дослідити основи технології блокчейн та принцип її роботи;
– дослідити можливості використання блокчейну у медицині, враховуючи переваги і недоліки;
– дослідити вимоги до безпеки зберігання медичних записів;
– проаналізувати існуючі загрози для рішень по збереженню медичних записів;
– проаналізувати існуючі рішення;
– розробити алгоритм для зберігання медичних записів із застосуванням технології блокчейн і криптографічного захисту.

5. Перелік графічного матеріалу у роботі:
– формування цифрового підпису;
– перевірка цифрового підпису;

– взаємодія вузлів лікарень з вузлом міністерства;

– однорівнева мережа лікувальних закладів та схема участі у досягненні консенсусу;

– схема системи зберігання медичних записів та взаємодії учасників за допомогою блокчейн технології;

– обчислення хеш-значення документів;

– перевірка валідності отриманих даних від вузла.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Основи технології блокчейн та її застосування в медицині	12.2022 р. – 03.2023 р.	
2	Вимоги до безпеки медичних записів та аналіз ландшафту загроз	03.2023 р. – 05.2023 р.	
3	Розробка алгоритмів безпечного зберігання медичних записів із застосуванням технології блокчейн	05.2023 р. – 11.2023 р.	

Студент _____ Помогаєв С.О.

(підпис)

Керівник роботи _____ д.т.н., професор В.В. Яцків

АНОТАЦІЯ

Кваліфікаційна робота на тему «Алгоритми безпечного зберігання медичних записів за допомогою Blockchain» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 77 сторінок і містить 7 ілюстрації, 2 таблиця, 1 додаток та 30 джерел за переліком посилань.

Метою кваліфікаційної роботи є підвищення ефективності безпечного зберігання медичних записів за допомогою Blockchain.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи забезпечення цілісності та конфіденційності даних, методи цифрового підпису, методи побудови розподілених систем.

Результати дослідження. Вдосконалено алгоритм безпечного зберігання медичних записів за допомогою Blockchain.

Розроблено систему зберігання медичних записів з використанням технології Blockchain.

Результати роботи можуть бути застосовані при розробці систем зберігання чутливої до розголошення інформації.

Ключові слова: ГЕШ-ФУНКЦІЇ, ДЕРЕВА МЕРКЛА, ТЕХНОЛОГІЯ БЛОКЧЕЙН.

ABSTRACT

Qualification work on "Secure Medical Record Storage Algorithms Using Blockchain" for the degree of "Master" in the specialty 125 "Cybersecurity" educational and professional program "Cybersecurity" is written in 77 pages and contains 7 illustrations, 2 tables, 1 appendices and 30 source according to the list of links.

The goal of the qualification work is to improve the efficiency of safe storage of medical records using Blockchain.

Research methods. To solve the tasks in this qualification work, the following methods were used: methods of ensuring data integrity and confidentiality, digital signature methods, methods of building distributed systems.

Research results. The algorithm for safe storage of medical records using Blockchain has been improved.

A system for storing medical records using Blockchain technology has been developed.

The results of the work can be applied in the development of storage systems for information sensitive to disclosure.

Keywords: HASH FUNCTIONS, MERKLA TREES, BLOCKCHAIN TECHNOLOGY.

ЗМІСТ

ВСТУП

Актуальність роботи. Серед потоків інформації, які несе сучасний світ, медичні дані вибиваються необхідністю особливої уваги та конфіденційності. Вони втілюють у собі не лише історію хвороб і лікування, але і якість життя та іншу особисту інформацію пацієнтів. Захист медичних даних стає важливішим, ніж будь-коли раніше, оскільки на кону - не лише приватність, а й здоров'я та довіра до системи охорони здоров'я [1 -3].

Короткий перелік причин, чому правильний підхід до забезпечення захисту медичних даних має вирішальне значення, може виглядати так:

– Конфіденційність і приватність пацієнтів, лікарська таємниця.
– Цілісність даних.
– Доступність медичних даних.
– Запобігання зловживанням.
– Ідентифікація і аутентифікація пацієнтів.
– Медична безпека.
– Відповідність законодавству.
– Дослідження та статистика.
– Довіра пацієнтів і громади.

Медичні дані містять особисту та надзвичайно конфіденційну інформацію про пацієнтів, включаючи їхні діагнози, стан здоров'я, історію хвороб, лікування та інше. Пацієнти мають право на приватність своїх медичних даних, і порушення конфіденційності може призвести до непоправних наслідків. Лікарська таємниця є обов'язковою для захисту прав пацієнтів та дотримання законодавства. У багатьох випадках потрібен високий рівень безпеки для збереження конфіденційності медичних записів. Ця проблема особливо актуальна в епоху цифрової трансформації медичної сфери.

Важливість цілісності медичних даних полягає у тому, щоб уникнути їхнього впливу або модифікації без належних дозволів. Зміни в медичних записах можуть вплинути на здоров'я пацієнта та призвести до негативних

наслідків – медичні дані важливі для проведення правильних і ефективних медичних процедур, лікування та діагностики. Невірні або підроблені дані можуть призвести до помилок при лікуванні та виникнення небезпеки для життя пацієнтів. Важливо забезпечити такий захист, щоб медичні дані не могли бути змінені або пошкоджені без дозволу пацієнта або довіреної особи.

Медичні записи повинні бути доступні в будь-який момент для лікарів та пацієнтів, однак вони також повинні бути захищені від втрати, зміни чи несанкціонованого доступу. Несанкціонований доступ до медичних даних може призвести до зловживань ідентичністю, шахрайства, крадіжки ідентифікаційної інформації, що може завдати серйозної шкоди пацієнтам і системам охорони здоров'я. Зберігання медичних даних в безпечному середовищі допомагає забезпечити достовірну ідентифікацію пацієнтів та запобігає помилкам при наданні медичних послуг.

Багато країн мають закони та нормативні акти, що регулюють зберігання та обробку медичних даних. Недотримання цих вимог може призвести до юридичних санкцій та штрафів.

Надійний процес зберігання медичних даних також важливий для медичних досліджень, статистичного аналізу та виявлення трендів у галузі охорони здоров'я.

Ця дипломна робота розглядає важливість захисту медичних даних та методи, які можуть забезпечити недоторканість цієї важливої інформації в світі, де кіберзагрози та технологічні виклики набувають обрисів загрози для нашого здоров'я та приватності. Спробуємо розглянути, які алгоритми та технології можуть стати надійними оборонними механізмами в цьому непередбачуваному цифровому ландшафті і як забезпечити безпеку медичних записів на блокчейні.

У нашому дослідженні ми поглибимося в світ сучасних викликів із збереження та захисту медичних даних та виявимо, які кроки можна зробити для збереження довіри до цієї важливої сфери нашого життя. Медичні дані - це не лише цифри та факти, це історії життів та можливість надати їм безпеку в цифровому віці.

Мета та завдання дослідження. Ця дипломна робота має на меті детальне дослідження алгоритмів та методології, спрямованих на забезпечення високого рівня безпеки, конфіденційності та цілісності медичних записів через використання технології блокчейн. Основною метою є розробка і визначення принципів, що дозволять створити надійну та ефективну систему, що відповідає всім вимогам щодо зберігання лікарської інформації та враховує основні принципи збереження медичних даних та збереження медичної конфіденційності.

Для досягнення вищезазначеної мети, дослідження включає наступні завдання:

1. Ретельно вивчити принципи роботи блокчейн та ознайомитися з основними концепціями, що стосуються цілісності даних, децентралізації та безпеки.

2. Розглянути та проаналізувати сучасні підходи до зберігання медичних записів та визначити їх переваги та недоліки.

3. Проаналізувати існуючі рішення та проекти для зберігання медичних даних, і дослідити їх особливості.

4. Дослідити вимоги до безпеки у роботі з медичними даними, у тому числі на базі блокчейн, враховуючи вимоги до конфіденційності, цілісності та доступності даних.

5. Реалізувати описовий прототип системи для зберігання медичних записів, використовуючи вирішені алгоритми та технологію блокчейн.

6. Ці завдання спрямовані на створення інноваційного рішення для зберігання медичних даних, яке враховує вимоги безпеки та конфіденційності у сфері медицини та відповідає сучасним викликам у цій галузі.

Методи дослідження. Для проведення дослідження ми застосуємо наступні методи, спрямовані на досягнення поставлених завдань та мети:

1. Аналіз літератури і попередніх досліджень – планується використання літератури та аналіз попередніх досліджень, щоб дізнатися про

існуючі підходи до зберігання медичних даних та виявити прогалини та виклики, які потребують уваги.

2. Дослідження принципів блокчейн – вивчення основних принципів та концепцій, які стосуються технології блокчейн, включаючи децентралізацію, криптографічний захист, консенсусні алгоритми та багато інших нюансів.

3. Аналіз вимог до безпеки медичних даних – я планую дослідити вимоги та стандарти, які встановлені для зберігання медичних даних з точки зору конфіденційності, цілісності та доступності.

4. Вивчення підходів до розробки алгоритмів і архітектури системи – це допоможе краще зрозуміти, як будувати алгоритми для безпечного зберігання медичних записів на базі блокчейн та розробляти архітектуру системи, яка враховує вимоги зберігання медичних даних (в т.ч. дотримання принципу лікарської таємниці).

5. Описова реалізація – опис розроблених алгоритмів та архітектури системи.

6. Аналіз результатів – оцінка отриманих результатів та виведення висновків щодо досягнутих цілей та завдань дослідження.

Об’єкт дослідження – процеси безпечного зберігання медичних записів за допомогою Blockchain.

Предмет дослідження – методи та алгоритми безпечного зберігання медичних записів за допомогою Blockchain.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: методи автентифікації, методи захисту даних, теорію алгоритмів та структур даних, алгоритми консенсусу, методи оцінки складності.

Наукова новизна одержаних результатів. Вдосконалено алгоритм безпечного зберігання медичних записів за допомогою Blockchain.

Практичне значення отриманих результатів. Розроблено систему зберігання медичних записів з використанням технології Blockchain

Публікації та апробація КР.

1. Басістий В.П., Ділай С.Я., Помогаєв С.О. Алгоритми доказу з нульовим знанням. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ – 2023), Тернопіль, 2023. – С.14-16.

2. Ділай С.Я., Кондратюк В.М., Помогаєв С.О. Використання доказів із нульовим розголошенням. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 48-49.

1 ОСНОВИ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА ЇЇ ЗАСТОСУВАННЯ В МЕДИЦИНІ

У даному розділі ми проаналізуємо ключові аспекти технології блокчейн та розглянемо її потенціал для використання в сфері медицини. Ми розглянемо основні принципи роботи блокчейн-системи, розглянемо переваги та особливості застосування в медицині, розглянемо виклики та обмеження, особливо у питаннях конфіденційності, масштабованості, вартості та децентралізації. Цей розділ є основою для подальшої аналітичної роботи.

1.1 Огляд принципів роботи блокчейн

Блокчейн – це технологія, яка дозволяє створювати безпечну та надійну базу даних, яка може бути розподілена між багатьма комп'ютерами. Кожна дія у системі (транзакція) записується і ці записи формуються у блоки, які з'єднані послідовно у ланцюг. При цьому ланцюг побудований за допомогою криптографії – кожен наступний блок містить посилання на попередній, тому будь-яка модифікація попередніх даних буде помічена негайно [4, 5].

Архітектурно ця система часто буває децентралізованою, що означає відсутність єдиного центрального елементу контролю (і, по суті, точки відмови), інформація захищена шифруванням, і коли дані додані до блокчейну, вони залишаються практично незмінними. Така технологія знаходить застосування в багатьох галузях, включаючи фінанси, логістику, медицину та багато інших сфер.

Виділимо декілька основних принципів роботи, характерних для блокчейн технології [6]:

– блокова структура;
– криптографічний захист і хеш-функції;
– імутабельність (незмінюваність);
– прозорість;

– алгоритми досягнення консенсусу;
– приватність та конфіденційність;
– децентралізація системи;
– смарт-контракти.

Блокова структура. Як ми описували вище, у блокчейні інформація групується у блоки, кожен із яких містить записи (транзакції). Кожен блок має унікальний ідентифікатор – хеш-значення (унікальна послідовність, отримана в результаті перетворення даних за допомогою хеш-функції), що обчислюється на основі вмісту блоку і хеш-значення попереднього блоку. Така послідовна ланцюжкова структура дозволяє забезпечити незмінність даних: будь-яка зміна в одному блоку призведе до зміни хешів у всіх попередніх блоках. Такий підхід значно ускладнює можливості для маніпуляції та допомагає зробити роботу з даними безпечною та надійною.

Криптографічний захист і хеш-функції. Криптографія відіграє важливу роль у побудові блокчейн-системи, забезпечуючи конфіденційність, безпеку і імутабельність даних. У цьому контексті важливими компонентами криптографії є криптографічні ключі, цифрові підписи, хеш-функції, алгоритми досягнення консенсусу, шифрування та смарт-контракти.

Кожен користувач блокчейн-мережі має свою ключову пару. Унікальний приватний ключ використовується для підписування транзакцій та ідентифікації. Під час створення транзакцій користувач підписує їх за допомогою свого приватного ключа, створюючи електронно-цифровий підпис, який ідентифікує власника та забезпечує конфіденційність та цілісність транзакції. З приватного ключа шляхом перетворення може бути виведений публічний ключ, який є відкритим і використовується іншими користувачами для перевірки підписів та ідентифікації власника приватного ключа.

Імутабельність. Принцип *імутабельності* даних у блокчейні досягається завдяки криптографії та хеш-функціям. Хеш-функції використовуються для створення унікальних хешів для кожного блоку та транзакції у системі. Хеш (хеш-значення) - це коротка послідовність чисел і букв, яка унікально ідентифікує вміст даного блоку чи транзакції.

Коли дані записуються в блок, обчислюється хеш цього блоку на основі його вмісту, і цей хеш включається до наступного блоку як один з елементів вмісту. При цьому, будь-яка навіть найменша зміна у вмісті блоку призведе до зміни обчисленого хешу. Це дуже важливо, оскільки це забезпечує виявлення будь-яких спроб маніпуляції даними. Якщо хтось намагатиметься змінити вміст блоку (наприклад, видалити чи змінити транзакцію), то хеш блоку зміниться, і це стане видимим для всіх учасників мережі.

Отже, завдяки використанню хеш-функцій та криптографії, дані стають імутабельними, оскільки будь-яка спроба зміни чи видалення даних вимагає перерахунку хешів у всіх попередніх блоках, що стає надзвичайно витратними за ресурсами та часом операціями. Це робить систему надійною для зберігання важливої історії та даних, оскільки будь-яка спроба маніпуляції буде легко виявлена та відхилена громадою учасників мережі.

Прозорість. Прозорість є одним із ключових принципів блокчейн-технології і визначається як відкритість та доступність інформації в мережі для всіх учасників. Під прозорістю у випадку блокчейн-системи розуміють публічність даних, відстежуваність дій, гарантована перевірка на легітимність, а інколи і відкритий доступ до коду.

Всі дані, що заносяться в блокчейн, стають публічно доступними і відкритими для перегляду всіма користувачами мережі. Це означає, що будь-який учасник може перевірити та відстежувати транзакції та дії інших учасників.

Транзакції та дії в мережі є легко відстежуваними та аудитованими завдяки відкритому журналу транзакцій. Це дозволяє виявляти будь-які незвичайні чи недопустимі дії та проводити аналіз діяльності.

Учасники мережі можуть перевіряти легітимність та цілісність транзакцій та даних без потреби довіряти централізованим посередникам чи авторитетам. Все підтверджується криптографічно, що робить систему надійною.

В деяких блокчейн-мережах є відкритий доступ до вихідного коду, що дозволяє всім бажаючим перевірити, як працює мережа та як обробляються дані.

Алгоритми досягнення консенсусу. Для забезпечення єдності даних у всій мережі всі вузли повинні досягти консенсусу щодо правильності транзакцій та блоків. Механізми досягнення консенсусу - це спеціальні алгоритми, які використовуються у розподілених системах, а основна мета цих механізмів - забезпечити єдину версію історії та стану мережі в умовах відсутності централізованого авторитету чи довіри між учасниками.

Приведемо приклади декількох найрозповсюдженіших механізмів консенсусу [7 - 8]:

1. Proof of Work (PoW).

PoW використовує складні обчислювальні задачі, які *майнери* (активні користувачі, які беруть участь у формуванні блоків) повинні вирішити, щоб створити новий блок та підтвердити транзакції. Перший користувач, який успішно розв'язує задачу, отримує право створити блок та отримує винагороду. PoW вимагає великої обчислювальної потужності та споживає багато електроенергії.

2. Proof of Stake (PoS).

У PoS користувачі не розв'язують обчислювальні задачі, але вони заморожують свої активи як гарантію права створити новий блок. Вибір користувача базується на його персональному внеску у мережу (кількість заморожених активів) у поєднанні з елементами випадкового відбору.

3. Delegated Proof of Stake (DPoS).

DPoS – це варіація PoS, де усі користувачі мережі обирають обмежену групу конкретних користувачів, які мають право створювати блоки та приймати

рішення від імені всієї мережі. Це підвищує швидкість та масштабованість мережі.

4. Proof of Authority (PoA).

У PoA, право створення блоків надається вузлам, які є довіреними учасниками мережі. Це дозволяє забезпечити високу швидкість та надійність мережі, але при цьому така система буде менш децентралізованою.

5. Proof of Space (PoSpace) та Proof of Time (PoT).

Ці механізми базуються на використанні вільного простору на жорстких дисках та обчислювального часу відповідно. Вони призначені для зменшення енергоспоживання, специфічні для децентралізованих сховищ та подібних застосувань.

6. BFT (Byzantine Fault Tolerance).

Даний клас алгоритмів, такий як Practical Byzantine Fault Tolerance (PBFT) та HoneyBadgerBFT, спроектований для досягнення консенсусу в умовах відмов та зловмисних атак. Вони дозволяють досягти консенсусу, навіть якщо частка вузлів тримаються зловмисниками.

7. FBA (Federated Byzantine Agreement).

Цей підхід використовується в Stellar, як приклад. Він розроблений для систем, де вузли розділені на федерації, і кожна федерація приймає рішення незалежно. FBA дозволяє досягати консенсусу між федераціями.

Кожен з цих механізмів має свої переваги та недоліки, і вибір механізму консенсусу залежить від конкретних потреб і вимог блокчейн-мережі. Наприклад, PoW використовується в Bitcoin-мережі, тоді як PoS застосовується у мережі Ethereum та багатьох інших блокчейн-платформах. DPoS широко використовується у комерційних блокчейн-проектах, а PoA застосовують у проектах децентралізованих сховищ.

Приватність та конфіденційність. Даний принцип у блокчейн-системі визначає те, як забезпечується захист конфіденційної інформації в умовах децентралізованої технології. У багатьох аспектах даний пункт пов'язаний із криптографічним захистом.

Для забезпечення конфіденційності, дані можуть бути зашифровані перед зберіганням на блокчейні. Шифрування робить дані нечитабельними для несанкціонованих користувачів, і вони можуть бути розшифровані лише з використанням відповідного ключа доступу. Це гарантує, що навіть якщо зловмисник отримає доступ до зашифрованих даних, він не зможе їх прочитати без правильного ключа.

Замість використання реальних імен чи ідентифікаторів, учасники можуть користуватися псевдонімами або випадковими номерами для збереження приватності. Це дозволяє приховувати особисту ідентифікацію в мережі.

У блокчейні можна використати захищені ідентифікатори. Існує, наприклад, така технологія, як Zero-Knowledge Proofs (доказ із нульовим розголошенням), яка дозволяє підтверджувати право на доступ до інформації без розкриття самої інформації. Наприклад, можна довести, що ви маєте право на доступ до медичних записів, не розкриваючи їх зміст.

Принципи приватності можуть бути реалізовані різними способами в залежності від рівня децентралізації системи. Публічні та приватні блокчейни можуть використовувати різні підходи до забезпечення конфіденційності медичних даних.

Децентралізація системи. Один із фундаментальних аспектів технології блокчейн – це ступінь децентралізації. Вона може бути різного рівня, від повністю децентралізованої мережі до централізованої системи, яка має лише елементи децентралізації. У повністю децентралізованій системі жоден центральний орган не контролює мережу, в той час як у централізованій системі можуть існувати централізовані сервери, але з можливістю перевірки операцій мережі. Розуміння цього аспекту дозволяє визначити оптимальний

рівень децентралізації для медичної системи в контексті конфіденційності, доступності та безпеки даних.

Смарт-контракти. Так звані смарт-контракти – це автоматизовані програми, які запускаються і виконуються в розподіленій мережі блокчейн після настання певугоди і операції без потреби посередників і забезпечуючи надійність, безпеку та прозорість у галузях, які вимагають угод та виконання умов) можуть бути використані для створення складних правил доступу до конфіденційної інформації. Такі контракти можуть визначати, хто та в яких умовах може мати доступ до конкретних даних.

Смарт-контракти – це програми, які виконуються автоматично при настанні певних умов. Вони розширюють можливості блокчейн технології, дозволяючи автоматизувати багато процесів у середовищі, де довіра між учасниками - важко виконувана або неможлива умова.

Вище описаний огляд принципів роботи блокчейн дозволяє врахувати різні рівні децентралізації та адаптувати їх для конкретних потреб медичної галузі. Розуміння цих принципів є ключовим для визначення оптимального підходу до розробки системи зберігання медичних записів з урахуванням вимог до конфіденційності, доступності та безпеки даних.

1.2 Огляд можливостей використання блокчейн в медицині

Вивчивши принципи роботи блокчейн, ми розуміємо, що технологія може бути використана (має потенціал) у медицині для безпечного та ефективного обміну медичною інформацією між закладами охорони здоров’я, лікарями та пацієнтами, забезпечення конфіденційності та безпеки медичних даних, відстеження походження та доставки ліків у ланцюжку постачання, а також автоматизації процесів страхування та відшкодування за медичні послуги за допомогою смарт-контрактів, що спрощує та поліпшує якість надання

медичних послуг та управління медичною інформацією. Нижче поговоримо про це більш детально [9].

Можна виділити декілька основних та найбільш очевидних сфер, де застосування блокчейну зробить роботу з медичними даними більш безпечною:

– *зберігання медичних записів* (надійне сховище медичних даних, що забезпечує їх цілісність та захист);

– *відслідковування медичних даних* (за допомогою цієї технології можна створювати ланцюжки подій та діагнозів пацієнтів);

– *автентифікація пацієнтів* (дозволяє запобігати несанкціонованому доступу до особистої інформації);

– *медична історія* (дозволяє лікарям та дослідникам легко отримувати доступ до важливих даних для діагностики та лікування);

– *дослідження та клінічні випробування* (більш прозоре та надійне ведення досліджень та зберігання результатів клінічних випробувань);

– *боротьба з фальсифікацією медичних препаратів* (можна відстежувати маршрут походження медичних препаратів та запобігати появі підроблених ліків);

– *обмін медичною інформацією* (безпечний обмін медичною інформацією між різними медичними установами та лікарями);

– *підтримка донорства та органотрансплантації* (ведення реєстрів донорів та спрощення процесу органотрансплантації за рахунок точного і швидкого аудиту);

– *інші медичні застосування* (від боротьби з епідеміями, за рахунок ведення і інтеграції між собою довірених реєстрів, до оптимізації медичного страхування – смарт-контракти можуть допомогти усунути людський фактор і зацікавленість отримати/не виплачувати нелегітимну винагороду при настанні страхового випадку).

1.3 Переваги та недоліки застосування Blockchain в медичних записах

Щодо переваг та недоліків використання технології блокчейн для зберігання медичних записів, тут треба сказати, що потрібно враховувати кінцеві вимоги до системи. В залежності від того, якою буде архітектура системи, переваги і недоліки можна врахувати і збалансувати систему.

Переваги застосування технології блокчейн для зберігання медичних записів

Якщо говорити про переваги, то це [10 -12]:

– безпека даних;
– цілісність даних;
– доступність даних;
– імутабельність даних;
– автентифікація пацієнтів;
– часова мітка (timestamp);
– синхронізація даних.

Розглянемо детальніше вищенаведені пункти. Однією з найбільших переваг використання технології блокчейн є високий рівень безпеки даних. Технологія використовує сильну криптографію та децентралізовану структуру для захисту медичних записів від несанкціонованого доступу та змін. Наприклад, якщо у системі використовується шифрування, то можна зробити, що тільки лікар та пацієнт матимуть доступ до власних приватних ключів для розшифрування даних. Коли лікар потребує доступ до історії пацієнта, можна зробити так, щоб смарт-контракт дозволяв лікарю отримати доступ за згодою пацієнта та автоматично зареєстрував всі взаємодії в журналі блокчейну.

Як ми вже знаємо завдяки використанню хеш-функцій, блокчейн забезпечує цілісність медичних даних. Якщо дані будуть змінені, то хеш-значення також зміниться, що робить виявлення будь-яких змін легким. Уявімо, що кожен медичний запис і тестовий результат піддаються хешуванню, створюючи унікальне хеш-значення. Ці дані можуть бути доступні лише

пацієнту та його лікарю, і будь-яка спроба несанкціонованої зміни даних призведе до зміни хеш-значення. Це означає, що будь-які спроби внести зміни в медичні дані будуть негайно виявлені, оскільки хеш-значення не відповідатимуть оригінальним значенням. Такий механізм гарантує цілісність медичних даних пацієнта і захищає їх від можливих маніпуляцій чи фальсифікацій, забезпечуючи надійний контроль над інформацією і довіру до медичних записів.

Медичні дані, збережені в блокчейні, можуть бути доступні для авторизованих сторін в будь-який час і з будь-якого місця. Це особливо корисно в ситуаціях надзвичайних станів, коли швидкий доступ до медичних записів є важливим. Якщо, наприклад, пацієнт потрапляє до лікаря в іншому місті чи країні в результаті надзвичайної ситуації, то завдяки медичним даним, збереженим в блокчейні, лікар може мати миттєвий та безперешкодний доступ до історії хвороби та медичних даних пацієнта, навіть якщо вони були створені в іншому закладі в іншому кутку світу. Це дозволяє надати можливу медичну допомогу швидко та ефективно, забезпечуючи високий рівень безпеки і доступності медичних даних для обох сторін і, таким чином, захищаючи пацієнта і допомагаючи лікарю приймати інформовані рішення у критичних ситуаціях. Або ж можна створити можливість для пацієнтів контролювати свої медичні дані та надавати доступ до них лікарям та іншим фахівцям за своєю згодою.

Дані, які зберігаються в блокчейні, є імутабельними, тобто вони не піддаються змінам або видаленню без відповідного авторизованого процесу. Це гарантує стійкість медичних записів до зовнішніх втручань. Уявімо сценарій, де пацієнт лікується у різних медичних закладах, і його медична історія зберігається в медичній системі, реалізованій за допомогою блокчейну. В цьому контексті імутабельність забезпечує надійний захист медичних записів пацієнта від змін чи видалень без належного авторизованого схвалення. Записи про лікування, діагнози та рецепти перебувають в імутабельному стані та захищені від зовнішніх атак і навіть внутрішніх втручань. Ця стійкість даних забезпечує

надійність медичної інформації і дозволяє лікарям різних медичних закладів отримувати доступ до цих даних з впевненістю у їхній цілісності, що в свою чергу підвищує довіру, забезпечує надійний аудит та зберігає конфіденційність медичних записів пацієнта у глобальному медичному середовищі.

Блокчейн може використовуватись для надійної автентифікації пацієнтів, забезпечуючи безпеку та конфіденційність їх медичних даних. Припустимо, що пацієнт потребує медичної допомоги в іншій медичній установі або країні. Для автентифікації пацієнта може бути створений криптографічний цифровий ідентифікатор пацієнта, який заснований на його біометричних даних та інших персональних даних. Цей ідентифікатор зберігається у блокчейні і може бути використаний для авторизації пацієнта в будь-якому медичному закладі. Лікарі та інші медичні працівники та системи охорони здоров'я можуть перевірити цей ідентифікатор, щоб переконатися в легітимності пацієнта та надати йому доступ до його медичних даних у безпечному та конфіденційному середовищі. Ця технологія забезпечує надійну і безпечну автентифікацію пацієнта та допомагає лікарям швидко та ефективно надавати медичну допомогу в умовах термінової потреби, зберігаючи конфіденційність медичних даних пацієнта у цьому процесі.

Важливим моментом є те, що кожен блок у блокчейні має часову мітку, яка фіксує точний момент створення блоку. Це дозволяє визначити, коли були внесені зміни до медичних записів, що може бути важливим для визначення хронології подій та проведення аудиту.

Технологія блокчейн може також використовуватися для синхронізації медичних даних між різними медичними системами та закладами, що покращує доступність та точність інформації.

Недоліки застосування технології блокчейн для зберігання медичних записів.

Тут треба виділити такі аспекти [13]:

– масштабовість;

– ресурсомісткість;

– загроза конфіденційності, якщо мережа публічна і відкрита;

– технічні виклики;

– легальні аспекти.

На сьогоднішній день, масштабовість блокчейн-систем є важкою задачею. Це суттєво залежить від архітектури системи і протоколу, за яким вона працює, але якщо ми говоримо про відкриту і публічну мережу, то часто кожна транзакція потребує сплати комісії за валідацію. Обробка великого обсягу медичних даних може бути повільною та дорогою.

Блокчейн також може бути витратним процесом, якщо розглядати велику обчислювальну потужність та витрати на енергію, але тут багато залежить від того, який механізм досягнення консенсусу обрати. Існують менш ресурсомісткі рішення, але тоді доведеться поступитись публічністю системи і можливостями прийняття рішень для кожного учасника.

У відкритих блокчейн-мережах конфіденційність медичних даних може бути порушеною. При проектуванні і реалізації таких систем треба враховувати вимоги до захисту конфіденційної інформації.

Розробка, налагодження та підтримка блокчейн-системи вимагає високої технічної компетенції та ресурсів, у тому числі і матеріальних.

У багатьох юрисдикціях ще не розроблені чіткі правила та стандарти щодо використання Blockchain в медицині, що може викликати юридичні питання.

Розуміння цих переваг та недоліків допомагає визначити, як використовувати технологію блокчейн для зберігання медичних записів ефективно та які аспекти потребують особливої уваги та вдосконалення.

2 ВИМОГИ ДО БЕЗПЕКИ МЕДИЧНИХ ЗАПИСІВ ТА АНАЛІЗ ЛАНДШАФТУ ЗАГРОЗ

У даному розділі роботи ми розглянемо основні вимоги до безпеки медичних записів в контексті використання технології блокчейн. Безпека медичних даних вимагає врахування тріади КЦД: конфіденційності, цілісності та доступності інформації. Загальний підхід до вимог до конфіденційності полягає в створенні комплексної системи заходів, яка поєднує технічні та організаційні заходи для забезпечення конфіденційності медичних даних в системі зберігання на основі технології блокчейн.

2.1 Вимоги до конфіденційності медичних даних

Конфіденційність медичних даних є важливою, оскільки вони містять особисту та чутливу інформацію пацієнтів. Для забезпечення конфіденційності, система повинна використовувати [14 – 16]:

– криптографічний захист;
– логіку управління доступом та принцип найменших привілеїв;
– аудит та журналювання.

Сильну криптографія потрібна для захисту даних під час зберігання та передачі. Інформація повинна бути захищена таким чином, щоб лише авторизовані користувачі мали доступ до вмісту.

Має бути встановлений деталізований ієрархічний контроль доступу до медичних даних, включаючи ролі та права доступу для різних користувачів. Система повинна надавати доступ тільки авторизованим користувачам та забезпечувати високий рівень автентифікації. Для цього важливо мати механізми автентифікації, такі як паролі, біометричні дані або мережеві сертифікати. Після автентифікації користувача важливо також контролювати його права доступу, щоб визначити, які дані він може переглядати та редагувати. Кожен користувач повинен мати обмежений доступ лише до необхідних медичних даних (принцип найменших привілеїв).

Наприклад, медичний асистент може мати доступ до базової інформації про пацієнтів, тоді як лікар може мати доступ до повної медичної історії. Лікар має право змінювати медичні записи своїх пацієнтів, але медична сестра не має цього права. Авторизація гарантує, що лише відповідні фахівці можуть внесення зміни до даних. Це обмеження доступу допомагає запобігти несанкціонованому розкриттю даних.

Система повинна вести докладний журнал всіх дій з медичними даними для можливості аудиту, виявлення можливих порушень та встановлення відповідальності.

2.2 Вимоги до цілісності медичних записів

Цілісність медичних записів передбачає, що дані не піддаються недозволеним змінам чи порушенням. Для досягнення цього використовуються хеш-функції, які генерують унікальний код (хеш) на основі вмісту даних. Будь-яка навіть найменша зміна в записі призведе до зміни хеш-значення. Медичні дані і їхні хеш-значення зберігаються в блокчейні, і будь-яка спроба незаконної зміни даних буде негайно виявлена через невідповідність хеш-значень. Такий механізм гарантує цілісність медичних даних та захищає їх від випадкових чи навмисних змін.

Тож тут ми спираємося на [17]:

– використання хеш-функцій для створення контрольних сум та перевірки цілісності даних;

– гарантування, що медичні записи, збережені в блокчейні, не підлягають змінам чи видаленню без належного авторизованого процесу.

Отже, розглянемо дане питання в аспекті хеш-функцій. Як ми знаємо – хеш-функції – це математичні алгоритми, які приймають вхідні дані будь-якого розміру і генерують фіксований вихідний хеш-код або контрольну суму. Основна роль хеш-функцій в забезпеченні цілісності даних полягає в тому, що

вони перетворюють будь-які дані в унікальний хеш-код, який може слугувати "відбитком пальця" для вихідних даних.

Процес створення контрольної суми за допомогою хеш-функції включає:

1. *Вхідні дані:* Хеш-функція приймає вхідні дані, які можуть бути будь-якого типу або розміру, включаючи медичні записи.

2. *Обчислення хешу*: Хеш-функція обчислює хеш-код на основі вмісту цих даних. Цей хеш-код є фіксованим, зазвичай фіксованого розміру, наприклад, 256 біт.

3. *Контрольна сума*: Отриманий хеш-код служить контрольною сумою для вихідних даних. Якщо вміст даних буде змінений (навіть найменша зміна), хеш-код також зміниться.

Перевірка цілісності даних полягає в порівнянні поточного хеш-коду, обчисленого на основі даних, і збереженого хеш-коду, який був обчислений при збереженні даних. Якщо ці хеш-коди співпадають, це означає, що дані залишилися незмінними та їх цілісність збережена. Якщо ж хеш-коди відрізняються, це вказує на те, що дані були змінені або пошкоджені.

У медичних сферах, де зберігання та доступ до медичних даних є критичними, використання хеш-функцій може бути особливо корисним.

Захист від незаконних змін: Хеш-функції можуть захищати медичні записи від недозволених змін. Якщо хеш-коди перевіряються регулярно, будь-яка невідома або незаконна зміна даних буде виявлена.

Збереження історії змін: Хеш-функції можуть бути використані для створення хеш-кодів для кожної версії медичних записів. Це дозволяє відстежувати історію змін та перевіряти, хто та коли змінив дані.

Забезпечення цілісності зображень та файлів: У медичних записах можуть бути важливі зображення, які також можуть підлягати цілісності за допомогою хеш-функцій.

Перевірка відправників даних: Хеш-коди можуть бути включені в медичні дані, надсиланні з одного медичного пристрою до іншого, щоб перевірити їхню цілісність та джерело.

Розглянемо переваги використання хеш-функцій у забезпеченні цілісності медичних даних. Включаємо аспекти, такі як швидкість, ефективність та вартість впровадження цієї технології.

1. Швидкість:

a. Обчислювальна швидкість. Хеш-функції швидко обчислюються навіть для великих об'ємів даних, що робить їх ефективними для використання в реальному часі, наприклад, при обробці потокової медичної інформації.

b. Мінімальний обсяг додаткових ресурсів. Використання хеш-функцій не вимагає значних обсягів обчислювальних або мережевих ресурсів, що дозволяє впроваджувати цю технологію навіть у медичних системах з обмеженими ресурсами.

c. Легка інтеграція. Хеш-функції можуть бути легко інтегровані в існуючі медичні системи без значних змін у архітектурі або розробці програмного забезпечення.

2. Вартість впровадження:

a. Відносно низька вартість. Використання хеш-функцій не вимагає дорогих апаратних або програмних рішень. Хеш-функції є вбудованими у багато сучасних обчислювальних платформ та програмних мовах, тому їх впровадження є відносно дешевим.

b. Низька обслуговування витрат. Після впровадження системи контролю цілісності на основі хеш-функцій, обслуговування є мінімальним. Це означає, що витрати на підтримку такої системи також є обмеженими.

3. Гарантована цілісність даних:

a. Надійність доказу цілісності. Однією з ключових переваг використання хеш-функцій є надійність доказу цілісності даних. Якщо хеш-код відповідає вихідним даним, це означає, що дані залишилися незмінними. Це може бути особливо корисним у випадках, коли необхідно довести перед судом цілісність медичних записів.

b. Захист від недозволених змін. Використання хеш-функцій гарантує, що навіть найменші зміни в записі призведуть до зміни хеш-коду. Це

забезпечує захист медичних даних від випадкових чи навмисних змін, включаючи зловмисні атаки.

4. Застосування у великих обсягах даних:

а. Скалабельність. Хеш-функції можна застосовувати до великих обсягів медичних даних без значного впливу на продуктивність системи. Це особливо важливо в медичних організаціях, де зберігається велика кількість медичної інформації.

Щодо гарантування, що медичні записи, збережені в блокчейні, не підлягають змінам чи видаленню без належного авторизованого процесу, тут враховуємо, що інформація зберігається у блокчейні і вона не може бути змінена чи видалена без створення нового блоку, який підтверджує ці зміни. Це гарантує незмінність медичних записів та стійкість до випадкових чи навмисних змін.

До того ж, за наявності авторизації і контролю доступу всі спроби змінити чи видалити медичні дані будуть суворо контрольовані та авторизовані. Це означає, що лише відповідно авторизовані користувачі, такі як лікарі, медичний персонал чи пацієнти, мають право внесення змін у дані. Авторизація може здійснюватися за допомогою електронних підписів, біометричних методів або інших безпечних засобів ідентифікації.

Блокчейн також надає можливість вести аудит та відстежувати всі зміни, які були внесені до медичних записів. Це важливо для подальшого аналізу та перевірки всіх дій, що стосуються медичних даних.

Розглянемо реальні приклади ситуацій, де цілісність медичних даних є критично важливою. Наприклад, екстренна медична допомога в аварійних ситуаціях, які вимагають точних і незмінних даних.

Екстренна медична допомога в аварійних ситуаціях – у випадках аварій, таких як дорожньо-транспортні пригоди, природні катастрофи або масові надзвичайні ситуації, надання точної та невідкладної медичної допомоги може врятувати життя постраждалим. В таких ситуаціях цілісність медичних даних є критично важливою.

Швидкий та точний обмін медичною інформацією між рятувальниками та лікарями може визначити успішність лікування. Використання хеш-функцій для забезпечення цілісності даних гарантує, що інформація не була змінена під час передачі.

У випадках аварій часто потрібно доступатися до медичних історій постраждалих для отримання докладних медичних даних, таких як алергії, хронічні захворювання, ліки та попередні медичні процедури. Забезпечення цілісності цих даних допомагає уникнути надзвичайних ситуацій через неправильні або недостовірні медичні дані.

Медичні дані, які передаються в режимі реального часу під час дистанційної консультації, повинні бути точними та незмінними. Навіть маленькі зміни в інформації можуть призвести до недооцінки ризиків або неправильного лікування.

Забезпечення цілісності медичних даних також допомагає захищати конфіденційність пацієнта. Це особливо важливо у випадках, коли медична інформація передається через відкриті мережі.

Під час консультацій та лікування пацієнтів важливо мати доступ до історії хвороби для прийняття інформованих рішень. Лікарі повинні мати можливість переглядати попередні діагнози, результати лабораторних досліджень та інші медичні дані для правильної діагностики та лікування. Забезпечення цілісності медичної інформації допомагає зменшити ризик помилок при прийнятті рішень, оскільки лікарі можуть покладатися на достовірну історію хвороби пацієнта.

Пацієнти з хронічними захворюваннями потребують постійного моніторингу та надання лікування відповідно до їхнього стану. У контексті цілісності важливі такі аспекти [18 - 20]:

1. Точна інформація для лікаря і пацієнта. Забезпечення цілісності даних допомагає лікарям та пацієнтам отримувати точну інформацію про хід хвороби та відповідати на зміни у стані пацієнта.

2. Попередження погіршення стану. Лікарі можуть вчасно реагувати на зміни в показниках пацієнта, щоб уникнути загострення хронічних захворювань.

Нарешті, обмін медичною інформацією між медичними установами є не менш важливим аспектом, який ставить вимоги до цілісності медичних записів. Медична інформація повинна лишатися незмінною під час передачі між установами, щоб уникнути помилок у діагностиці та лікуванні. Медичні установи повинні мати доступ до повної історії лікування пацієнта, щоб надавати якісну медичну допомогу.

2.3 Вимоги до доступності медичних даних

Доступність медичних даних означає, що система повинна забезпечувати швидкий та надійний доступ до цих даних, коли він необхідний. У ситуаціях, де швидкий доступ може врятувати життя, доступність даних є критичною. Система повинна мати високий рівень доступності, бекапи та відновлення даних, щоб уникнути втрати медичної інформації в разі виникнення аварій або збоїв в роботі системи. Також важливо мати механізми авторизації, які забезпечують доступ до медичних даних тільки відповідно авторизованим користувачам.

Тобто, при досягненні доступності треба врахувати наступні аспекти [21]:

– система повинна мати високий рівень доступності, щоб надавати медичну інформацію у будь-який момент, навіть під час надзвичайних ситуацій;

– резервне копіювання та відновлення – наявність механізмів для регулярного резервного копіювання даних та їх відновлення в разі аварій чи збоїв в системі;

– скорочення відмов – вдосконалення стійкості медичних систем до відмов і забезпечення постійного доступу до даних (система повинна

автоматично перевіряти стан даних і виявляти можливі проблеми в доступності, щоб швидко реагувати та усувати їх).

Якщо більш детально заглибитись у питання доступності, то треба сказати, що сучасному світі доступність медичних даних відіграє вирішальну роль у забезпеченні ефективної системи охорони здоров'я. У багатьох ситуаціях, особливо в надзвичайних обставинах, швидкий та надійний доступ до медичних даних може виявитися критичним для рятування життя пацієнтів.

З огляду на стрімкий розвиток технологій та комп'ютеризацію сфери охорони здоров'я, електронні медичні записи стали необхідністю у сучасній медицині. Зараз більшість медичних даних зберігається та обробляється у цифровому форматі, що робить можливим їхню швидку та легку доступність:

1) Електронні медичні картки. Багато лікарень та медичних установ впроваджують системи електронних медичних карток для своїх пацієнтів. Кожен пацієнт має електронну картку, в якій зберігаються дані про їхню медичну історію, рецепти, результати аналізів і обстежень. Лікарі мають доступ до цих даних з будь-якого медичного пристрою, що підключений до мережі.

2) Електронні рецепти. В деяких країнах електронні рецепти замінюють паперові. Лікарі можуть надсилати рецепти прямо до аптеки за допомогою електронних систем. Це спрощує і прискорює процес виписування ліків та запобігає помилкам при розгортанні рецептів.

3) Телемедицина. За допомогою телемедицини пацієнти можуть отримувати консультації лікарів віддалено. Лікарі можуть переглядати медичні записи пацієнтів та надавати поради та лікування через відеозв'язок, що дозволяє швидко та ефективно надавати медичну допомогу.

4) Діагностичні засоби з електронними звітами. Медичні прилади для діагностики, такі як рентгенівські апарати або магнітно-резонансні томографи, генерують цифрові зображення та звіти. Це дозволяє лікарям миттєво переглядати та аналізувати результати обстеження та визначати діагнози.

5) Мобільні додатки для здоров'я: Існують різноманітні мобільні додатки, які дозволяють пацієнтам вести власний медичний журнал, слідкувати

за станом здоров'я та зберігати дані про прийом ліків. Ці дані можуть бути легко доступні для лікарів у разі потреби.

У багатьох випадках доступ до медичних даних може вирішити питання про життя та смерть. Наприклад, під час надзвичайних ситуацій, таких як серцевий напад, травми або отруєння, лікарі повинні оперативно отримати доступ до історії хвороби та медичних даних пацієнта, щоб прийняти найкращі рішення щодо діагностики та лікування.

У випадку серцевого нападу кожна секунда має велике значення. Медичні дані пацієнта, такі як попередні інфаркти, алергії на ліки, аналізи крові та ЕКГ-результати, необхідні лікарям для швидкої діагностики та вибору найефективніших методів лікування. Доступ до цих даних може врятувати життя та попередити подальше поширення ураження серця.

Якщо людина отримала травми (аварії, падіння або нещасні випадки) медичний персонал повинен оперативно оцінити стан постраждалих осіб. Знання попередніх травм, алергій, хірургічних втручань та інших медичних фактів є надзвичайно важливими для прийняття рішень щодо подальшого лікування.

У випадку, наприклад, отруєння швидкий доступ до історії хвороби та медичних даних пацієнта може допомогти визначити тип отрути (наприклад, якщо людина працює на шкідливому виробництві, або отримує лікування препаратами, які при передозуванні можуть вести до гострої інтоксикації) та надати необхідну антидотну допомогу. Затримка у доступі до цих даних може призвести до серйозних ускладнень.

Вимога до наявності механізмів резервного копіювання та відновлення медичних даних стає критичною для забезпечення доступності цих даних у будь-якій ситуації. Наведемо декілька прикладів, що ілюструють важливість цього аспекту в контексті доступності медичної інформації:

1. Аварійна ситуація у лікарні під час природної катастрофи. Наприклад, при надходженні надзвичайного стихійного лиха, такого як землетрус чи повінь, може статися пошкодження обладнання та інфраструктури

лікарні. У такому випадку система регулярного резервного копіювання забезпечить, що медичні дані не втратяться, а можуть бути відновлені на інших серверах чи в хмарному сховищі, щоб забезпечити продовження надання медичної допомоги пацієнтам.

2. Вірусні атаки та кіберзлочинці. Кіберзлочинці можуть атакувати медичні системи та зашифровувати дані у вимогах викупу. Якщо система має механізми регулярного резервного копіювання, адміністратори можуть відновити дані з неушкоджених копій та уникнути втрати доступу до медичної інформації.

3. Помилки та випадкова видалення даних. Навіть у безаварійних умовах, помилкові дії персоналу можуть призвести до втрати важливих медичних записів. Існування резервних копій дозволяє відновити дані після таких помилок та зберегти доступність даних для лікарів і пацієнтів.

4. Планове обслуговування та оновлення систем. Під час планового обслуговування медичних систем, таких як оновлення програмного забезпечення чи обладнання, може бути вимкнено доступ до даних. Проте існування резервних копій дозволяє забезпечити доступність медичних записів після завершення таких процедур.

Всі ці приклади підкреслюють значущість механізмів резервного копіювання та відновлення медичних даних для забезпечення надійного та постійного доступу до них. Вони гарантують, що жодна ситуація, чи то аварія, кібератака, помилка чи планове обслуговування, не завадить доступності важливої медичної інформації для медичного персоналу та пацієнтів.

Вимога до системи скорочення відмов та забезпечення стійкості медичних систем стає важливою для забезпечення неперервного доступу до медичних даних. Нижче подано приклади, які допомагають зрозуміти, чому ця вимога така критична [22 – 24]:

1. Мережеві збої. У великих медичних установах мережеві збої можуть спричинити тимчасовий втрату зв'язку з серверами медичних записів. Система,

яка автоматично виявляє ці збої та переключається на альтернативні мережеві шляхи, дозволяє уникнути втрати доступності даних.

2. Навантаження системи. У надзвичайних ситуаціях, наприклад, під час масових подій або пандемій, навантаження на медичні системи може зростати значно. Ефективна система моніторингу може виявити підвищену навантаження та автоматично розподілити ресурси, щоб забезпечити доступність даних для всіх користувачів.

3. Забруднення даних. Поява помилкових або забруднених даних у медичних записах може призвести до великих проблем. Система, яка автоматично виявляє та ізолює забруднені дані, допомагає зберегти точність та достовірність медичної інформації.

4. Системні відмови. Спроможність системи автоматично виявляти та відновлювати роботу в разі системних відмов або падінь серверів є важливою. Це дозволяє забезпечити практично неперервний доступ до медичних даних, навіть у випадку серйозних системних збоїв.

5. Забезпечення безпеки. Вдосконалення стійкості систем також включає в себе заходи для запобігання кібератакам та забезпечення безпеки даних. Системи виявлення вторгнень та захисту від кіберзагроз допомагають забезпечити доступність медичних записів, захищаючи їх від несанкціонованого доступу.

Наведені вище приклади демонструють, що скорочення відмов і забезпечення стійкості медичних систем є критично важливими для забезпечення доступності медичних даних навіть у випадках виникнення непередбачуваних обставин чи проблем у системі. Ретельне планування, моніторинг і вдосконалення цих механізмів допомагають підтримувати доступність медичних даних на високому рівні.

2.4 Аналіз існуючих загроз безпеці медичних записів

У цьому підпункті розділу аналізуються існуючі загрози та потенційні атаки на безпеку медичних записів. Це включає в себе загрози, які можуть виникнути як внаслідок технічних вразливостей, так і через людські дії. Детальний аналіз допомагає визначити потреби в захисті та прийняти відповідні заходи щодо кібербезпеки для зберігання медичних записів за допомогою блокчейн.

Перш ніж перейдемо до аналізу атак, оцінимо потенційні наслідки. Атаки на безпеку медичних записів можуть мати серйозні наслідки для різних зацікавлених сторін, включаючи пацієнтів, медичні установи та інших. Наведемо декілька можливих наслідки цих атак [25 - 27] :

1. Пацієнти:

a. Якщо атака призведе до витоку медичних даних, пацієнти можуть стати жертвами порушення конфіденційності. Наприклад, їхні особисті дані, діагнози, лікування та інша конфіденційна інформація можуть опинитися в руках зловмисників або сторонніх осіб.

b. Якщо медична інформація використовується для здійснення шахрайства або ідентифікації пацієнтів, це може призвести до фізичних ризиків для них. Наприклад, зловмисники можуть використовувати медичну інформацію для вчинення шахрайств чи погроз.

c. Витік медичної інформації може призвести до загального втрати довіри пацієнтів до медичних установ і технологій, які використовуються для зберігання їхніх даних.

2. Медичні установи:

a. Витік медичної інформації може призвести до суттєвих порушень конфіденційності пацієнтів і спричинити їм матеріальні збитки або шкоду.

b. Порушення конфіденційності медичних записів може призвести до значних втрат репутації для медичних установ, що може вплинути на їхню здатність привертати пацієнтів і співпрацювати з іншими медичними організаціями.

c. Атаки, такі як вимагання викупу, можуть призвести до фінансових втрат, які пов'язані з відновленням систем та компенсацією пацієнтам, чий медичний запис був пошкоджений.

3. Інші зацікавлені сторони:

a. Може виникнути ситуація, коли інші зацікавлені сторони, такі як страхові компанії або правоохоронні органи, можуть бути втягнуті в юридичні питання та розслідування.

b. Інші організації можуть мати доступ до медичних даних пацієнтів (наприклад, лабораторії або страхові компанії), і вони також можуть зазнати втрат в разі атаки.

4. Системи охорони здоров'я загалом:

a. Атаки можуть призвести до порушення нормативних вимог щодо захисту медичної інформації, що може призвести до санкцій та штрафів.

b. Якщо атаки вплинуть на доступ до медичних записів пацієнтів, це може мати серйозні наслідки для їхнього здоров'я, оскільки лікарі можуть не мати доступу до критичної інформації про стан пацієнта.

Далі розглянемо атаки, з якими стикаються традиційні системи зберігання медичних даних.

Атака на конфіденційність – загроза полягає в неправомірному доступі до конфіденційних медичних даних. Зловмисники, які отримують доступ до логінів та паролів медичного персоналу (наприклад, персонал використовує слабкі паролі), можуть зламати систему та отримати доступ до чутливої інформації про пацієнтів. Наприклад, зловмисники можуть використовувати отриману інформацію для вимагання викупу або для продажу конфіденційних медичних даних на чорному ринку.

Атака на цілісність – тут загроза полягає в маніпуляції медичними записами з метою зміни даних або введення хибної інформації. Це може призвести до надання невірних діагнозів або лікування, що загрожує здоров'ю пацієнтів. Зловмисники можуть змінити діагноз або результати аналізів в медичних записах, що може вплинути на подальше лікування.

Атака на доступність – дана загроза включає збої в системі або кібератаки, які можуть призвести до тимчасової недоступності медичних даних. У критичних моментах, коли лікар потребує доступу до інформації пацієнта, це може бути життєво важливо. Наприклад, DDoS-атака (такі атаки можуть призвести до перекриття доступу до системи, що може бути особливо небезпечним у ситуаціях, коли потрібно негайний доступ до медичної інформації) може перевантажити мережу і зробити систему електронної медичної історії (EMR) недоступною. Велика DDoS-атака може паралізувати роботу лікарні, що загрожує пацієнтам в екстрених ситуаціях.

Фішингові атаки – це спроби отримати конфіденційну інформацію, таку як паролі або облікові записи, від лікарів або персоналу медичних установ, використовуючи підроблені комунікації чи веб-сайти.

Соціальний інжиніринг – загроза включає в себе обман медичного персоналу або інших учасників системи з метою отримання доступу до конфіденційних даних. Зловмисники можуть використовувати фішингові атаки або соціальні маніпуляції для цього, наприклад, психологічний тиск на персонал, щоб отримати доступ до паролів або інших облікових даних.

Витік інформації – це процес незаконного виходу або розголошення конфіденційної інформації, який може стати наслідком атаки на конфіденційність, але має свої особливості. Відмінність в тому, що в атаках на конфіденційність зазвичай хакери намагаються отримати доступ до інформації для власного використання або вимагання викупу, тоді як витік інформації відбувається вже після отримання доступу до конфіденційних даних і може включати їхнє незаконне розголошення або продаж. Це може призвести до серйозних наслідків, таких як порушення конфіденційності пацієнта, негативний вплив на репутацію організації або навіть фінансові втрати для пацієнтів і лікарень.

Змінення ідентифікаційних даних – зловмисники можуть змінювати ідентифікаційні дані пацієнтів або лікарів, щоб отримати неправомірний доступ до медичних послуг або страхових виплат. Наприклад, можна змінити ім'я

пацієнта або інші ідентифікаційні дані для отримання лікування за чужим обліковим записом.

Внутрішні загрози – іноді інсайдери, такі як лікарі чи персонал медичних установ, можуть стати загрозою безпеці, намагаючись незаконно отримати, використовувати або розголошувати конфіденційні медичні дані.

Маніпуляція даними в мережі – зловмисники можуть перехоплювати і маніпулювати медичними даними під час їх передачі по мережі.

Як бачимо, запобігання цим загрозам включає в себе впровадження високих стандартів безпеки, моніторинг і виявлення інцидентів, навчання персоналу та регулярне оновлення заходів безпеки, щоб захистити медичну інформацію пацієнтів і забезпечити її конфіденційність, цілісність та доступність. Системи з традиційними алгоритмами зберігання медичних даних вимагають багато ресурсів для захисту, в особливості для захисту периметру.

Блокчейн технологія вже за своїм дизайном змінює парадигму до захисту, оскільки частина атак стає неактуальною. Блокчейн-системи мають свої особливості, які можуть зменшити або усунути деякі звичайні загрози, що стосуються традиційних систем зберігання медичних записів. До таких загроз можна віднести:

– витік інформації через втрату фізичного носія даних – блокчейн, зазвичай, не залежить від фізичних носіїв даних, таких як USB-накопичувачі, оскільки дані зберігаються в розподілених мережах, тому загублення або крадіжка фізичного носія дуже ускладнена і часто не має сенсу;

– *фішинг* – блокчейн-системи можуть використовувати сильну криптографію і автентифікацію за допомогою криптографічних ключів, що робить їх менш вразливими до атак фішингу (зловмисникам не вдасться здійснити аутентифікацію без правильного ключа);

– *маніпуляція даними в мережі* – хеш-функції для підтвердження цілісності даних ускладнюють маніпуляції даними під час передачі через мережу, крім того, транзакції в блокчейні підлягають підтвердженню мережею, що знижує ризик нелегітимних змін.

– *внутрішні загрози* – блокчейн-системи можуть встановлювати рівні доступу та контролю доступу, що допомагає керувати ризиком внутрішніх загроз;

– *централізована атака на сервер* – оскільки блокчейн часто є розподіленою системою без центрального сервера, централізована атака на сервер майже неможлива. Це робить систему менш вразливою та більш *відмовостійкою*;

– *атаки Man-in-the-Middle* – блокчейн використовує криптографію для забезпечення конфіденційності та цілісності даних, що робить атаки даного типу безуспішними. Зловмисникам технічно дуже важко перехопити та модифікувати дані;

– *атаки на конфіденційність даних* – зазвичай вміст блокчейну доступний лише обмеженому колу учасників з відповідними правами доступу (це робить атаки на конфіденційність даних складнішими для виконання, оскільки несанкціонованим особам важко отримати доступ до конфіденційної інформації).

Однак існують атаки, до яких може бути чутлива і система, реалізована із застосуванням блокчейн технології. Вони нерідко потребують багато ресурсів, але із ростом популярності технології з'являються і нові виклики, і нові рішення для захисту. Наведемо кілька прикладів атак, до яких може бути чутлива блокчейн-система:

– *51% атака (51% Attack)* – зловмисник намагається контролювати більше половини обчислювальної потужності (хешрейту) мережі. Якщо вдалося отримати більше 51% потужності, зловмисник може маніпулювати транзакціями та історією;

– *атака на консенсус (Consensus Attack)* – зловмисники можуть намагатися перешкодити процесу досягнення консенсусу в мережі, таким чином впливаючи на правильність транзакцій та блоків;

– *векторні атаки на блокчейн (Blockchain Vector Attacks)* – це атаки, спрямовані на вразливості програмного забезпечення в мережі, такі як недоліки

у реалізації смарт-контрактів, які можуть призвести до втрати коштів або інших проблем;

– *атака на індивідуальні користувацькі ключі* – якщо користувач втратив (скомпрометував/розголосив) свій приватний ключ до гаманця або облікового запису, то зловмисники можуть використовувати це для відкриття доступу до його активів або даних;

– *соціальна інженерія* – зловмисники можуть намагатися обманом використовувати соціальну інженерію для отримання ключів або паролів від користувачів;

– *атака на смарт-контракти* – якщо смарт-контракт має недоліки або помилки в коді, це може призвести до виконання небажаних дій або втрати коштів користувачів;

– *дослідницька атака (Research Attack) на приватність* – в деяких випадках реалізація публічного блокчейна може розголошувати інформацію про транзакції, що порушує приватність користувачів (зловмисник може проаналізувати графік транзакцій; якщо користувач бере участь в низці транзакцій, його активність може бути використана для створення повного зображення його фінансових дій; іноді витрати на транзакції можуть розкрити інформацію про те, що користувач робить і т.д.);

– *атака на голосування (Blockchain Voting Attack)* – у виборчих системах на блокчейні зловмисники можуть намагатися фальсифікувати голоси або перехоплювати виборчий процес. Такі атаки можуть вплинути на результати голосування і вибори.

І хоча блокчейн має видимі переваги, важливо пам'ятати, що жодна система не є абсолютно безпечною, і вона може бути вразливою до нових загроз чи атак, особливо якщо не дотримуватися високих стандартів безпеки та обережності. Також, безпека блокчейну може залежати від впровадження інших технічних заходів безпеки, таких як захищені ключі і процедури автентифікації.

3. РОЗРОБКА АЛГОРИТМІВ БЕЗПЕЧНОГО ЗБЕРІГАННЯ МЕДИЧНИХ ЗАПИСІВ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Перш ніж приступити до аналізу і розробки, розглянемо існуючі рішення для зберігання медичних записів та основні принципові підходи.

3.1 Огляд існуючих рішень для зберігання медичних записів

На сьогодні існують різні рішення для зберігання медичних записів. Варто сказати, що деякі з них навіть використовують блокчейн, але більшість обирає традиційно зберігати дані на централізованих серверах. Розглянемо декілька прикладів разом з основними принципами роботи, перевагами та недоліками [28]:

1. Epic Systems Corporation.

За своїм принципом роботи – це інтегрована система управління медичними записами, яка забезпечує зберігання та обмін медичними даними між різними лікарнями та медичними закладами. Дана система широко використовується у США, є інтегрованим рішенням для медичних організацій, добре підтримує стандарти безпеки даних у сфері охорони здоров'я. Але система дорога у впровадженні та підтримці, може бути обмеженою для обміну даними між різними медичними системами. Вразлива до атак на централізовані сервери.

2. IBM Watson Health.

Система використовує розподілену обчислювальну платформу для аналізу та зберігання медичних даних. Що є перевагою – працює з великими обсягами даних, може надавати аналітичні рішення для медичних закладів, що допомагає виявляти закономірності та покращувати діагностику. Але питання конфіденційності та безпеки даних можуть все рівно можуть виникати, оскільки дані зазвичай зберігаються на централізованих серверах.

3. OpenEHR.

Рішення використовує відкритий стандарт для представлення медичних даних та їхнього зберігання. Дозволяє зберігати дані в структурованому форматі.

Відкритий стандарт сприяє інтероперабельності, дозволяє зберігати дані у форматі, який не обмежується конкретною платформою. Але впровадження та сумісність з іншими системами є дуже комплексною задачею.

4. Медична інформаційна система Китаю (CMIS):

Ця система зберігає медичні дані пацієнтів в розподіленій базі даних та забезпечує доступ до них лікарям у Китаї.

Вона покликана покращити доступ до медичних записів та координацію догляду, але занадто централізована та можлива вразливість щодо конфіденційності.

5. MedRec (заснований на Ethereum).

Використовує технологію блокчейн для зберігання медичних записів та надає кожному пацієнту контроль над своєю медичною інформацією. Із переваг треба відмітити дійсно високу безпеку і конфіденційність завдяки криптографії, пацієнти мають контроль над своєю інформацією. Але є і недоліки у реалізації – система вимагає значних зусиль для впровадження, витратна та надалі потребує комплексної та активної підтримки для сумісності з іншими системами.

Незважаючи на багато спільних принципів, в тому числі на те, що усі ці системи прагнуть забезпечити конфіденційність медичних даних, вони стикаються з рядом викликів і обмежень:

1. Слабка інтероперабельність – в одних системах дані можуть бути представлені у форматі, який важко інтерпретувати для інших систем. Це ускладнює обмін даними між різними медичними закладами та системами.

2. Брак стандартизації – в сфері медичної інформатики все ще не вистачає загальної стандартизації для формату даних, обміну даними та взаємодії між системами. Це може ускладнювати інтеграцію різних рішень.

3. Проблеми з приватністю та безпекою – навіть у великих системах, як Epic, виникають проблеми з конфіденційністю та безпекою даних, особливо з огляду на постійні загрози кібербезпеці.

4. Високі витрати на впровадження та підтримку – великі системи, як Epic, дуже дорогі у впровадженні та підтримці, що робить їх недосяжними для менших медичних закладів.

5. Адаптація до нових технологій – швидкі зміни в області інформаційних технологій можуть ускладнювати зберігання та обмін медичними даними, оскільки системи мають постійно адаптуватися до нових технологічних вимог. Виникають питання сумісності.

6. Етичні питання та законодавство – зберігання та обмін медичними даними також пов'язані з етичними питаннями та законодавством, особливо в сфері захисту приватності пацієнтів. Необхідно дотримуватися законів щодо обробки медичних даних. А отже система має бути регулюватися, що також треба врахувати при проектуванні архітектури із застосуванням блокчейн.

3.2 Вибір типу блокчейну

В залежності від того, чи потрібно отримувати дозвіл на роботу у блокчейн-мережі, чи будь-хто може брати участь у її роботі, виділяють публічні блокчейни – permissionless, а також приватні блокчейни – permissioned (дозвіл на доступ до системи потрібен).

Зберігання медичних даних на публічних та приватних блокчейнах вимагає ретельного аналізу та вибору оптимального підходу з урахуванням різниці у властивостях та потребах кожного типу блокчейну та кінцевої системи. Проведемо більш докладне порівняння властивостей.

Для публічного блокчейну характерні [29]:

1. *Прозорість та відсутність необхідності комусь довіряти* – публічний блокчейн має відкритий доступ до всіх даних та транзакцій у мережі.

Це забезпечує високий рівень довіри (у контексті, що ви довіряєте більшості спільноти, а не визначеній групі користувачів) і можливість перевірки операцій (аудит).

2. *Децентралізація* – система децентралізована, а це означає, що дані розподілені по вузлах у мережі. Це забезпечує високий рівень безпеки і захищеності від відмов та зовнішніх атак.

3. *Увага до конфіденційності* – приватність даних може страждати, оскільки всі транзакції та дані є публічними. Для збереження конфіденційності можливе використання шифрування або анонімність гаманців, але при неурахуванні усіх вимог конфіденційність даних може страждати (наприклад, та ж дослідницька атака), тому треба ретельно вивчати питання.

Прикладами публічних блокчейнів є Ethereum або Bitcoin, відомі своєю високою стійкістю до атак та валідністю транзакцій завдяки розподіленому характеру мережі та консенсусу. Однак публічні блокчейни за замовчуванням є анонімними та відкритими для всіх, і всі транзакції на них є гласними. Це може створювати проблеми з конфіденційністю медичних записів, оскільки інформація може бути доступною для будь-якого користувача мережі.

Приватний блокчейн має свої властивості [30]:

1. *Контроль над доступом* – приватний блокчейн керується обраними учасниками, і доступ до даних обмежується. Це забезпечує більший контроль над системою та стійкість до несанкціонованого доступу.

2. *Конфіденційність* – приватний блокчейн за замовчуванням надає більший рівень конфіденційності. Шифрування може бути використано для забезпечення додаткової конфіденційності.

3. *Пропускна здатність і масштабованість* – приватні блокчейни зазвичай мають вищу пропускну здатність (обчислюється у транзакціях за секунду) та масштабованість, оскільки вони менш витратні з точки зору обчислювальних ресурсів.

Отже, приватні блокчейни, на відміну від публічних, можуть мати обмежений доступ та більшу керованість. Це може бути корисним для

збереження конфіденційної медичної інформації. Прикладами реалізації приватного блокчейну є Hyperledger Fabric, Corda, Quorum і тд., основний фокус яких спрямований на посилення конфіденційності та налаштування рівнів доступу до даних.

Узагальнимо переваги і недоліки публічного і приватного блокчейнів у даному контексті (таблиця 3.1).

Таблиця 3.1 - переваги і недоліки приватного і публічного блокчейнів

Характеристика	Публічний блокчейн	Приватний блокчейн
Переваги		
Прозорість і довіра до системи	Так	Зазвичай менше
Висока стійкість до атак та відмов	Так	Зазвичай менше
Децентралізована природа	Так	Може бути менше
Недоліки		
Обмежена конфіденційність даних	Зазвичай так	Може бути краще
Проблема із масштабуванням та швидкістю	Зазвичай так	Може бути краще

Як бачимо із таблиці публічний блокчейн має свої переваги (прозорість і довіра до системи, висока стійкість до атак та відмов, а децентралізована природа забезпечує більшу надійність). Щодо недоліків, то це обмежена

конфіденційність даних та потенційна проблема із масштабуванням та швидкістю обробки транзакцій (пропускною здатністю).

Приватний блокчейн із переваг має більшу довіру до конфіденційності даних, а також контроль над доступом до системи та вищу пропускну здатність і масштабованість. До недоліків можна віднести те, що така система потребує більше довіри через відсутність повної прозорості та має меншу стійкість до атак, оскільки система керується обмеженою кількістю учасників (однак багато залежить від архітектури).

Вибір між публічним і приватним блокчейном повинен базуватися на конкретних потребах і вимогах до конфіденційності, які визначаються для збереження медичних даних в конкретному проекті. Але все ж, проаналізувавши вищеописане, можемо заключити наступне.

Публічні (permissionless) системи блокчейну краще застосовувати в випадках, де потрібно забезпечити громадську доступність та високий рівень прозорості, і коли відкритий доступ для всіх бажаючих важливіший за контроль над конфіденційністю даних та обмеженням учасників. Такі системи найбільш підходять для використання в глобальних мережах та проектах, де цілеспрямована громадська перевірка та громадська довіра є ключовими аспектами, наприклад, у криптовалютних системах, де всі користувачі можуть перевіряти транзакції.

Приватні системи блокчейну (permissioned – з дозволом) найбільш ефективно використовувати у випадках, де велика увага приділяється конфіденційності та безпеці даних, таких як у медицина, фінанси, логістика та урядові ініціативи. У цих областях приватні блокчейни забезпечують високий рівень захисту конфіденційності і дозволяють контролювати доступ до інформації, що є важливими аспектами для дотримання регуляторних вимог та забезпечення безпеки даних у вимогливих середовищах.

Ми розглянули крайні точки, але є і проміжні варіанти між публічними і приватними. Альянс блокчейнів (Alliance Chain) – це термін, який може використовуватися для позначення блокчейн-мереж, створених або

використовуваних альянсами або групами організацій для спільного керування та обміну даними.

Alliance Chain часто є приватною мережею, до якої мають доступ тільки авторизовані користувачі або учасники альянсу. Це забезпечує більший контроль над даними та конфіденційністю.

Учасники альянсу спільно приймають рішення щодо правил та управління мережею. Це різниться від публічних блокчейнів, де рішення приймаються загальнодоступною спільнотою.

Alliance Chain може мати складну систему прав і ролей для різних учасників. Деякі можуть мати право на запис, інші - на перегляд або підтвердження транзакцій.

Часто вони мають вищу швидкість обробки та масштабованість порівняно з публічними блокчейнами, оскільки менше учасників потребують для досягнення консенсусу.

Alliance Chain можуть використовуватись корпораціями та організаціями для розв'язання таких завдань, як обмін даними, відстеження постачання або управління медичними даними.

Відмінність від приватного та публічного блокчейну полягає в тому, що Alliance Chain – це форма приватного блокчейну, створеного для конкретних груп організацій або альянсів. Приватний блокчейн призначений для обмеженого кола учасників, він працює на дозволі і контролюється учасниками мережі. Публічний блокчейн, навпаки, відкритий для всіх і керується глобальною спільнотою, не потребує дозволу і має більшу ступінь децентралізації. Ми виділили Alliance Chain в окрему групу, бо є багато варіантів реалізації таких проміжних рішень у різних конфігураціях.

Нижче наведемо порівняльну характеристику розглянутих типів блокчейнів (таблиця 3.2).

Таблиця 3.2 – Порівняльна характеристика типів блокчейнів

Характеристика	Приватний блокчейн	Публічний блокчейн	Alliance Chain
Рівень доступу	Налаштовується	Відкритий	Налаштовується
Учасники мережі	Які мають дозвіл	Будь-хто	Які мають дозвіл
Децентралізація	Низька	Висока	Середня
Валідатори	Довірені особи	Будь-хто може стати валідатором	Довірені особи
Конфіденційність	Висока	Середня	Висока
Прозорість	Низька	Висока	Середня
Швидкість підтвердження блоків	Висока	Залежнить від механізму досягнення консенсусу	Середня
Вирішення скарг і конфліктів	Централізоване	Відкрите	Помірно децентралізовано
Емісія активів	Централізована	Децентралізована	Тяжіє до централізованої

3.3 Вибір криптографічних методів для захисту даних

Для реалізації описової моделі візьмемо за основу декілька технологічних рішень [18 – 20]:

– блокчейн технологію для реалізації зберігання медичних записів і взаємодії між учасниками (основи технології описані вище);

– протокол обміну ключами за схемою Діффі-Хеллмана;

– симетричне шифрування за стандартом AES256;

– хешування за алгоритмом SHA256;

– алгоритм цифрового підпису на еліптичних кривих ECDSA.

Diffie-Hellman. Протокол обміну ключами за схемою Діффі-Хеллмана, який зазвичай використовується між двома сторонами, у нашому випадку може бути розширений до n сторін. Це дозволить n лікарням, а точніше вузлам лікарень у блокчейн-мережі, створити спільний секрет, який буде однаковим для всіх учасників взаємодії.

Нехай цей спільний секрет буде називатись “Спільний секрет лікарень”. Тоді протокол працюватиме наступним чином (під “лікарня № k” мається на увазі вузол цієї лікарні) [25]:

1. Параметри, такі як модуль групи p та генератор g, повинні бути встановлені завчасно.

2. У кожної лікарні є своя ключова пара, яка складається з приватного ключа a та публічного $A = g^a$. Лікарні знають публічні ключі один одного.

3. Для того, щоб сформувати спільний секрет, лікарня №2 рахує $S_{12} = (g^{a_1})^{a_2} = g^{a_1 a_2}$. Вона може це зробити, так як знає свій приватний ключ a_2 та публічний ключ $A_1 = g^{a_1}$ лікарні №1.

4. Лікарня №2 надсилає отримане значення до лікарні №3.

5. Лікарня №3 обчислює $S_{123} = (S_{12})^{a_3} = (g^{a_1 a_2})^{a_3} = g^{a_1 a_2 a_3}$ та отримує спільний секрет між лікарнями №1, 2 та 3. Ці дані надсилаються до лікарні №4.

6. Лікарня №4 робить такі ж обчислення з отриманим значенням та своїм приватним ключем.

7. Процедура продовжується до тих пір, поки проміжне обчислюване значення не надійде до останньої лікарні № n. Зробивши ці самі обчислення, у останньої лікарні буде спільний секрет між усіма лікарнями. Це “коло обчислень” може початись з лікарні №3 і закінчитись на лікарні №1. В такому випадку у лікарні №1 буде спільний секрет усіх лікарень. Цей алгоритм повинні пройти усі лікарні системи, щоб у всіх був спільний секрет.

Таким чином пацієнт, який має встановлений додаток (цей додаток буде відповідати за отримання та зберігання даних пацієнта, його ключів тощо), при реєстрації в лікарні (наприклад, підписання декларації з лікарем) отримає “спільний ключ лікарень” та зможе обчислити спільний секрет між лікарнями та собою – $S_P = (S_{1\ldots n})^u$, де u - приватний ключ пацієнта. Цим секретом будуть шифруватись та розшифровуватись документи пацієнта, які будуть зберігатись в блокчейні.

Ми вважаємо, що у даному випадку доцільно мати довірену сторону – “Міністерство”, яка підтримується та захищається державою та має ключові пари усіх лікарень, користувачів та додаткові ключі для лікарень, які буде створено у майбутньому. У практичній реалізації спільний секрет лікарень буде обчислюватися із самого початку з урахуванням усіх додаткових ключів із резерву для майбутніх лікарень (це число повинно обрано заздалегідь відповідно до критеріїв бажаної масштабованості системи). Таким чином, вузол лікарні зможе звернутись до вузла міністерства та отримати обрахований спільний секрет. В такому випадку усі обчислення будуть відбуватись на боці “Міністерства” (ми рахуємо, що його інфраструктура з точки зору безпеки управління ключами буде надійно захищатися найсучаснішими криптографічними стандартами).

Дані користувача (документи про сдачу аналізів, стан здоров’я тощо) будуть шифруватись спільним секретом між лікарнями та користувачем, як

зазначено вище. Отже, користувач має можливість знайти свої документи в блокчейні (це буде робити додаток) та розшифрувати їх.

SHA256. SHA-256 (Secure Hash Algorithm 256-bit) — це частина криптографічної хеш-функції сімейства SHA-2, розроблена Агентством національної безпеки (NSA) Сполучених Штатів. Ми пропонуємо використовувати саме цю хеш-функцію, або її варіант з більшим значенням хеш-значення, що забезпечить більшу безпеку.

Алгоритм виробляє 256-бітне (32-байтове) хеш-значення, яке зазвичай відображається як шістнадцяткове число довжиною 64 цифри.

SHA-256 є односторонньою функцією, тобто вона перетворює вхідні дані в хеш фіксованого розміру, але процес не можна повернути назад, щоб отримати вихідні дані.

Він детермінований, тому однакові вхідні дані завжди призведуть до того самого хешу, але навіть невелика зміна вхідних даних дає істотно інший результат.

Функція розроблена таким чином, щоб бути стійкою до зіткнень, що робить надзвичайно складним пошук двох різних вхідних даних, які дають однакове хеш-значення.

SHA-256 обробляє дані блоками по 512 бітів і включає доповнення та кодування довжини, щоб гарантувати, що загальна довжина даних є кратною 512 бітам.

Алгоритм використовує побітові операції, логічні функції та модульні доповнення для змішування вхідних даних у кінцевий хеш.

SHA-256 широко використовується в різних додатках і протоколах безпеки, включаючи TLS і SSL, PGP і блокчейн Bitcoin для перевірки цілісності та автентичності даних.

Його високий рівень безпеки робить його придатним для цифрових підписів, створення сертифікатів та інших криптографічних цілей, де потрібен безпечний і унікальний ідентифікатор для даних.

Алгоритм буде використаний для обчислення хеш-значень блоків, документів пацієнта (потрібно для підпису) тощо.

AES256. AES (Advanced Encryption Standard) – це алгоритм шифрування з симетричним ключем, який широко використовується для безпечної передачі даних. AES256 відноситься до AES з 256-бітним ключем, що є найдовшим розміром ключа, який він підтримує, що забезпечує високий рівень безпеки. Він працює з блоками даних фіксованого розміру (128 біт), використовуючи низку перетворень. Дані розбиваються на блоки фіксованого розміру та шифруються.

Симетричним ключем у нашому випадку буде виступати спільний секрет між лікарнями та пацієнтом. Алгоритм також має функцію розшифрування, яка приймає на вхід зашифровані дані (документ пацієнта) та ключ яким зашифрувались ці дані, і повертає дані в розшифрованому вигляді. За допомогою шифрування буде забезпечуватись конфіденційність даних пацієнта – лише лікарні, міністерство та сам пацієнт зможуть їх розшифрувати.

ECDSA. ECDSA (алгоритм цифрового підпису на еліптичній кривій) – це криптографічний алгоритм, який використовується для цифрових підписів і базується на теорії еліптичних кривих.

Сильна сторона ECDSA полягає в складності вирішення проблеми дискретного логарифмування еліптичної кривої, фундаментальної проблеми в теорії чисел. Алгоритм цифрового підпису подібний до звичайного підпису на документі, але цифровий підпис можна використовувати в інформаційних системах та для автентифікації сторін.

Підпис – це пара чисел, отриманих із вибраного випадкового числа, закритого ключа та хеш-значення повідомлення. Щоб підписати повідомлення, відправник спочатку генерує випадкове число, потім обчислює точку на кривій, використовуючи це число, і, нарешті, обчислює підпис, використовуючи цю точку, закритий ключ і хеш повідомлення (рисунок 3.1).

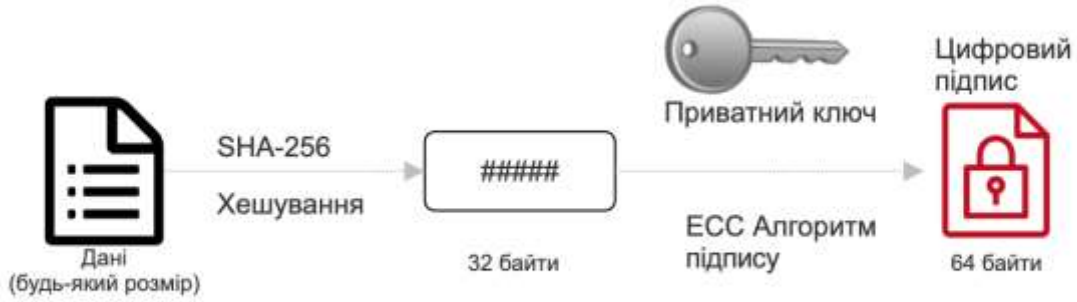

Рисунок 3.1 – Формування цифрового підпису

Щоб перевірити підпис, одержувач використовує відкритий ключ, хеш повідомлення та підпис для виконання обчислень, які включають точки на кривій (рисунок 3.2).

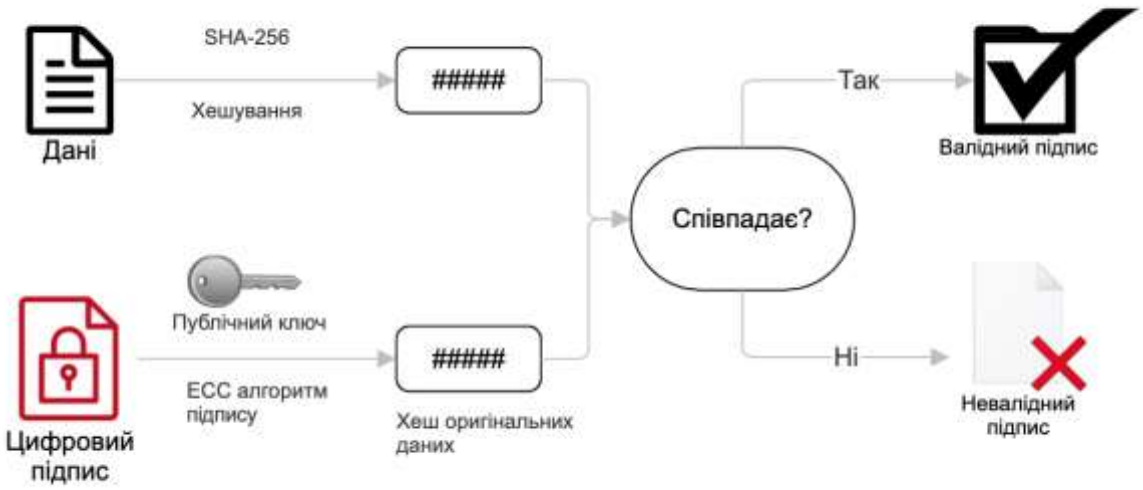

Рисунок 3.2 – Перевірка цифрового підпису

Якщо обчислення вірні – підпис дійсний. Цей процес використовує властивості еліптичної кривої та проблеми дискретного логарифмування.

ECDSA пропонує вищий рівень безпеки, ніж традиційний DSA для даного розміру ключа, дозволяючи використовувати коротші ключі для аналогічних рівнів безпеки. Він широко використовується в різних програмах,

включаючи SSL/TLS для безпечного веб-зв’язку, транзакцій у криптовалюті та цифрової перевірки особи.

Ми пропонуємо використовувати ECDSA для автентифікації вузлів лікарень, згоди пацієнта на надання послуг (лікування) і для підпису лікарем документів пацієнта.

3.4 Розробка алгоритму зберігання медичних записів

У запропонованій ідеї (Proof-of-Concept) описової моделі маємо n лікарень, кожна з яких підтримує свій вузол у блокчейн-мережі, з’єднаний з вузлами інших лікарень та має можливість надіслати запит до вузла міністерства (рисунок 3.3).

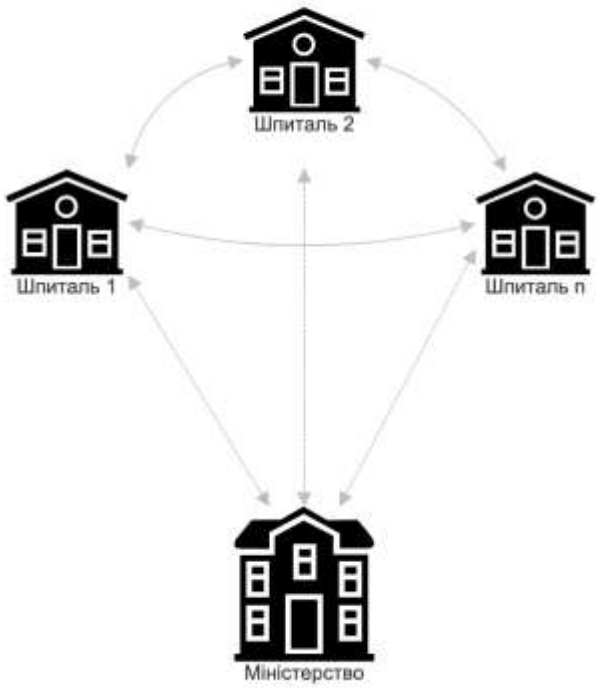

Рисунок 3.3 – Взаємодія вузлів лікарень з вузлом міністерства

У кожного пацієнта та працівника лікарні є встановлений додаток, який відповідає за взаємодію з ключами, надсилання запитів до серверів лікарень або міністерства та за отримання і зберігання даних пацієнта.

Вузли лікарень мають з’єднання один з одним та разом утворюють блокчейн-мережу (рисунок 3.4). Вузли відповідають за створення блоків, обробку запитів та мають досягати консенсусу один з одним на рахунок стану спільної бази даних (блокчейну). В блоках зберігатимуться зашифровані документи пацієнтів.

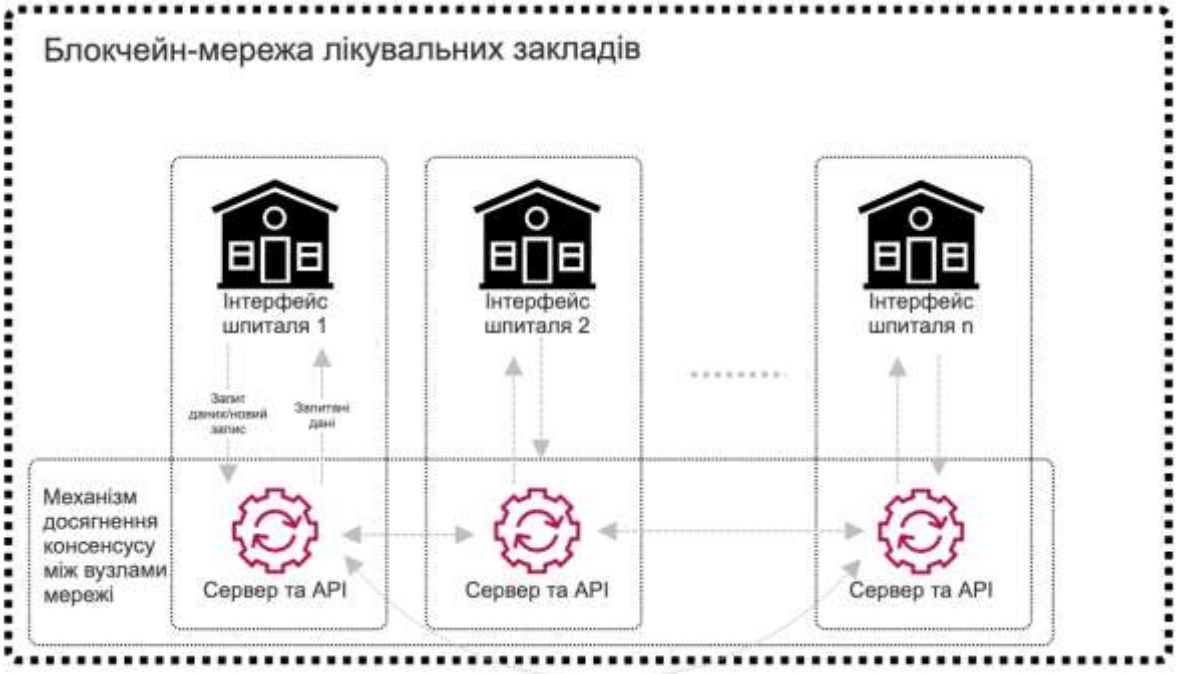

Рисунок 3.4 – Однорівнева мережа лікувальних закладів та схема участі у досягненні консенсусу

На рисунку нижче (рисунок 3.5) зображена запропонована інфраструктура, в яку входять:

1. Блокчейн-мережа лікувальних закладів.

a. Кожна лікарня має свій вузол, який з’єднаний з усіма вузлами інших лікарень.

b. Вузли обмінюються отриманими повідомлення від додатків користувачів. Їх можуть відправляти як лікарі, так і пацієнти, але повідомлення

від лікарів можуть вносити “нові” записи, а повідомлення від пацієнтів можуть лише отримувати інформацію про записи, які їх стосуються.

c. Вузол лікарні 1, отримавши повідомлення від користувача-лікаря, додає до нього системну інформацію, підписує та надсилає його вузлам усіх інших лікувальних закладів.

d. Вузли лікарень 2, 3, … n, отримавши це повідомлення, перевіряють підпис вузла лікарні 1. Якщо підпис валідний – перевірка вважається успішною, і вузол додає це повідомлення до “списку транзакцій, які очікують на відправку” (мається на увазі на відправку в блокчейн-реєстр).

e. Алгоритм досягнення консенсусу PoA припускає наявність вузла-лідера, який може змінюватися з часом та є одним з вузлів лікарень. В певний момент часу вузол-лідер формує новий блок з наявними в нього повідомленнями з “списку транзакцій, які очікують на відправку”, підписує цей блок та надсилає усім іншим вузлам.

f. Вузли інших лікарень перевіряють блок (підпис лідера, правильність формування блоку, наявність в ньому усіх або більшості повідомлень зі списку) і у позитивному випадку перевірки – додають його до своєї бази даних (локального блокчейн реєстру).

g. На кінцевому кроці всі вузли додадуть новий блок до локального блокчейн-реєстру, що означає, що консенсус досягнутий і локальні реєстри у всіх вузлів лікарень однакові.

2. Блокчейн реєстр, який фактично є базою даних у кожного вузла.

3. Міністерство, яке вважається надійно захищеною третьою стороною. Воно не приймає участь у досягненні консенсусу, але за потреби (наприклад, запитом від вузла лікарні) може надати лікарням потрібні ключі (спільні секрети лікарень, або ж секрет між лікарнями та користувачем).

4. Кінцевий користувач. Сюди входять як працівники лікарень, так і пацієнти.

5. Пацієнт може бачити в своєму додатку всю історію своїх документів і, за потреби, звертатись до лікарні, щоб записатись на

консультацію, діагностичні процедури, отримання результатів аналізів тощо. Співробітник лікарні може отримувати доступ до даних конкретного пацієнта (обсяг даних залежить від ролі, наприклад, медична сестра буде бачити тільки актуальні призначення лікаря та алергологічний анамнез; лікар буде бачити повні дані про історію своєї взаємодії з пацієнтом, а за потреби може надіслати запит на отримання усіх даних, які стосуються конкретного пацієнта), вносити зміни (також у залежності від ролі – деяким співробітникам достатньо доступу на перегляд без можливості модифікації) тощо (рисунок 3.5).

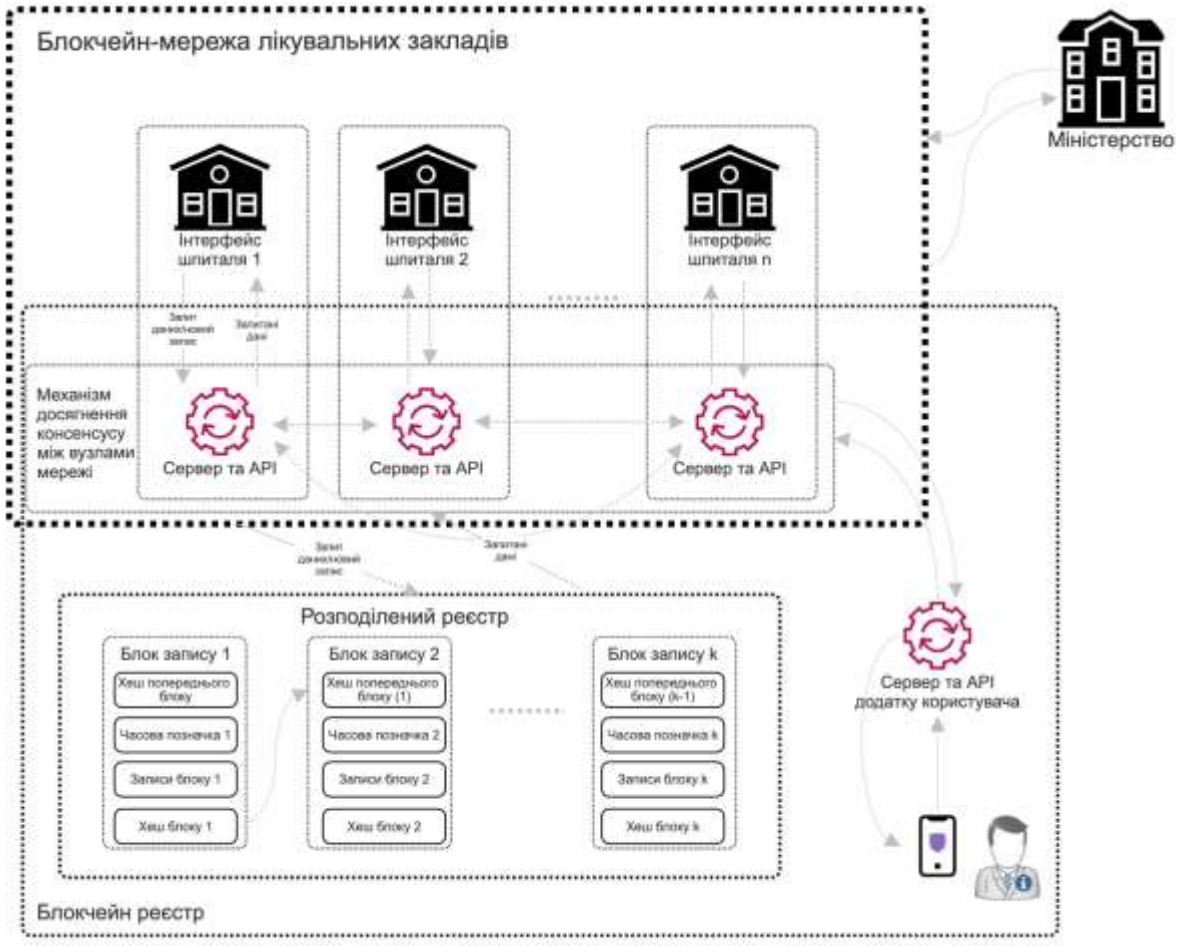

Рисунок 3.5 – Схема системи зберігання медичних записів та взаємодії учасників за допомогою блокчейн технології

Пацієнт, звернувшись вперше до лікарні 1, має пройти процедуру реєстрації, а саме встановити додаток на свій пристрій (смартфон / планшет) та підписати декларацію з лікарем:

1. Пацієнт встановлює додаток, обирає безпечний пароль, та сканує QR-код, згенерований лікарем. Додаток генерує пацієнту ключову пару, використовуючи його пароль та відображає зміст QR-коду — запит на підпис декларації з лікарем та "спільний секрет лікарень" (S_n).

2. Пізніше пацієнту потрібно буде звернутись до міністерства та надіслати свій публічний ключ вузлу міністерства. Він може зробити це через додаток. Можлива опція, коли це може зробити лікарня, яка обслуговує пацієнта.

3. Підписавши документ (декларацію) своїм ключем, додаток пацієнта відправляє підпис та публічний ключ пацієнта лікарю. Лікар перевіряє підпис пацієнта, додає свій підпис та обчислює спільний секрет між ключем пацієнта та спільним секретом лікарень. Далі додаток лікаря зашифровує цим секретом вміст документу. Нарешті повідомлення, яке складається з зашифрованого документу (декларація з доданим підписом користувача), підпису лікаря та системної інформації (до цієї системної інформації входить, наприклад, хеш документу) відправляється до вузла лікарні 1.

4. Отримавши це повідомлення, вузол лікарні 1 додасть потрібну системну інформацію, перевірить підпис лікаря та сформує повідомлення, яке містить документ, підпис лікаря та системну інформацію. Вузол лікарні 1 підписує дане повідомлення та відправляє його вузлам інших лікарень.

5. Інші вузли, отримавши це повідомлення, перевіряють підпис відправника та додають його до "списку транзакцій, які очікують на відправку".

6. Вузол, який є поточним лідером і відповідає за створення нового блоку, додає усі невідправлені транзакції (наявні в його списку) до нового блоку, підписує цей блок та відправляє його усім іншим вузлам, після чого додає блок до своєї бази даних (блокчейн-реєстру).

7. Отримавши новий блок, вузли інших лікарень перевіряють, що він дійсно створений поточним лідером, перевіряють щоб усі (або більшість) невідправлених транзакцій були присутні в ньому, перевіряють підпис вузла-лідера і, якщо перевірки успішні, додають цей блок до своїх локальних блокчейн-реєстрів. Таким чином документ пацієнта потрапляє у спільну базу даних (глобальний блокчейн-реєстр).

Подальші документи (наприклад, звіт про аналізи пацієнта буде проходити таку ж саму процедуру, починаючи з пункту 3 описаного вище алгоритму). Дані документи не матимуть підпису пацієнта, але після ознайомлення він зможе підписати їх, відправити до вузла лікарні та, за потреби, новий документ вже з підписом “ознайомлення” пацієнта буде також додано до блокчейну. Дана процедура не обов’язкова, але може бути додана до системи для випадків, де потрібна інформована згода пацієнта.

Щоб отримати документи, додаток пацієнта надсилає запит на “оновлення стану” і отримує нові дані, які є у глобальному реєстрі, але відсутні у локальному реєстрі пацієнта. В такому випадку відправляється запит до вузла лікарні, яка знаходить у своїй базі даних та повертає усі документи, які стосуються даного пацієнта. Додаток, маючи ключ, може розшифрувати ці дані та зберегти їх на пристрої (локально дані зберігаються у зашифрованому паролем користувача вигляді).

Уявімо ситуацію, коли пацієнт втратив свідомість, і не має доступу до додатку. Для надання невідкладної допомоги лікарям потрібно буде дізнатись про його стан здоров’я (історію хвороб, аналізів тощо). В такому випадку, лікар може надіслати запит до вузла лікарні, який в свою чергу надішле запит до міністерства, щоб отримати ключ розшифрування для цього пацієнта.

Як було зазначено вище, повідомлення між лікарем та вузлом лікарні містить хеш-значення документу. Розглянемо більш детально, як воно обчислюється, адже це дуже важливий аспект у організації рівнів доступу до даних:

1. Документ – це поля у певному форматі (наприклад, JSON), які містять ключ та значення (наприклад, Діабет - 2, що означає діабет другого типу).

2. Кожне значення з цих полів хешується, після чого отримані значення конкатенуються (з'єднуються в одне) та хешуються знову. Описані дії повторюються, поки не буде отримане єдине значення, яке і буде хеш-значенням документу (рисунок 3.6)

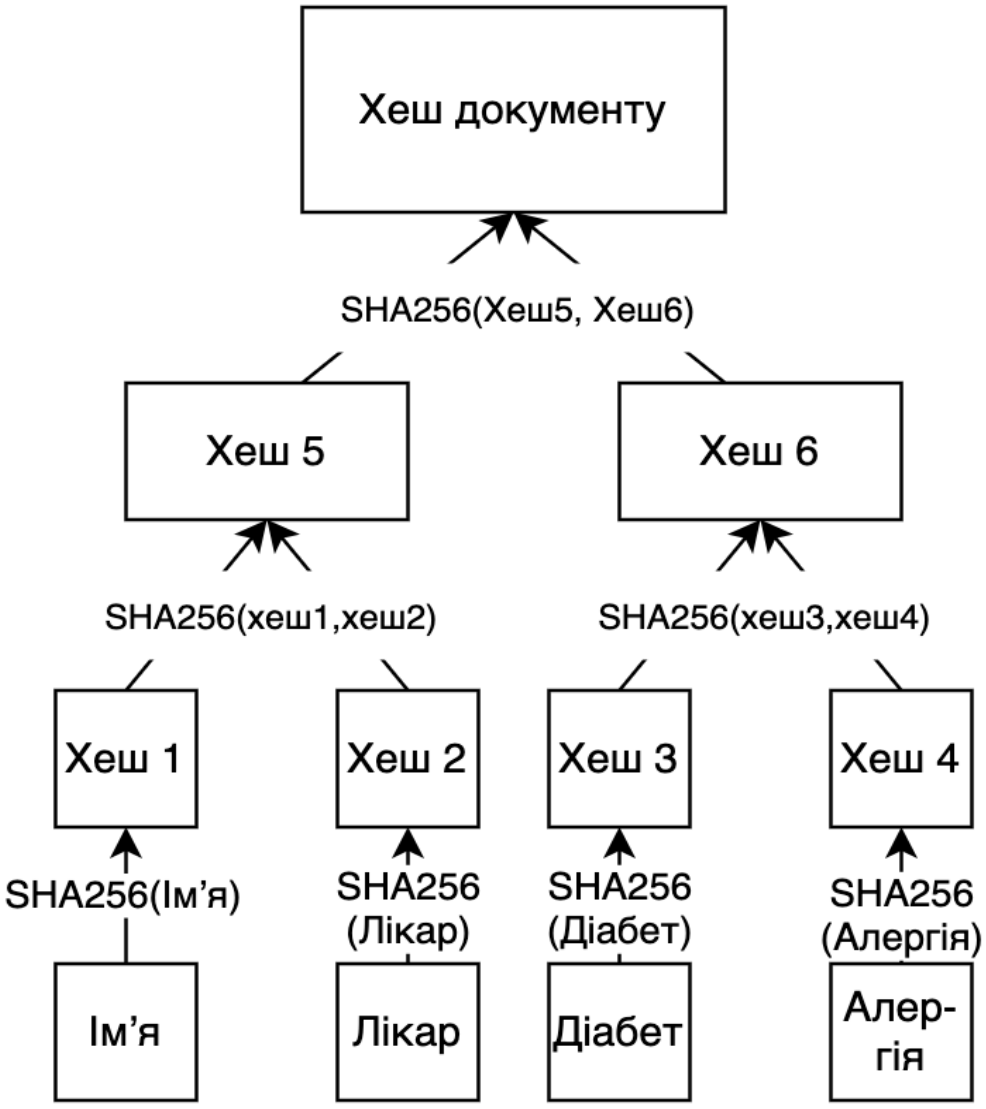

Рисунок 3.6 – Обчислення хеш-значення документів

Такий підхід дозволяє зручно організувати доступ до даних пацієнтів відповідно до ролі співробітника:

1. В базі даних лікарні (та міністерства) міститься інформація про публічний ключ користувача та роль, яка відповідає цьому публічному ключу. Наприклад, <Публічний_ключ_лікаря, Роль_Лікар, лікарня_k>, <Публічний_ключ_санітара, Роль_Санітар, лікарня_k>, <Публічний_ключ_пацієнта, Роль_Пацієнт, лікарня_k>.

2. Відповідно до ролі, вузол лікарні може повертати не весь документ, а лише його частину та доказ того, що “недоступні” частини разом з отриманою утворюють хеш потрібного документу.

Наприклад, санітару потрібно знати лише про наявністість у пацієнта алергії. Щоб дізнатись цю інформацію, він може звернутись (використовуючи додаток) до вузла лікарні та запросити потрібну інформацію. У відповідь вузол надішле ім’я пацієнта та дані про наявність алергії (відмічено зеленим на рисунку 3.7), разом з хеш-значеннями “недоступних” даних (відмічено помаранчевим на рисунок 3.7), а саме – лікаря, з яким укладено декларацію та дані про наявність діабету.

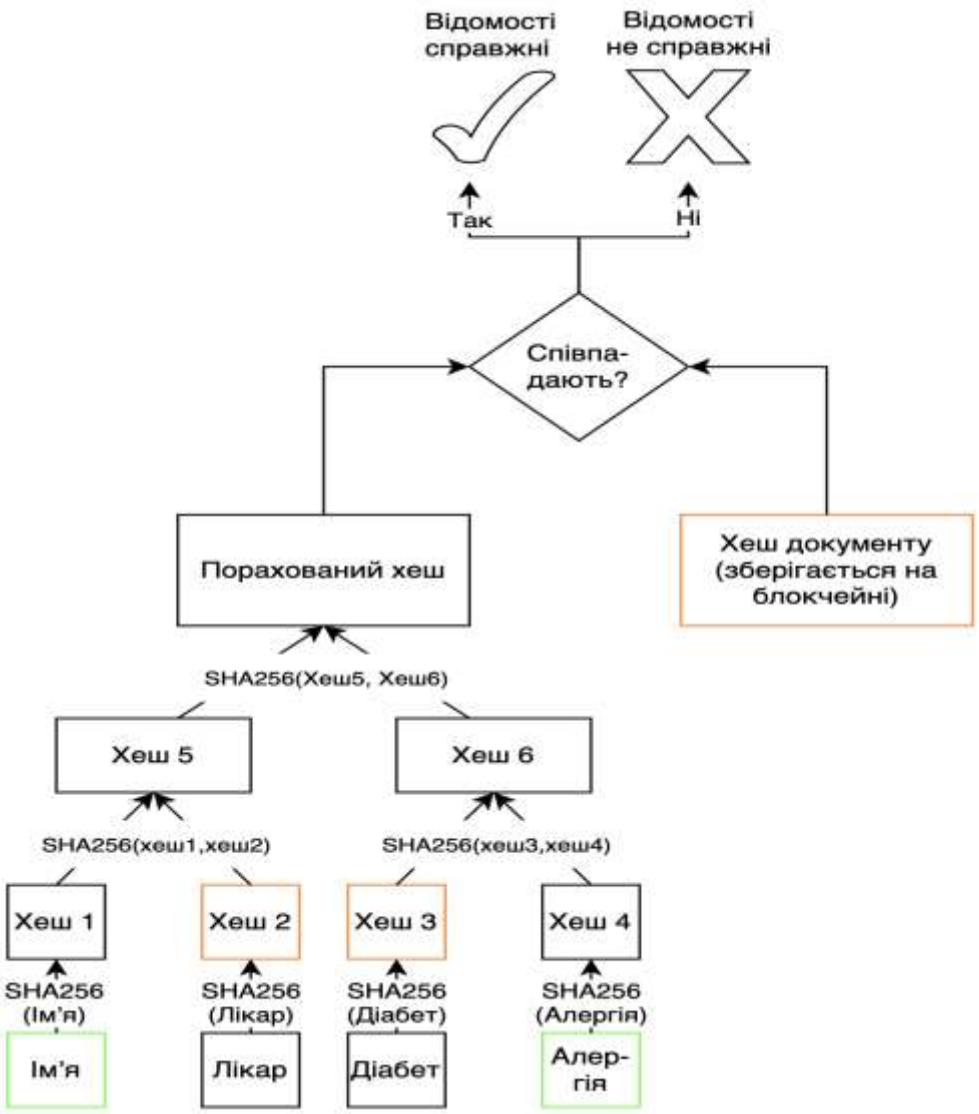

Рисунок 3.7 – Перевірка валідності отриманих даних від вузла

Додаток обчислює проміжні хеш значення та рахує кінцевий хеш документу. Якщо отримане хеш-значення співпадає з наявним у блокчейні – санітар може бути впевнений, що відомості про алергію валідні.

Таким чином, маємо запропоновану описову модель системи для зберігання медичних записів, реалізовану за допомогою технології блокчейн. Дана система стійка до відмов, адже процес зберігання даних розподілений між вузлами лікарень та глобальний стан зберігається кожним учасником у блокчейні. Система задовольняє актуальним вимогам до зберігання медичних записів і стійка до більшості атак на традиційні централізовані системи.

Найважливішим недоліком системи гіпотетично можна вважати наявність центру зберігання та розподілення ключів – міністерства, але наша модель базується на припущенні, що воно має найвищий рівень інформаційного захисту, який гарантується на державному рівні.

Перед практичною реалізацією модель потребує детальної уваги до організації процесів генерації, передачі, обробки та зберігання ключів. Усі користувачі системи мають бути обізнаними у вищезгаданих аспектах управління ключами і питаннях інформаційної гігієни.

ВИСНОВОК

В кваліфікаційній роботі розв’язано актуальну задачу з розробки алгоритму зберігання медичних записів за допомогою технології блокчейн. При цьому отримано наступні результати:

1. Проведено аналіз принципів роботи технології блокчейн.
2. Розкрито можливості та переваги технології блокчейн, зокрема такі, як безпека, цілісність, доступність, імутабельність даних, автентифікація пацієнтів, часова мітка (timestamp), синхронізація даних.
3. Проведений аналіз вимог до зберігання медичних записів, а саме вимог до конфіденційності, цілісності та доступності таких даних.
4. Досліджено ландшафт загроз для систем зберігання медичних даних, який базується на описі принципів актуальних атак та вразливостей як традиційних систем, так і систем, реалізованих за допомогою блокчейн технології.
5. Оглянуто існуючі рішення та принципи їх роботи, обмеження та недоліки, стосовно останніх, це слабка інтероперабельність, брак стандартизації, проблеми з приватністю та безпекою, високі витрати на впровадження та підтримку.
6. Розроблено алгоритм для системи, яка реалізує зберігання та обробку медичних записів. Алгоритм реалізує високі вимоги до конфіденційності, цілісності та доступності записів, безпечну взаємодію між закладами охорони здоров’я та пацієнтами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf
2. Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.
3. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.
4. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.
5. Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media, Inc.
6. Roman-Belmonte, J. M., De-La-Hoz-Franco, E., & Rodríguez-Hernández, M. Á. (2019). A systematic literature review of blockchain in healthcare: Framework, challenges, solutions and future research directions. Computers in Biology and Medicine, 108, 354-366.
7. Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: “MedRec” prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference (Vol. 3).
8. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 218.
9. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.
10. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

11. Zheng, X., Mukkamala, R. R., Vatrapu, R., Ordieres-Meré, J., & Veijalainen, J. (2017). Research perspectives on the role of blockchain in the Internet of Things. Journal of Information Security and Applications, 36, 1-10.

12. Krawiec, R. J., & Barr, D. J. (2019). Understanding Blockchain Technology and Its Potential in Health Care. The Ochsner Journal, 19(1), 28-32.

13. Li, X., Ma, Z., Zhang, S., & Xu, X. (2017). A survey of big data architectures and machine learning algorithms in healthcare. Journal of King Saud University-Computer and Information Sciences.

14. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society, 39, 283-297.

15. Mera, M. A., & Trujillo, S. (2018). Blockchain for Decentralized Multi-source Electronic Health Record Management. IEEE Access, 6, 21118-21128.

16. Swan, M. (2015). Blockchain Thinking: The Brain as a Decentralized Autonomous Corporation. In Blockchain: Blueprint for a New Economy (pp. 179-192). O'Reilly Media, Inc.

17. Nguyen, D., Pathirana, P. N., Ding, M., & Seneviratne, A. (2018). Blockchain for secure EHRs sharing of mobile cloud based E-health systems. IEEE Access, 6, 11665-11672.

18. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., Faxvaag, A., & Kostov, B. (2018). Security analysis of the Fast Healthcare Interoperability Resources (FHIR) standard. Journal of medical Internet research, 20(6), e10129.

19. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2016). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

20. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.

21. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

22. Roehrs, A., da Costa, C. A., da Rosa Righi, R., & Omni, D. (2017). SimplyVitalHealth. Proc. 19th Int. Symp. Comput. In Health Care.

23. Tseng, J. H., Liao, Y. C., Chong, B., & Liao, S. W. (2019). A secure EHR system based on decentralized blockchain. Journal of medical systems, 43(3), 55.

24. Sun, Y., Song, Y., Jara, A. J., & Bie, R. (2016). Internet of things and big data analytics for smart and connected communities. IEEE Access, 4, 766-773.

25. Al Omar, A., Bhuiyan, M. Z. A., & Basu, A. (2018). A taxonomy of cyber-attacks on the internet of things (IoT). arXiv preprint arXiv:1801.07612.

26. Diffie, W., and Hellman, M. "New Directions in Cryptography." IEEE Transactions on Information Theory, vol. 22, no. 6, 1976, pp. 644-654.

27. National Institute of Standards and Technology (NIST). "Secure Hash Standard (SHS)." FIPS PUB 180-4, March 2012, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

28. Daemen, J., and Rijmen, V. "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer, 2002. ISBN 978-3-540-42580-9.

29. Johnson, D., Menezes, A., and Vanstone, S. "The Elliptic Curve Digital Signature Algorithm (ECDSA)." International Journal of Information Security, vol. 1, no. 1, 2001, pp. 36-63.

30. Adibuzzaman, M., DeLaurentis, P., Hill, J., and Benneyworth, B. D., "Big data in digital healthcare: lessons learnt and recommendations for general practice," Heredity, vol. 122, no. 4, pp. 381-390, 2019.

ДОДАТОК А

Копії публікацій

ГРОМАДСЬКЕ ОБЄДНАННЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2023
Тернопіль

ЗМІСТ

низькому рівні заряду, однак повинні передавати дані з мінімальними затримками;

– вразливості пристроїв мають пряму залежність рівню їх інтелектуальності, тобто чим розумнішим і складнішим є пристрій, тим більше потенційних вразливостей в ньому, які іноді важко виявити дослідникам та тестувальникам.

Висновки.

Зазвичай атаки на пристрої IoT можуть бути різноманітні, тому для їх захисту необхідно використовувати комплексний підхід, включаючи як цифрові так і фізичні заходи захисту, що разом допомагають убезпечити пристрої та мережу IoT від можливих загроз.

Перелік використаних джерел.

1. Bagirov A.M., Gaudioso M., Karmitsa N., Makela M.M., Taheri S.(eds.) Numerical Nonsmooth Optimization: State of the Art Algorithms.- New York: Springer, 2020. — 700 p.

2. Klemm M., Cownie J. High Performance Parallel Runtimes: Design and Implementation.-De Gruyter Oldenbourg, 2021. - 356 p.

УДК 004.056.5

ДІЛАЙ С.Я., КОНДРАТЮК В.М., ПОМОГАЄВ С.О.

Західноукраїнський національний університет

ВИКОРИСТАННЯ ДОКАЗІВ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ

Вступ. У епоху, коли інформація вільно поширюється в Інтернеті, і особисті дані потенційно можуть бути зламані, необхідною є система, яка надає якомога менше даних. Це можливо з використанням методу доказу з нульовим розголошенням (ZKP).

Доказ з нульовим розголошенням (zero-knowledge proofs, ZKP), також відомий як протоколом з нульовим розголошенням – це математичний метод перевірки правдивості інформації без розкриття самої інформації.

Метод вперше був представлений дослідниками з MIT у статті 1985 р. [1].

Мета рорботи: дослідження можливостей використання доказів з нульовим розголошенням.

1. Доказ з нульовим розголошенням

Доказ з нульовим розголошенням дозволяє комусь довести право власності або достовірність частини інформації, не розкриваючи саму інформацію. Протоколи з нульовим розголошенням можуть спростити конфіденційність і створити довіру в системах, де дві сторони не хочуть ділитися особистою інформацією.

Докази з нульовим розголошенням поділяються на дві категорії:

- інтерактивні
- неінтерактивні.

Інтерактивні ZKP вимагають відповіді на низку запитань та/або виконання набору дій, перш ніж знання можна буде вважати «надійними». Однак це створює проблему – і перевіряючий, і верифікаційний повинні бути онлайн одночасно для завершення перевірки, що не практично для реальних програм.

Неінтерактивні ZKP вирішують цю проблему, усуваючи потребу у взаємодії, покладаючись замість цього на використання хеш-функції для вибору випадкового виклику для перевірки.

Щоб доказ нульового розголошенням вважався легітимним, він має відповідати трьом основним умовам [2]:

- Повнота: якщо твердження є істинним, перевіряючий повинен бути в змозі переконати верифікатор, що твердження правдиве.
- Обгрунтованість: якщо твердження є хибним, перевіряючий не повинен бути в змозі переконати перевіряючого, що воно правдиве.
- Нульове розголошення (знання): якщо твердження правдиве, то верифікатор не повинен дізнатися жодної інформації, окрім факту, що твердження правдиве.

Вже розроблено багато варіантів доказів з нульовим розголошенням, зокрема zk-SNARKS, zk-STARKS, zk-SNARGS, Bulletproofs і zk Rollups [2].

2. Використання доказів із нульовим розголошенням

Підтвердження особи. Proof of Identity використовує підтвердження з нульовим розголошенням у процесі автентифікації, під час якого одна сторона доводить іншій, що вона має певну інформацію, яка встановлює особу особи, що перевіряє. Пристрій перевірки перевіряє необхідні дані, не надаючи більше конфіденційних чи особистих даних у зворотному зв'язку між пристроєм перевірки та верифікатором.

Підтверджувач передає свою інформацію комп'ютерному алгоритму, який перевіряє інформацію, і якщо перевіряльник надає достатні докази, верифікатор отримує повідомлення про те, що перевіряльник має необхідну інформацію для підтвердження своєї особи.

Таким чином верифікатор не знає жодної інформації, але верифікатор успішно підтвердив, що перевіряльник насправді володіє необхідною ідентифікацією для продовження певного процесу. Це гарантує, що перевіряльник має контроль над своєю особистою інформацією та не повинен відмовлятися від неї.

Підтвердження паролів. Підтвердження пароля з нульовим розголошенням (ZKPP) – це підтвердження, яке дозволяє перевіряючому довести іншій стороні (верифікатору), що він знає значення пароля, не розкриваючи нічого, крім факту, що він знає пароль для верифікатор. Підтвердження пароля з нульовим розголошенням зазвичай використовують у системах автентифікації, де одна сторона хоче підтвердити свою особу іншій стороні за допомогою пароля,

але не хоче, щоб друга сторона чи будь-хто інший дізнався будь-яку інформацію про пароль. Наприклад, програми можуть підтверджувати пароль, не обробляючи його, а платіжна програма може перевіряти баланс рахунку, не торкаючись суми та не дізнаючись нічого про неї.

Підтвердження членства. Голландський банк ING вже інтегрував підтвердження членства в наборі з нульовими розголошеннями. Приналежність до набору з нульовим розголошенням (ZKSM) дозволяє користувачам доводити, що вони включені до частини великого загальнодоступного набору, не розкриваючи, до якої частини великого загальнодоступного набору вони включені. У випадку ING рішення ZKSM дозволяє банку підтвердити, що клієнт проживає в країні, яка належить до Європейського Союзу, не розкриваючи точну країну, в якій проживає

Докази з нульовим розголошенням у Blockchain. Докази з нульовим розголошенням в основному використовуються в криптографії та технології блокчейн. Докази з нульовим розголошенням привертають увагу інституцій і були прийняті багатьма установами, включаючи банки.

Висновки.

Отже, підтвердження з нульовим розголошенням – це метод криптографії, в якому одна сторона повідомляє іншій, що вона знає певну інформацію, ніколи не розкриваючи цю інформацію, зберігаючи конфіденційність.

Наразі доступно багато різних форм доказів нульового розголошення, усі вони забезпечують підвищену конфіденційність для користувачів.

Перелік використаних джерел.

1. What is a Zero-Knowledge Proof? ZKPs Explained. [Електронний ресурс]. - Режим доступу: https://blog.thirdweb.com/zero-knowledge-proof-zkp/

2. Zero-Knowledge Proofs: Non-Techie's Guide to Online Privacy Tech. [Електронний ресурс]. - Режим доступу: https://www.dock.io/post/zero-knowledge-proofs

УДК 681.32

ДМИТРІВ О., ХОМЯК Р.Д., СЛОБОДЯН В.Р.

Західноукраїнський національний університет

СИСТЕМА КОМП'ЮТЕРНОГО МОДЕЛЮВАННЯ ДЕЦЕНТРАЛІЗОВАНОЇ МЕРЕЖІ

Вступ. Завдання системи моделювання комп'ютерних мереж Під час досліджень з метою перевірки ефективності розроблених алгоритмів шифрування на основі НПСС у децентралізованих комп'ютерних мережах необхідно проводити експерименти із застосуванням комп'ютерного моделювання однорантової мережі.

Моделювання або симуляція системи полягає у використанні моделей -



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

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

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2023
Тернопіль

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

УДК 004.056.5

Басістий В.П., Ділай С.Я., Помогаєв С.О.

Західноукраїнський національний університет

АЛГОРИТМИ ДОКАЗУ З НУЛЬОВИМ ЗНАННЯМ

Вступ. У світі зростаючих цифрових технологій та збільшеної кількості взаємодій в онлайн середовищі, питання приватності та безпеки стає все більш актуальним. Одним із революційних підходів до вирішення цих питань є використання алгоритмів доказу із нульовим розголошенням або zero-knowledge proofs (ZKP). Дані алгоритми забезпечують підтвердження істинності деякої інформації без розголошення самої цієї інформації. ZKP є корисними як для підвищення конфіденційності, оскільки вони зменшують обсяг інформації, що передається між сторонами, так і для масштабованості, оскільки вони дозволяють перевіряти докази швидше, ніж якби потрібно було перевірити весь набір даних.

Мета: дослідження доказів із нульовим знанням як технології збереження конфіденційності та масштабованості.

1. Криптографічний протокол ZK – SNARK

ZK – SNARK (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) – це криптографічний протокол, призначений для створення доказів з нульовим знанням з метою перевірки автентичності інформації без розкриття фактичних даних.

Акронім відображає його основні атрибути, які наведені нижче [1]:

Нульове знання: це означає, що верифікатор не отримує жодних знань про твердження, крім його істинності чи хибності.

Стислий: ZK – докази SNARK достатньо компактні, щоб можна їх швидко перевірити.

Неінтерактивний: на відміну від попередніх систем підтвердження, які вимагали багаторазового обміну повідомленнями між перевірками та верифікаторами, SNARK вимагає лише початкового подання доказу.

Аргумент: SNARK – це «обчислювально обґрунтована» заява, яка відповідає суворим критеріям, тому створювати шахрайські докази надзвичайно складно.

Знання: докази на основі SNARK не можуть бути створені з доступом до базових даних або свідка, що забезпечує конфіденційність конфіденційної інформації.

Протокол ZK – SNARK зазвичай включає двох ключових учасників:

1) доказувач, який є стороною, що подає претензію;

2) верифікатор, який відповідає за перевірку обґрунтованості твердження перевіряючого.

Практичне застосування ZK – SNARK можна побачити у сфері верифікації особи. Наприклад, особа може підтвердити свій статус громадянина певної країни, не розкриваючи особистих даних, таких як номер паспорта.

Переваги ZK-SNARK. До основних переваг використання ZK – SNARK необхідно віднести: високу пропускну здатність, компактні розміри для перевірки

дійсності та підвищена безпека.

ZK-SNARK значно підвищує пропускну здатність за рахунок зменшення обчислювального навантаження на базовому рівні Ethereum.

Невеликі розміри доказів SNARK спрощують їх перевірку на головному ланцюзі. На Ethereum це означає зниження плати за газ для підтвердження транзакцій поза ланцюгом, що в кінцевому підсумку знижує витрати на зведення для кінцевих користувачів.

Докази ZK-SNARK дотримуються обчислювально надійної структури, що робить надзвичайно складним завданням обдурити верифікаторів і брати участь у зловмисних діях. Крім того, неінтерактивність ZK-SNARK гарантує, що докази можуть бути надійно перевірені будь-якою стороною, що ще більше зміцнює їхній профіль безпеки.

Основні недоліки ZK-SNARK: вимога надійної установки, вразливість до атак квантових обчислень і залежність від спеціалізованого обладнання.

Реалізація протоколу ZK-SNARK вимагає створення універсального загального еталонного рядка (CRS), який також називають загальнодоступними параметрами. Ці загальнодоступні параметри сприяють безпечному спілкуванню між перевіряючими та верифікаторами. Однак, якщо зловмисники отримають доступ до загальнодоступних параметрів, вони можуть сфабрикувати фальшиві докази дійсності. Деякі проекти намагаються вирішити цю проблему, використовуючи багатостороннє обчислення (MPC), залучаючи різних осіб до створення загальнодоступних параметрів. Тим не менш, цей підхід вимагає, щоб користувачі довіряли чесності залучених сторін. Це створює проблему, оскільки технологія блокчейн має на меті зменшити залежність від довірених органів.

ZK-SNARK покладається на еліптичну криптографію (ECC) для шифрування інформації, яка використовується для отримання доказів дійсності. Хоча наразі ECC пропонує розумний рівень безпеки, прогрес у квантових обчисленнях створює потенційну загрозу для моделі безпеки.

Генерація підтверджень дійсності за допомогою ZK-SNARK –процес, що потребує інтенсивних обчислень, і вимагає від перевірників інвестувати в спеціалізоване обладнання. Враховуючи обмежену доступність цих машин, виникає занепокоєння щодо централізації процесу перевірки ZK-SNARK, оскільки лише кілька обраних можуть дозволити собі таке обладнання.

2. Криптографічний протокол ZK – STARK

ZK-STARKs – це абревіатура Zero-Knowledge Scalable Transparent Argument of Knowledge, виконує аналогічну задачу з ZK-SNARKs у тому, що він надає засоби перевірки автентичності заяви без розкриття будь-яких деталей про саму заяву.

Докази дійсності на основі STARK створюються з використанням конфіденційної інформації, яка залишається прихованою від верифікатора. Подібним чином STARK можна використовувати для перевірки точності транзакцій, зберігаючи вхідні дані транзакцій нерозкритими.

Основна відмінність, яка відрізняє ZK-STARK, полягає в їх масштабованості та прозорості:

ZK-STARK називається прозорим, тому що він працює без необхідності

довіреного налаштування, що включає загальний еталонний рядок (CRS).

Масштабованість ZK-STARK є особливістю, яка заслуговує на увагу, оскільки складність як доказу, так і перевірки масштабується майже лінійно по відношенню до обчислювальної складності. Навпаки, ZK-SNARK демонструють лінійне масштабування складності підтвердження та перевірки щодо обчислення.

На практиці це означає, що ZK-SNARK вимагають більше часу для генерації та перевірки доказів під час виконання великих обчислювальних завдань. Отже, ZK-STARK краще підходять для програм, що обробляють значні обсяги транзакцій.

Переваги STARKS. До основних переваг ZK – STARK можна віднести: відсутність потреби в довіреній установці, масштабованість, можливість досягнення максимальної пропускної здатності та надійні гарантії безпеки.

ZK-STARK працюють без необхідності довіреної установки, натомість покладаючись на публічну випадковість. Ця менша залежність від припущень про довіру підвищує безпеку протоколів на основі STARK і зменшує потребу користувачів довіряти зовнішнім об'єктам.

STARK демонструють переваги масштабованості порівняно з SNARK. При цьому ZK-STARK дозволяють швидше виконувати обчислення та перевірку, навіть якщо складність базових обчислень зростає експоненціально. Подібно до SNARK, STARK сприяють масштабованості блокчейнів, сприяючи безпечним і перевіреним обчисленням поза мережею.

ZK-STARK використовує стійкі до зіткнень хеші для шифрування, на відміну від схем еліптичної кривої, що використовуються в ZK-SNARK. Цей вибір шифрування вважається стійким проти потенційних квантових обчислювальних атак, підвищуючи безпеку ZK-STARK у порівнянні з еліптичними кривими, які використовуються в SNARK.

До недоліків ZK-STARK можна віднести: більші розміри перевірки та нижче впровадження.

Незважаючи на їхню перевагу у швидшому забезпеченні доказів, STARK мають недолік, пов'язаний із створенням більших розмірів доказів порівняно з доказами на основі SNARK. Цей збільшений розмір призводить до збільшення плати за газ для перевірки доказів STARK на Ethereum, що робить їх дорожчим у використанні.

Висновок. Еволюція доказів із нульовим знанням, зокрема ZK-SNARK і ZK-STARK, стала важливою віхою в технологіях збереження конфіденційності та масштабованості. Як демонструє зростаюче впровадження пакетів ZK, очевидно, що ці криптографічні методи будуть відігравати ключову роль у просуванні масштабованості блокчейн-платформ, таких як Ethereum.

Перелік використаних джерел.

1. Understanding the Difference Between zk-SNARKs and zk-STARKS. Електронний ресурс]. - Режим доступу: https://chain.link/education-hub/zk-snarks-vs-zk-starks

2. Chen, T., Lu, H., Kunpittaya, T., & Luo, A. (2022). A review of zk-snarks. arXiv preprint arXiv:2202.06877