Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження, проєктування та розробка програмних компонентів для системи зберігання та передачі конфіденційної інформації
(тема)

Виконав:
здобувач 2 року навчання,
групи СПм-23-3
Олександр РАГУЛІН
(власне ім'я, прізвище)

Спеціальність
123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: Доцент Олександр ШМАТКО
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Рагуліну Олександру Євгеновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження, проєктування та розробка програмних компонентів для системи зберігання та передачи конфіденційної інформації
затверджена наказом по університету від "21" квітня 2025 р. № 296 Ст
2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.
3. Вхідні дані до роботи
1)Нормативні документи щодо зберігання та обробки конфіденційних даних;
2) Літературні джерела за темою дослідження;

4. Перелік питань, що потрібно опрацювати у роботі
1) аналіз проблеми та огляд існуючих рішень;
2) огляд методів та підходів до розробки систем зберігання та обміну інформацією
3) розробка опису програмних компонентів;
4) розробка програмних модулів;
5) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій Слайд-презентація – 20 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	22.04.25-29.04.25	
2	Дослідження технології блокчейн	30.04.25-05.05.25	
3	Вибір технологій та інструментів для розробки	06.05.25-09.05.25	
4	Розробка програмних модулів	10.05.25-21.05.25	
5	Запуск та тестування програмних модулів	22.05.25-02.06.25	
6	Оформлення матеріалів кваліфікаційної роботи	3.06.25-05.06.25	
7	Подання кваліфікаційної роботи керівникові	06.06.25-09.06.25	
	та її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	10.06.25-12.06.25	
	вання		

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ Доц. Олександр ШМАТКО

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 82 с., 15 рис., 12 табл., 1 дод., 40 джерел.

МЕДИЧНІ ІНФОРМАЦІЙНІ СИСТЕМИ, БЛОКЧЕЙН, ETHEREUM, SMART-CONTRACT.

Об'єктом дослідження є системи передачі медичної інформації, які забезпечують ефективний обмін даними між медичними закладами, фахівцями та пацієнтами з урахуванням необхідності гарантування конфіденційності, цілісності та доступності цих даних.

Предметом дослідження є методи та інструментальні засоби проєктування та розробки програмних компонентів, необхідних для побудови захищених систем обміну медичною інформацією.

Метою роботи є підвищення рівня конфіденційності, цілісності та доступності медичної інформації шляхом проєктування та реалізації програмних компонентів, які забезпечують надійний і безпечний обмін цією інформацією між усіма учасниками медичного процесу.

Результати роботи свідчать про значний потенціал застосування децентралізованих технологій для вирішення актуальних проблем в галузі охорони здоров’я. Розроблена система дозволяє підвищити ефективність медичного обслуговування, покращити координацію лікування пацієнтів, забезпечити точність діагностичних даних та прискорити доступ до важливої медичної інформації. Впровадження таких рішень може суттєво змінити підходи до зберігання та обміну медичними даними, сприяючи формуванню безпечного цифрового середовища в сфері охорони здоров’я.

ABSTRACT

Master’s thesis: 82 pages, 15 figures, 12 tables, 1 appendices, 40 sources.

MEDICAL INFORMATION SYSTEMS, BLOCKCHAIN, ETHEREUM, SMART CONTRACTS

The object of this research encompasses systems for the transmission of medical information, which enable data exchange among healthcare institutions, specialists, and patients, while ensuring the confidentiality, integrity, and availability of this data.

The subject of the study focuses on the software components necessary for the development and maintenance of secure medical information transmission systems. These components include software for encryption, authentication, authorization, as well as mechanisms to ensure fault tolerance and data recovery.

The goal of this research is to enhance the confidentiality, integrity, and availability of medical data and to ensure reliable data exchange between medical institutions and other stakeholders by designing and developing software components for secure medical information transmission systems.

The development of such systems can significantly impact the efficiency of healthcare services, particularly in terms of faster access to medical information, accuracy of diagnostic data, and overall coordination of patient treatment.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

API – інтерфейс прикладного програмування (англ., Application Programming Interface)

AES – стандарт симетричного шифрування даних (англ., Advanced Encryption Standard)

BaaS – блокчейн як послуга (англ., Blockchain as a Service)

CID – ідентифікатор вмісту в IPFS (англ., Content Identifier)

dApp – децентралізований застосунок (англ., Decentralized Application)

EHR – електронна медична картка пацієнта (англ., Electronic Health Record)

ETH – платформа блокчейн Ethereum (англ., Ethereum)

GAN – генеративна змагальна мережа (англ., Generative Adversarial Network)

HIPAA – закон США щодо конфіденційності медичних даних (англ., Health Insurance Portability and Accountability Act)

IoMT – інтернет медичних речей (англ., Internet of Medical Things)

IPFS – міжпланетна файлова система (англ., InterPlanetary File System)

JSON – формат обміну даними (англ., JavaScript Object Notation)

KYC – процедура ідентифікації користувачів (англ., Know Your Customer)

NFT – невзаємозамінний токен (англ., Non-Fungible Token)

PBFT – протокол консенсусу, стійкий до візантійських збоїв (англ., Practical Byzantine Fault Tolerance)

PoW – доказ виконаної роботи (англ., Proof of Work)

PoS – доказ частки володіння (англ., Proof of Stake)

SDK – набір інструментів для розробника (англ., Software Development Kit)

SHA – криптографічна хеш-функція (англ., Secure Hash Algorithm)

ВСТУП

У сучасних умовах цифровізації охорони здоров’я питання безпечного зберігання, обміну та обробки конфіденційної медичної інформації набуває особливої актуальності. Зростаюча кількість кіберзагроз, недостатня захищеність централізованих інформаційних систем та складність дотримання нормативних вимог щодо конфіденційності персональних даних вимагають впровадження новітніх технологічних рішень. Одним із перспективних підходів до вирішення зазначених проблем є використання технології блокчейн у поєднанні зі смарт-контрактами.

Блокчейн як розподілений реєстр забезпечує незмінність записів, прозорість дій користувачів та високу надійність зберігання інформації. Смарт-контракти дозволяють автоматизувати контроль доступу до медичних даних та підвищити ефективність міжвідомчої взаємодії. Таким чином, розробка інноваційного програмного забезпечення, що інтегрує ці технології у сфері медичних інформаційних систем, є своєчасним і необхідним напрямом науково-прикладних досліджень.

Об'єкт дослідження включає в себе системи передачі медичної інформації, які забезпечують обмін даними між медичними закладами, спеціалістами та пацієнтами, забезпечуючи конфіденційність, цілісність та доступність цих даних.

Предметом дослідження є програмні компоненти, необхідні для створення і підтримки захищених систем передачі медичної інформації. Ці компоненти включають в себе програмне забезпечення для шифрування, аутентифікації, авторизації, а також механізми для забезпечення відмовостійкості та відновлення даних.

Метою даного дослідження є підвищення конфіденційності медичних даних, їх цілісності та доступності, а також забезпечення надійного обміну цими даними між медичними закладами та іншими учасниками за рахунок

проєктування та розробки програмних компонентів для створення захищених систем передачі медичної інформації.

Для досягнення поставленої мети необхідно виконати такі основні завдання:

- проаналізувати існуючі архітектури систем електронної охорони здоров’я, що використовують блокчейн-технології;
- визначити функціональні та нефункціональні вимоги до цільової системи;
- розробити архітектуру програмних компонентів, що включає смарт-контракти, механізми авторизації, шифрування, логування та аудиту доступу;
- реалізувати прототип системи та забезпечити взаємодію між її компонентами;
- провести тестування з точки зору безпеки, продуктивності та відповідності функціональним вимогам.

У процесі виконання дослідження було застосовано комплекс наукових методів, зокрема:

- аналіз і синтез – для вивчення літературних джерел та формування вимог до системи;
- моделювання – для побудови архітектури програмних компонентів;
- методи криптографічного захисту даних – для забезпечення конфіденційності та цілісності інформації;
- експериментальне тестування – для перевірки працездатності та надійності реалізованого рішення;
- порівняльний аналіз – для зіставлення функціональних характеристик із наявними аналогами.

Наукова новизна полягає в розробці та обґрунтуванні підходу до проєктування безпечної системи зберігання та передачі конфіденційної медичної інформації з використанням децентралізованих технологій блокчейн та смарт-контрактів. Запропонована модель дозволяє досягти високого рівня захисту даних без залучення централізованих серверів, що

мінімізує ризики несанкціонованого доступу та модифікації даних.

Практична значущість дослідження полягає в можливості впровадження розробленої системи у медичних установах з метою підвищення рівня безпеки обігу медичних даних, забезпечення прозорості процесів доступу до них та автоматизації перевірки прав доступу. Запропоноване рішення може стати основою для подальшого розвитку цифрової інфраструктури охорони здоров’я на принципах безпеки, децентралізації та довіри.

1 ОГЛЯД ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН В СФЕРІ ОБМІНУ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

1.1 Загальні відомості

Останніми роками постійне зростання рівня економіки та якості життя спричинило суттєве зростання суспільного попиту на доступну та якісну медичну допомогу. Медична галузь перетворилася на одну з найбільших і найдинамічніших у світі, особливо після спалаху пандемії COVID-19, яка серйозно загрожувала здоров'ю населення, порушила функціонування глобальної економіки та призвела до суттєвого збільшення національних інвестицій у сферу охорони здоров'я [1]. Паралельно з цим, розвиток і впровадження сучасних технологій – зокрема штучного інтелекту, інтелектуальних діагностичних засобів і медичних інформаційних систем – сприяє трансформації охорони здоров'я у напрямі підвищення інтелектуальності, точності та цифровізації [2, 3].

У центрі цієї цифрової трансформації знаходяться медичні дані, які є основою для розбудови системи «розумної» та персоналізованої медицини. Вони відіграють ключову роль у біомедичних дослідженнях, розробці лікарських засобів, клінічних рішеннях і управлінні громадським здоров'ям. Водночас медичні дані мають складну структуру, обумовлену розмаїттям джерел, різноманітністю форматів і відмінностями у стандартах охорони здоров'я між регіонами. Через це вони розпорошені, мають несумісні формати та велику структурну гетерогенність, що ускладнює їх об'єднане управління та ефективне використання [4].

З метою подолання цих викликів було створено низку платформ для обробки медичних даних, які забезпечують стандартизований доступ до медичної інформації для лікарень, науково-дослідних інститутів, фармацевтичних компаній і регуляторних органів [5, 6]. Такі платформи

агрегують дані з багатьох медичних установ, залучають фахівців для їх анотування та обробки за допомогою спеціалізованого програмного забезпечення й алгоритмів. Оброблені таким чином дані використовуються для створення моделей захворювань, які слугують основою для медичних досліджень [7], управління охороною здоров'я [8], державного планування [9] та розробки інноваційних препаратів [10].

Попри свою корисність, ці платформи мають істотні обмеження щодо можливості перевірки достовірності та цілісності медичних даних на всіх етапах – від збору до обробки та надання третім сторонам. Для таких користувачів, як наукові установи, фармацевтичні компанії чи органи державного управління, необхідне впровадження надійних механізмів, що дозволяють верифікувати як початкові дані, так і операції, що виконувалися під час їх обробки, а також кінцеві результати. Відповідно, усі етапи життєвого циклу медичних даних – включно з вхідними, проміжними та кінцевими даними, діями операторів і записами доступу – повинні бути прозорими, верифікованими та такими, що підлягають простежуваності [11].

1.2 Огляд публікацій за темою дослідження

У зв'язку з активною цифровізацією галузі охорони здоров'я проблема безпечного зберігання та обміну медичною інформацією набула особливої актуальності. Зі зростанням обсягів електронних медичних записів (EHR) виникає потреба у забезпеченні конфіденційності, цілісності та контролю доступу до медичних даних. Дослідники акцентують увагу на обмеженій ефективності традиційних централізованих рішень та відзначають потенціал блокчейн-технологій у вирішенні цих викликів [1], [5].

Блокчейн дозволяє створювати децентралізовані й незмінні журнали записів пацієнтів, що робить можливим надійне зберігання даних та забезпечення їх простежуваності [2], [10]. Дослідження підтверджують ефективність permissioned-блокчейнів, зокрема Hyperledger Fabric, у

медичних інформаційних системах завдяки їхній гнучкості та підтримці модульного управління правами доступу [3]. Водночас зберігання великих обсягів даних у блокчейні пов’язане з технічними обмеженнями, тому інтеграція з децентралізованими файловими системами, як-от IPFS, стала популярним напрямом досліджень [17], [26]. Такі гібридні моделі дозволяють зберігати метадані у блокчейні, а великі об’єми — поза мережею, що знижує навантаження на блокчейн-інфраструктуру.

Огляд, проведений Azbeg K. та співавторами, класифікує сучасні підходи до зберігання EHR у блокчейні, зосереджуючись на проблемах сумісності, безпеки та масштабованості [3]. Zhang Y. у своєму дослідженні аналізує архітектурні особливості зберігання медичних записів із використанням IPFS, звертаючи увагу на питання доступу та конфіденційності [17]. Серед викликів, які залишаються актуальними для галузі, дослідники виділяють обмежену масштабованість платформ при роботі з великими обсягами медичних даних, а також складність забезпечення високої швидкодії у режимі реального часу.

Іншим перспективним напрямом є застосування смарт-контрактів, які дозволяють автоматизувати процеси контролю доступу, управління згодою пацієнтів на обробку персональних даних, а також фінансові розрахунки між учасниками системи [8], [16], [36]. Наприклад, у роботі [33] запропоновано архітектуру доступу до медичних даних на основі смарт-контрактів, що динамічно враховує зміни в політиках конфіденційності. У свою чергу, [34] описує модель обміну медичними записами між закладами охорони здоров’я із залученням смарт-контрактів для верифікації транзакцій.

Практичні реалізації демонструють реальний потенціал цієї технології. Зокрема, дослідження Omar I.A. описує впровадження довірених смарт-контрактів для безпечного обміну EHR через IPFS, підкреслюючи їхню ефективність у захисті персональних даних [16]. Lin Y. пропонує використання смарт-контрактів для забезпечення прозорості та простежуваності в рамках клінічних досліджень, акцентуючи на юридичних

аспектах автоматизації контролю [36]. Незважаючи на прогрес, залишається відкритим питання юридичної легітимності таких рішень, зокрема, щодо автоматизованого правового захисту персональних даних, а також верифікації логіки смарт-контрактів при їх оновленні чи модифікації.

Ще одним важливим аспектом досліджень є архітектурні рішення програмних платформ. Сучасні блокчейн-системи для медицини переважно будуються на мікросервісній архітектурі, що забезпечує гнучкість, масштабованість і можливість незалежного оновлення окремих компонентів [4], [26]. У роботі [26] детально проаналізовано поєднання Ethereum і IPFS для створення надійного програмного комплексу, а також підкреслено важливість використання моделей управління доступом, зокрема на основі ролей. Rajput A.R. у своїй роботі пропонує систему EACMS, яка реалізує контроль доступу до електронних записів за допомогою смарт-контрактів на базі Ethereum [35].

Інтеграція блокчейн-систем з традиційними електронними медичними записами (EHR) також є предметом численних досліджень. Роботи [6], [18], [22] аналізують шляхи інтеграції, при цьому акцент робиться на створенні шлюзів для взаємодії з існуючими базами даних [19], а також на забезпеченні сумісності з міжнародними стандартами обміну медичними даними, такими як HL7 та FHIR. У пілотному проєкті Dubovitskaya A. було продемонстровано ефективну реалізацію обміну EHR між лікарнями за допомогою блокчейн, що дозволило забезпечити високий рівень безпеки та контролю [6].

У контексті безпеки, приватності та регуляторного забезпечення сучасні дослідження зосереджуються на впровадженні гомоморфного шифрування, доказів з нульовим розголошенням знань (ZKP) і федеративного навчання [5], [27], [31], [39]. Особливу увагу приділено безпечній обробці медичних даних у середовищах штучного інтелекту, що використовується, наприклад, для діагностики на основі зображень [24], [32]. У роботі Cao Y. узагальнено методи захисту конфіденційності, сумісні з

блокчейн-архітектурами, зокрема у контексті обробки даних пацієнтів [5]. Dwivedi A.D. запропонував децентралізовану платформу для IoT-медичних пристроїв, яка забезпечує високий рівень анонімності [31]. Водночас залишається відкритим питання правового регулювання, зокрема щодо впровадження вимог GDPR та HIPAA в блокчейн-архітектури.

Практичні кейси демонструють реальні застосування блокчейну в охороні здоров'я — від реєстрації вакцинацій [9] до телемедицини [25], обміну медичними зображеннями [32] та підтримки клінічних досліджень [36]. Kumar N.M. надає огляд рішень, що застосовувалися під час пандемії COVID-19 для обліку вакцинацій та моніторингу пацієнтів [9]. Alam T. пропонує фреймворк на основі IPFS для безпечного обміну медичними зображеннями, що дозволяє ефективно передавати великі файли між закладами [32].

Попри різноманіття запропонованих рішень, дослідники наголошують на потребі подальшого вдосконалення таких аспектів, як продуктивність систем при високому навантаженні, вартість розгортання у закладах охорони здоров'я та забезпечення сумісності з інфраструктурою національних медичних систем. Особливу увагу приділяють також довготривалому зберіганню медичних зображень та відео, захищеному оновленню смарт-контрактів і створенню механізмів репутації для вузлів мережі [28].

1.3 Постановка задачі досліджень

У сучасних медичних інформаційних системах зберігаються великі обсяги персоналізованої інформації про стан здоров'я пацієнтів, історії хвороб, результати діагностики, призначення лікарів тощо. Забезпечення конфіденційності, цілісності та доступності таких даних є критично важливим для ефективного функціонування системи охорони здоров'я. Традиційні централізовані рішення, що застосовуються для зберігання та обміну медичними даними, мають обмеження у сфері захисту інформації,

зокрема вразливість до зовнішніх атак, технічних збоїв та несанкціонованого доступу.

Використання блокчейн-технологій разом зі смарт-контрактами відкриває нові можливості для створення децентралізованих, стійких до фальсифікації систем управління медичними даними. Завдяки незмінності записів, прозорості транзакцій та автоматизації правил доступу, такі системи можуть забезпечити високий рівень інформаційної безпеки та довіри між учасниками процесу.

Таким чином, перед дослідженням постає необхідність вирішення наступної науково-прикладної задачі:

Розробка програмних компонентів, які забезпечують захищену передачу та зберігання конфіденційної медичної інформації на основі технологій блокчейн і смарт-контрактів, з урахуванням вимог до захисту персональних даних, надійності доступу та функціональної масштабованості.

Для реалізації поставленої задачі необхідно:

- проаналізувати існуючі архітектури систем електронної охорони здоров’я, що використовують блокчейн-технології;
- визначити функціональні та нефункціональні вимоги до цільової системи;
- розробити архітектуру програмних компонентів, що включає смарт-контракти, механізми авторизації, шифрування, логування та аудиту доступу;
- реалізувати прототип системи та забезпечити взаємодію між її компонентами;
- провести тестування з точки зору безпеки, продуктивності та відповідності функціональним вимогам.

Постановка цієї задачі формує основу дослідження, що спрямоване на створення безпечної, прозорої та ефективної програмної інфраструктури для зберігання та обміну чутливою медичною інформацією.

2 ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН В СИСТЕМАХ ЗБЕРІГАННЯ ТА ОБМІНУ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

2.1 Основи блокчейн-технологій

Блокчейн-технологія є децентралізованою мережею вузлів, яка використовується для зберігання, обміну та захисту даних у розподіленому середовищі. Вона виступає як ефективний інструмент для забезпечення конфіденційності, цілісності та доступності даних, що особливо актуально у сферах, де обробляється чутлива або критично важлива інформація, зокрема в охороні здоров’я [10], [11]. Блокчейн дає змогу не лише централізовано, але і безпечно зберігати пов’язані документи в одному середовищі, забезпечуючи захист від несанкціонованих змін і доступу [12].

З технічної точки зору, блокчейн — це однорангова (peer-to-peer, P2P) мережа комп’ютерів, які називаються вузлами (nodes). Усі вузли зберігають однакову копію розподіленого реєстру транзакцій і автоматично оновлюють її у разі додавання нового блоку. Такий механізм забезпечує незмінність даних та створює умови для надійної взаємодії між усіма учасниками мережі без посередників. Унікальною особливістю блокчейну є постійне відстеження історичних і поточних транзакцій у мережі, що підвищує прозорість та довіру до системи [10], [11].

Архітектура блокчейну ґрунтується на трьох ключових поняттях: блоках, вузлах і майнерах. На відміну від традиційних централізованих систем, блокчейн не зберігає дані в одному місці — натомість, інформація розподіляється по всій мережі. Кожен комп’ютер-учасник мережі зберігає копію блокчейну, яка оновлюється при кожному додаванні нового блоку, що робить неможливою несанкціоновану зміну або підміну даних без згоди більшості вузлів [11], [12].

Блокчейн функціонує через узгоджений протокол, який дозволяє

обмінюватися цінностями або транзакційними даними між учасниками без потреби в централізованому посереднику. У результаті досягається повна автономність і прозорість взаємодій. Існує кілька типів блокчейн-систем, кожна з яких має свої переваги та обмеження, що впливають на вибір технології для конкретних сценаріїв застосування [11].

Публічний блокчейн є найпершим типом блокчейн-мережі, на основі якого виникли криптовалюти, такі як Bitcoin. Така мережа дозволяє будь-кому приєднатися до неї, зберігаючи високу ступінь децентралізації, прозорості та стійкості до фальсифікацій. У публічних блокчейнах усі дані відкриті, а автентичність транзакцій забезпечується консенсусними алгоритмами, такими як Proof of Work або Proof of Stake [12].

Приватний блокчейн функціонує в закритому середовищі, де доступ до мережі мають лише уповноважені учасники. Така система зазвичай використовується в межах однієї організації або між кількома довіреними суб’єктами, що забезпечує вищу швидкодію, зниження витрат на обчислення та більший контроль над інформацією. Учасники мережі заздалегідь відомі, а транзакції залишаються конфіденційними [11].

Гібридний блокчейн поєднує елементи публічного та приватного блокчейну. Це дозволяє організаціям створити приватну мережу з контрольованим доступом до даних, одночасно забезпечуючи публічний доступ до окремих аспектів або транзакцій. Такий підхід дає змогу встановлювати точні правила щодо того, яка інформація є доступною для загалу, а яка — лише для певних категорій користувачів [11].

У межах медичних інформаційних систем блокчейн-технології використовуються для об’єднання розрізнених баз даних, підвищення рівня довіри між медичними установами та пацієнтами, а також для автоматизації процесів перевірки, зберігання й обміну медичною інформацією. Крім того, блокчейн відкриває нові можливості для персоналізованої медицини, оскільки дозволяє формувати єдину базу даних пацієнтів, що значно пришвидшує пошук відповідних кандидатів для участі в клінічних

дослідженнях і покращує якість лікування [10], [12].

2.2 Використання блокчейн технологій для обміну конфіденційними даними

Початкове застосування блокчейн-технології відбулося у 2008 році з появою криптовалюти Bitcoin. Три ключові характеристики — децентралізація, прозорість та конфіденційність — відрізняють блокчейн від інших технологічних рішень [1]. Саме ці властивості привернули увагу до можливого застосування блокчейну в інших галузях, орієнтованих на дані, зокрема в медицині [3]. Компанія IBM прогнозує значний вплив блокчейн-технологій у трьох основних напрямах охорони здоров'я: децентралізований обмін електронними медичними записами (EHR), адміністрування клінічних досліджень і дотримання нормативних вимог [4], [5] (рисунок 2.1).

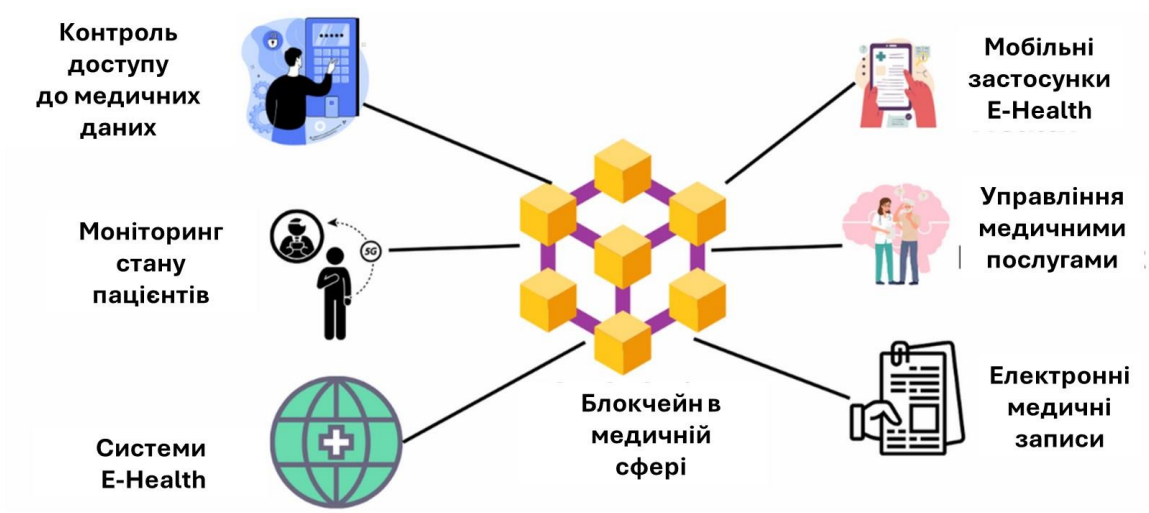

Рисунок 2.1 – Сфери застосування блокчейн технологій [10]

Інтернет речей (IoT), як технологія передачі даних між пристроями через бездротові канали, відіграє важливу роль у трансформації медицини. Зокрема, мережа Інтернету медичних речей (IoMT) зосереджується на наданні допомоги пацієнтам, забезпечуючи збір фізіологічних даних за допомогою медичних сенсорів і пристроїв, що дозволяє лікарям формувати

точні діагнози [26]. Завдяки безпеці даних і простому керуванню пристроями, блокчейн утвердився як надійна децентралізована платформа. Його використання охоплює безпечний доступ, зберігання інформації та підтримку медичних досліджень. Звернення до питань конфіденційності пацієнтів і протоколів обміну даними сприяє точній візуалізації даних, що є особливо важливим у періоди пандемій, як-от під час COVID-19 [33].

Інтеграція блокчейн-технології з пристроями IoMT підвищує рівень конфіденційності пацієнтів і ефективність розподілу даних. Надійність смарт-контрактів запобігає маніпуляції інформацією, а децентралізоване зберігання сприяє прозорості збирання, обміну та збереження медичних даних [10–12]. Блокчейн як розподілений одноранговий реєстр дає змогу забезпечити безпечне, прозоре й незмінне зберігання записів. Завдяки своєму успішному впровадженню у сфері криптовалют, до 2019 року було здійснено понад 400 мільйонів транзакцій у мережі Bitcoin [2], що демонструє широкий потенціал технології.

Одним із прикладів є система HealthChain, яка реалізована на приватному блокчейні з використанням Hyperledger Fabric компанії IBM. Вона забезпечує конфіденційність, масштабованість і безпеку медичних даних [6]. HealthChain також використовує смарт-контракти (chaincode) для контролю авторизацій і прав доступу в межах мережі [7]. Аналогічні рішення реалізовано в Ancile, що базується на платформі Ethereum, де смарт-контракти використовуються для контролю доступу, безпеки, конфіденційності та сумісності даних [8]. Інші приклади впровадження блокчейну в електронні медичні записи включають MedRec, DPS (розробка Li та ін.) [9–11], а також MedBlock [12], BlockHIE [13], FHIRChain [14] і MeDShare [15] (Таблиця 2.1).

Таблиця 2.1 - Порівняння блокчейн-рішень для електронних медичних записів (EHR)

Система / Платформа	Блокчейн-платформа	Основні функції	Особливості реалізації	Джерело
1	2	3	4	5
HealthChain	Hyperledger Fabric (IBM)	Конфіденційність, масштабованість, безпека	Приватна permissioned-мережа; використання смарт-контрактів (chaincode) для контролю доступу	[6], [7]
Ancile	Ethereum	Контроль доступу, безпека, конфіденційність, інтероперабельність	Смарт-контракти керують правами доступу до EHR; публічний блокчейн	[8]
MedRec	Ethereum	Розподілений контроль над доступом до EHR	Орієнтація на інтеграцію з медичними закладами; зберігає метадані, а не самі дані	[9]

Продовження таблиці 2.1

1	2	3	4	5
DPS (Li et al.)	Ethereum	Зберігання та підтвердження цілісності медичних даних	Проста схема збереження та перевірки медичних записів	[10], [11]
MedBlock	Не вказано (ймовірно Ethereum)	Зберігання та обмін медичними записами	Забезпечує зручну взаємодію між пацієнтами та медичними закладами	[12]
BlockHIE	Не вказано	Інтероперабельність між різними EHR-системами	Орієнтація на створення Health Information Exchange (HIE)	[13]
FHIRChain	Ethereum	Відповідність стандартам HL7 FHIR, доступ за допомогою смарт-контрактів	Підтримка сучасних стандартів обміну медичними даними	[14]
MeDShare	Не вказано	Контроль доступу до даних, дотримання політик конфіденційності	Призначена для обміну великими медичними даними між установами	[15]

Очікується, що до 2022 року ринок блокчейн-технологій у сфері охорони здоров’я досягне піку свого розвитку [16]. Це пов’язано з визнанням потенціалу блокчейну для підвищення безпеки даних, оптимізації адміністрування й ефективного обміну EHR, що, в свою чергу, стимулює інновації в медицині [5].

Попри активне впровадження, на сьогоднішній день все ще існує суттєвий розрив між розробкою, тестуванням та масштабним впровадженням блокчейн-рішень у медицині [17]. Водночас, у галузі невідкладної допомоги спостерігається зсув від традиційних моделей лікування до впровадження цифрових технологій, таких як штучний інтелект (AI), машинне навчання (ML) та аналіз великих даних [18]. Ці технології значно збільшують обсяги, швидкість і різноманітність персональних медичних даних, що, у свою чергу, породжує необхідність в ефективному обміні даними між усіма учасниками медичної екосистеми [19].

Поряд із цим зростає увага до питань захисту персональних даних пацієнтів і контролю за правом власності на них [20]. Прикладом є витік даних у 2018 році, що охопив понад 13 мільйонів медичних записів, і став сигналом тривоги щодо вразливості систем [21]. Блокчейн 1.0 реалізував перші криптовалютні платформи [22], блокчейн 2.0 додав можливість реалізації смарт-контрактів [24], а блокчейн 3.0 розширює застосування технології в інших галузях, включно з охороною здоров’я [23].

Незважаючи на загальне визнання потенціалу блокчейну, багато дискусій довкола його застосування у сфері охорони здоров’я залишаються теоретичними або базуються на неправильних припущеннях. Тому необхідно здійснити глибокий аналіз поточного стану досліджень у сферах медицини, медичної інформатики та освіти [23], [28].

У цьому контексті важливу роль відіграють пристрої IoT, які забезпечують енергоефективні бездротові канали обміну даними [25]. Пристрої IoMT збирають фізіологічні показники пацієнтів — такі як артеріальний тиск, рівень кисню, пульс, температура тіла, маса, зріст і навіть

фази сну. У лікарняному середовищі це дозволяє лікарям і медсестрам оперативно діагностувати стан пацієнта та визначати подальші дії [26], [29].

Інтеграція електронних систем у звичні об’єкти (наприклад, ліжка, візки) у межах IoMT розширює можливості моніторингу пацієнтів у реальному часі. У разі необхідності лікарі мають більше часу на оцінку стану пацієнта, що може бути критичним для прийняття рішень про порятунок життя [27]. Такий підхід дає змогу не лише оптимізувати терапію, а й індивідуалізувати лікування відповідно до реальних біомедичних показників.

Сенсорні технології в межах IoMT здатні не лише моніторити стан здоров’я пацієнта, а й запобігати кризовим ситуаціям шляхом автоматичного аналізу показників та ініціювання відповідних дій. Вони формують нову парадигму у прийнятті медичних рішень, базуючись на реальних даних, доступних у режимі реального часу.

У сучасному контексті блокчейн все частіше розглядається як ключова технологія для безпечного, прозорого та контрольованого управління даними в IoT-платформах [30], [31], [32]. Застосування блокчейн у медицині дозволяє прискорити наукові дослідження, забезпечити захист конфіденційної інформації та створити нові канали співпраці між науковцями. Під час пандемії COVID-19 блокчейн продемонстрував ефективність у зборі та візуалізації даних, а також у боротьбі з маніпуляцією статистикою [33], [34].

2.3 Формування функціональних та нефункціональних вимог до системи обміну конфіденційною інформацією

В рамках даної роботи розглядається проєктування інформаційної системи, що реалізує безпечне зберігання, обмін і контроль доступу до конфіденційної медичної інформації із використанням блокчейн-технології та смарт-контрактів. Таке рішення дозволяє забезпечити незмінність, простежуваність та контрольовану відкритість даних, що є критично важливим у сфері охорони здоров’я.

Для коректного проєктування системи необхідно визначити ключових акторів, які взаємодіятимуть з системою, сформулювати функціональні вимоги, а також сценарії використання, які охоплюють типові дії користувачів.

У межах запропонованої інформаційної системи передбачено три основні категорії користувачів, які відіграють ключову роль у забезпеченні функціонування платформи. Першим актором є пацієнт, який виступає джерелом медичних даних та має повний контроль над їх обробкою. Він має можливість надавати або відкликати згоду на обробку своїх персональних медичних записів, а також переглядати історію доступу до них, що забезпечує прозорість дій з боку інших користувачів.

Другим актором є медичний працівник, який виступає у ролі споживача даних, необхідних для надання медичних послуг. Доступ до інформації пацієнта надається виключно після авторизації через смарт-контракти, що дозволяє гарантувати дотримання політик безпеки. Медичні фахівці можуть переглядати історії хвороб, вносити нові записи та фільтрувати інформацію відповідно до встановлених прав доступу.

Третім актором виступає адміністратор системи, відповідальний за технічне забезпечення функціонування блокчейн-мережі. До його обов’язків належать управління вузлами, обслуговування інфраструктури, а також створення та оновлення смарт-контрактів, що регулюють доступ до інформації. Ця роль не передбачає доступу до вмісту медичних записів, однак забезпечує цілісність і стабільність системи на інфраструктурному рівні.

Відповідно до визначених ролей користувачів та специфіки предметної області, система повинна задовольняти низку функціональних вимог, необхідних для її ефективного та безпечного функціонування. По-перше, передбачено реалізацію механізму реєстрації та автентифікації користувачів, що дозволяє ідентифікувати особу та забезпечити розмежування прав доступу до інформації. По-друге, контроль доступу до медичних даних має

здійснюватися за допомогою смарт-контрактів, які автоматично визначають можливість перегляду, редагування чи відкликання доступу згідно з політиками безпеки, зафіксованими у системі.

Крім того, система повинна підтримувати механізми журналізації дій користувачів із збереженням усіх транзакцій у блокчейні з точними часовими мітками, що забезпечить їхню прозорість і верифікацію. Надання та відкликання згоди на обробку персональних даних пацієнта також повинні бути реалізовані у вигляді смарт-контрактів, що зберігаються у реєстрі та мають юридичну силу. Важливою вимогою є підтримка інтеграції із зовнішніми системами (такими як EHR або PACS) із дотриманням стандартів обміну медичними даними, зокрема HL7 та FHIR, що забезпечить сумісність з існуючою інфраструктурою медичних закладів.

Для підвищення рівня достовірності інформації система повинна містити функціонал перевірки цілісності записів через хеш-функції, що унеможливлює зміну або підробку даних. Крім того, важливо реалізувати інструменти для зручного пошуку, фільтрації та перегляду записів відповідно до прав доступу користувачів, що покращить практичне використання платформи у щоденній роботі медичних установ.

Функціональні вимоги до системи представлено у таблиці 2.2

Таблиця 2.2 – Взаємозв’язок акторів, сценаріїв використання та функціональних вимог

Актор	Сценарій використання	Функціональні вимоги
1	2	3
Пацієнт	Надання згоди на обробку медичних даних	F4 – Надання згоди
	Відкликання згоди на обробку даних	F2 – Контроль доступу через смарт-контракти

Продовження таблиці 2.2

1	2	3
	Перегляд історії доступу до своїх записів	F3 – Журналізація дій користувачів
Медичний працівник	Запит доступу до медичних записів пацієнта	F2 – Контроль доступу через смарт-контракти
	Внесення нових медичних записів	F6 – Перевірка цілісності даних
	Пошук та перегляд історії медичних записів	F7 – Пошук, перегляд і фільтрація
Адміністратор системи	Створення та конфігурація смарт-контрактів	F2, F4 – Контроль доступу, згода
	Управління вузлами та мережею блокчейну	F1 – Реєстрація та автентифікація
	Забезпечення технічного обслуговування	F1 – Інфраструктурне адміністрування

У процесі проєктування системи зберігання та обміну конфіденційною медичною інформацією на основі блокчейну та смарт-контрактів особливу увагу слід приділити нефункціональним вимогам, які визначають якість, надійність, сумісність та ефективність роботи системи в реальних умовах. Ці вимоги не описують конкретні функції системи, однак безпосередньо впливають на її здатність до стабільного та безпечного функціонування в умовах динамічного навантаження та високих вимог до захисту даних.

Одним із критично важливих аспектів є захищене зберігання даних. У зв’язку з великим обсягом медичних даних, зокрема діагностичних зображень, відеофайлів та звітів, система повинна реалізовувати гібридну

модель зберігання. Вона передбачає використання блокчейну для збереження хешів і метаданих, тоді як самі файли зберігаються у зовнішніх репозиторіях, таких як IPFS або хмарні сховища. Такий підхід дозволяє ефективно перевіряти цілісність інформації при мінімальному навантаженні на блокчейн.

Не менш важливою є реалізація механізмів автоматизованого надання та відкликання згоди пацієнта. Система має фіксувати кожен факт згоди чи її відкликання за допомогою смарт-контрактів, що забезпечує юридичну легітимність дій користувачів і виключає можливість підробки. Цей механізм має працювати в межах заздалегідь визначених сценаріїв (наприклад, участь у клінічних дослідженнях або тимчасовий доступ до даних).

Високі вимоги пред’являються і до механізмів простежуваності походження даних. Система повинна зберігати повну історію трансформацій даних, дозволяючи чітко визначити, хто, коли і з якою метою вносив зміни до записів. Це підвищує рівень довіри до даних як з боку пацієнтів, так і з боку лікарів і дослідників.

Однією з необхідних нефункціональних характеристик є міжсистемна сумісність. Система повинна підтримувати стандарти HL7 FHIR, що дозволяє забезпечити обмін інформацією з іншими медичними інформаційними системами без втрати даних або дублювання інформації. Така сумісність дає змогу інтегрувати платформу в існуючу інфраструктуру охорони здоров’я.

Надійність і відмовостійкість також є невід’ємними складовими. Система повинна забезпечувати безперервність функціонування навіть у випадку виходу з ладу окремих вузлів блокчейн-мережі. Розподілений характер архітектури дозволяє мінімізувати ризики втрати даних або порушення їхньої цілісності.

Останнім важливим нефункціональним параметром є масштабованість і продуктивність. Система повинна обробляти велику кількість транзакцій у режимі реального часу, що можливо лише за умови використання високоефективних механізмів консенсусу, таких як PBFT або Raft, що

дозволяють збалансувати швидкодію та безпеку.

В таблиці 2.3 представлено нефункціональні вимоги, критерії вимірювання та цільові значення.

Таблиця 2.3 – Нефункціональні вимоги, критерії вимірювання та цільові значення

№	Нефункціональна вимога	Критерій вимірювання	Цільове значення
1	2	3	4
1	Захищене зберігання даних	Тип архітектури зберігання	Гібридна: IPFS + хеші у блокчейні
2	Автоматизоване управління згодою пацієнта	Час обробки запиту на зміну згоди	Не більше 2 секунд
3	Простежуваність і доказ походження даних	Повнота журналу змін	100% збереження історії змін у блокчейні
4	Міжсистемна сумісність	Підтримка відкритих медичних стандартів	HL7 FHIR (v4.0 і вище), REST API
5	Надійність і відмовостійкість	Доступність системи (Uptime)	Не менше 99.9% на місяць
6	Масштабованість і продуктивність	Кількість оброблених транзакцій на секунду (TPS)	Мінімум 100 TPS при піковому навантаженні
7	Перевірка цілісності даних	Час хеш-верифікації запису	Не більше 500 мс

3 ПРОЄКТУВАННЯ АРХІТЕКТУРИ ТА ПРОГРАМНИХ КОМПОНЕНТІВ СИСТЕМИ ЗБЕРІГАННЯ ТА ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

3.1 Проєктування архітектури системи

Архітектура системи, реалізованої на основі Hyperledger Fabric, спрямована на забезпечення безпечного, надійного та контрольованого управління медичними даними в умовах багатосторонньої взаємодії між суб’єктами медичної сфери. Вона реалізує концепцію багаторівневої розподіленої системи, яка охоплює клієнтський рівень, рівень сервісної логіки, мережевий рівень розподіленого реєстру та інфраструктурний рівень зберігання даних. У такій архітектурі кожен структурний компонент виконує чітко визначену функцію, зберігаючи при цьому цілісність інформаційних потоків і відповідність стандартам інформаційної безпеки у сфері охорони здоров’я.

Клієнтський рівень представлено програмними інтерфейсами для трьох основних типів користувачів: пацієнтів, медичних працівників та адміністраторів. Застосунок для пацієнтів дозволяє керувати згодою на обробку персональних медичних даних та переглядати історію доступу до них. Медичний застосунок забезпечує введення нових медичних записів та запити на доступ до наявної інформації, а адміністративний інтерфейс використовується для конфігурації мережі, керування доступом та підтримки смарт-контрактів. Усі клієнтські застосунки взаємодіють з мережею за допомогою відповідних SDK, що реалізують механізми підпису, шифрування і надсилання транзакцій до блокчейн-мережі.

Сервісна логіка, що реалізується у вигляді незалежних прикладних сервісів, виконує основну бізнес-функціональність системи. Компонент автентифікації перевіряє сертифікати користувачів за допомогою Membership Service Provider (MSP), що функціонує в межах Fabric. Сервіс управління

доступом обробляє запити на доступ, перевіряє дозволи та фіксує факти взаємодії з медичними даними у розподіленому реєстрі. Обробник медичних записів виконує синхронізацію між блокчейн-реєстром та зовнішнім сховищем, зберігаючи об’ємні або чутливі дані поза межами ланцюга блоків.

На рівні блокчейн-мережі функціонує інфраструктура Hyperledger Fabric, яка включає peer-вузли, ordering service, chaincode та інші допоміжні сервіси. Peer-вузли, що належать до організацій-учасників, приймають транзакції, виконують chaincode, зберігають журнали та забезпечують доступ до розподіленого реєстру. Ordering service формує блоки транзакцій і поширює їх серед peer-вузлів. Смарт-контракти, реалізовані як chaincode, виконують бізнес-логіку перевірки згод, реєстрації доступу та фіксації операцій. Верифікація всіх учасників, зокрема користувачів, застосунків і вузлів, здійснюється через MSP, який базується на сертифікатній інфраструктурі з використанням X.509-сертифікатів.

Для забезпечення ефективного зберігання медичних даних система використовує комбінований підхід, що поєднує збереження у розподіленому реєстрі (on-chain) і в зовнішніх базах даних (off-chain). У розподіленому реєстрі зберігається інформація про згоду, операції доступу та посилання на медичні записи, тоді як самі записи, через обсяг або конфіденційність, зберігаються у зовнішньому сховищі, наприклад, у CouchDB або PostgreSQL. Зв’язок між on-chain і off-chain елементами підтримується за допомогою хешів та ідентифікаторів, що гарантує контроль цілісності та узгодженості даних.

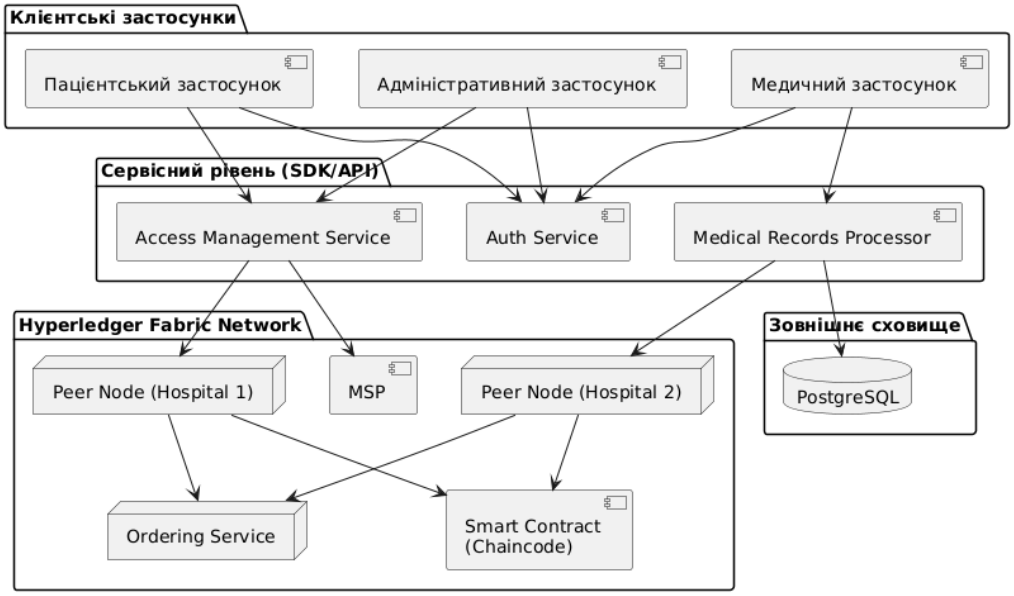

Рисунок 3.1 – Архітектура системи

Загалом, архітектура системи (рисунок 3.1) створює надійне середовище для взаємодії між медичними установами, пацієнтами та регуляторними органами. Вона підтримує ключові принципи розподіленого управління даними, включно з прозорістю, незмінністю, контрольованим доступом та масштабованістю. Застосування Hyperledger Fabric дозволяє досягти високого рівня конфіденційності через підтримку приватних каналів, гнучкі політики ендорсменту та криптографічну перевірку кожного учасника мережі. Таким чином, запропонована архітектура відповідає вимогам до сучасних інформаційних систем у сфері охорони здоров’я як з технічного, так і з нормативно-правового погляду.

3.2 Проєктування програмних компонентів системи

3.2.1 Діаграма варіантів використання

Визначення акторів у п.2.3 дозволяє окреслити основні варіанти використання системи, що відповідають їхнім функціональним ролям. Пацієнт, як основне джерело медичної інформації, може самостійно надати

або відкликати згоду на обробку персональних даних шляхом взаємодії з відповідним смарт-контрактом. Він також має змогу здійснювати моніторинг історії доступу до своїх даних, що підвищує довіру до системи з боку користувачів.

Медичний працівник, у межах наданих йому прав, здійснює запит доступу до медичних записів пацієнта для діагностики або лікування. Після отримання дозволу через смарт-контракт, він має можливість переглядати відповідні дані, вносити нові медичні записи, а також використовувати інструменти пошуку та фільтрації, що спрощують роботу з великим обсягом інформації.

Адміністратор системи взаємодіє з нею на інфраструктурному рівні, забезпечуючи стабільну роботу блокчейн-мережі, створюючи смарт-контракти, а також контролюючи технічні параметри функціонування вузлів. Його діяльність критично важлива для забезпечення надійності, безпеки та безперебійності роботи всієї системи. Діаграма використання системи представлена на рисунку 3.1.

Рисунок 3.2 – Діаграмма варіантів використання

3.2.2 Діаграма компонентів

Діаграма компонентів (рисунок 3.3) відображає архітектуру системи електронної взаємодії між пацієнтами, медичними працівниками та адміністраторами в контексті управління медичними даними із застосуванням смарт-контрактів та блокчейн-технологій. Архітектура системи побудована за принципами розподіленої модульності, де кожен компонент виконує чітко визначену функцію, забезпечуючи при цьому масштабованість та безпеку.

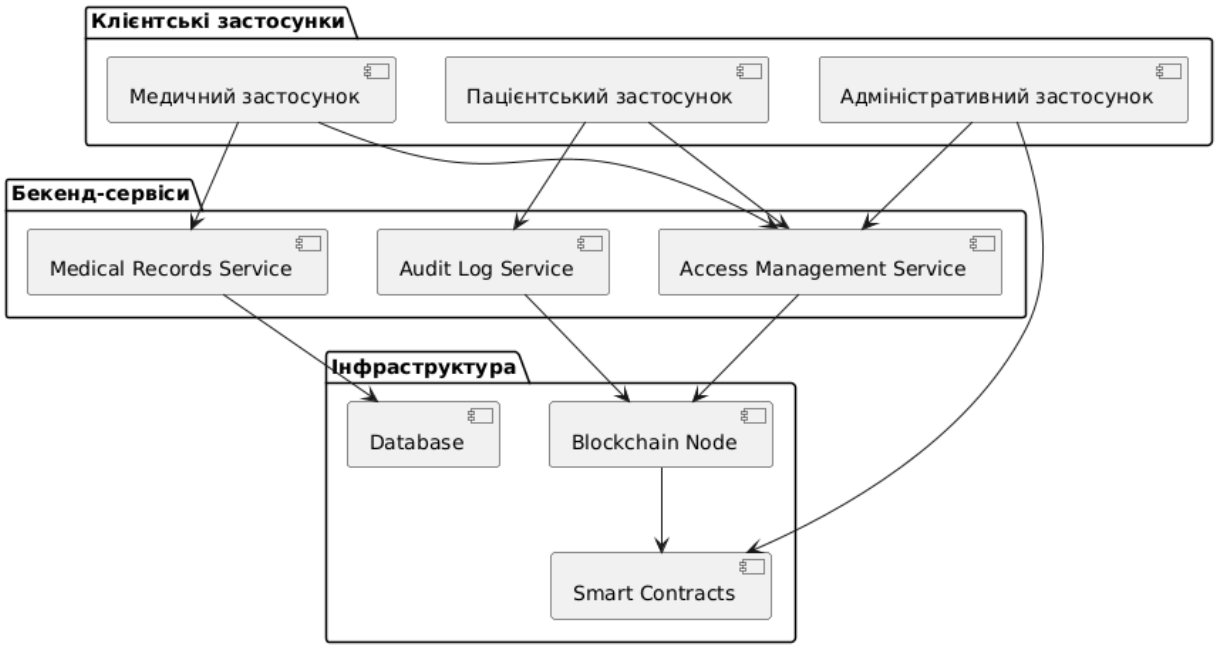

Рисунок 3.3 – Діаграма компонентів

На рівні клієнта передбачено три типи застосунків, кожен з яких відповідає за взаємодію конкретного типу користувача з системою. Пацієнтський застосунок забезпечує інтерфейс для надання або відкликання згоди на обробку персональних даних, а також перегляд історії доступу до них. Медичний застосунок дозволяє медичним працівникам отримувати доступ до медичних записів пацієнтів та додавати нові дані. Адміністративний застосунок орієнтований на забезпечення конфігурації системи, зокрема на управління смарт-контрактами та іншими аспектами

інфраструктури.

У бекенд-частині системи виділяються три основні сервіси. Сервіс управління доступом (Access Management Service) є ключовим елементом, який здійснює перевірку прав доступу, обробку згод пацієнтів та взаємодію зі смарт-контрактами через блокчейн-вузол. Сервіс медичних записів (Medical Records Service) відповідає за зберігання, обробку та надання доступу до медичної інформації, яка фізично зберігається у базі даних за межами блокчейну. Сервіс журналу аудиту (Audit Log Service) фіксує всі звернення до персональних даних, забезпечуючи прозорість доступу.

Інфраструктурна частина системи базується на блокчейн-вузлі, який забезпечує виконання смарт-контрактів і гарантує незмінність транзакцій, пов’язаних із наданням згод і логуванням дій. Смарт-контракти реалізують бізнес-логіку, пов’язану з управлінням згодами, перевіркою прав доступу та створенням записів аудиту. База даних використовується для зберігання об’ємної та чутливої інформації, яка не потребує прямого збереження у блокчейні, однак її доступ строго регламентується через смарт-контракти та відповідні сервіси.

Узгоджена взаємодія між цими компонентами забезпечує як функціональну повноту системи, так і відповідність вимогам безпеки, прозорості та контролю доступу до медичних даних в умовах децентралізованої архітектури.

3.2.3 Діаграма послідовності

Діаграма послідовності (рисунок 3.4) описує взаємодію між ключовими учасниками системи електронного медичного документообігу, реалізованої на основі Hyperledger Fabric. В рамках сценарію внесення медичних даних, пацієнт передає інформацію через госпітальний клієнт, який автентифікується за допомогою MSP (Membership Service Provider). Після підтвердження ідентичності, застосунок формує транзакцію та відправляє її

на peer-вузол для ендорсменту, де відбувається симуляція виконання chaincode. Отримані підписи передаються до ordering service, який агрегує транзакції у блоки та надсилає їх назад до peer-вузлів, де відбувається остаточне виконання chaincode та запис у ledger.

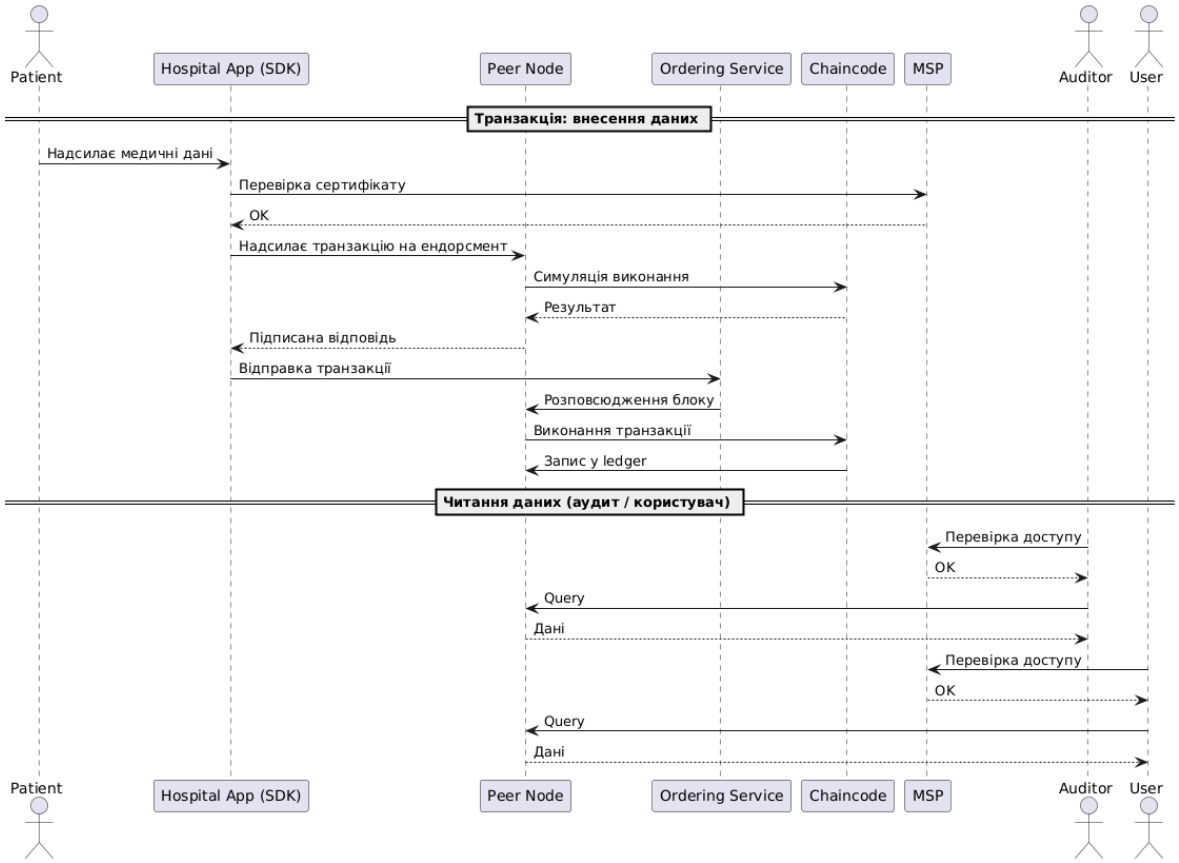

Рисунок 3.4 – Діаграма послідовності

У сценарії читання даних аудитором або користувачем, запит проходить перевірку прав доступу через MSP і після підтвердження пересилається на peer-вузол, який відповідає необхідними даними. Це забезпечує цілісність доступу, прозорість дій та захищеність конфіденційної інформації у межах розподіленої довіреної інфраструктури.

3.2.4 Діаграма розгортання

Діаграма розгортання (рисунок 3.5) ілюструє архітектуру системи керування медичними даними, реалізованої на основі Hyperledger Fabric. Пацієнт ініціює передачу даних через клієнтський застосунок, що взаємодіє з SDK Fabric, після чого дані надсилаються до обробника, який готує їх до запису у блокчейн. Оброблені дані надходять до peer-вузлів госпіталів, де активується chaincode (смарт-контракт), і формується транзакція.

Усі peer-вузли надсилають пропозиції до ordering service, який формує блоки й розповсюджує їх до peer-вузлів для остаточного збереження. Chaincode виконується на рівні peer-вузлів, а автентифікація та авторизація всіх учасників — як лікарень, так і зовнішніх клієнтів (аудиторів, користувачів) — здійснюється через компонент MSP.

Ця структура дозволяє досягти високого рівня безпеки, прозорості та контрольованого доступу до чутливих медичних записів у децентралізованому середовищі.

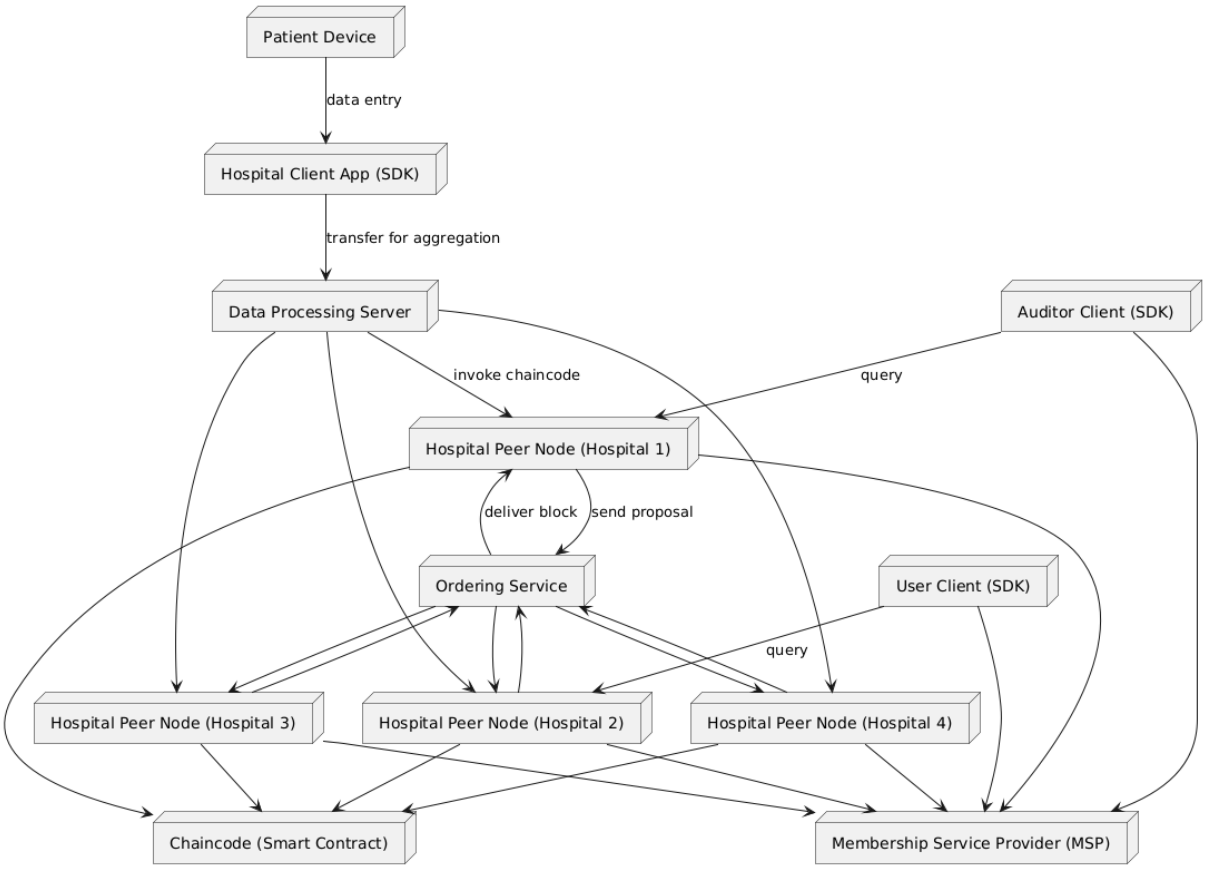

Рисунок 3.5 – Діаграма розгортання

3.3 Проєктування моделі даних

У контексті побудови децентралізованої системи для управління медичною інформацією модель даних має ключове значення для забезпечення структурованості, достовірності та відповідності правовим нормам. Оновлена модель охоплює чотири взаємопов’язані сутності: MedicalData, OperationalBehavior, User та Consent.

Сутність MedicalData описує кожен блок даних, що записується у блокчейн, із вказанням його типу, джерела, формату, стадії обробки та криптографічного підпису. Кожен медичний запис пов’язаний з операцією (OperationalBehavior), яка його згенерувала або модифікувала. Ця друга сутність відображає транзакційні дії в системі, їх авторство та входи/виходи у вигляді зв’язків з іншими медичними даними. Важливу роль відіграє атрибут OpSign, який виступає унікальним ідентифікатором кожної операції та пов’язує дії з результатами.

Модель доповнюється сутністю User, яка репрезентує всіх учасників системи: пацієнтів, лікарів, адміністраторів або аудиторів. Кожен користувач має унікальний ідентифікатор, роль, криптографічний сертифікат та інформацію про організаційну приналежність. Це дозволяє контролювати права доступу та здійснювати персоніфіковану верифікацію транзакцій.

Сутність Consent формалізує процес надання або відкликання згоди користувачем на обробку його персональних медичних даних. Кожна згода пов’язується з конкретним користувачем, фіксується у вигляді транзакції в блокчейні, містить часові позначки, статус, а також може посилатися на відповідний DataSign. Завдяки цьому створюється юридично обґрунтована та технологічно верифікована модель управління доступом до чутливої інформації. Опис сутностей представлено в таблиці 3.1 та на рисунку 3.6.

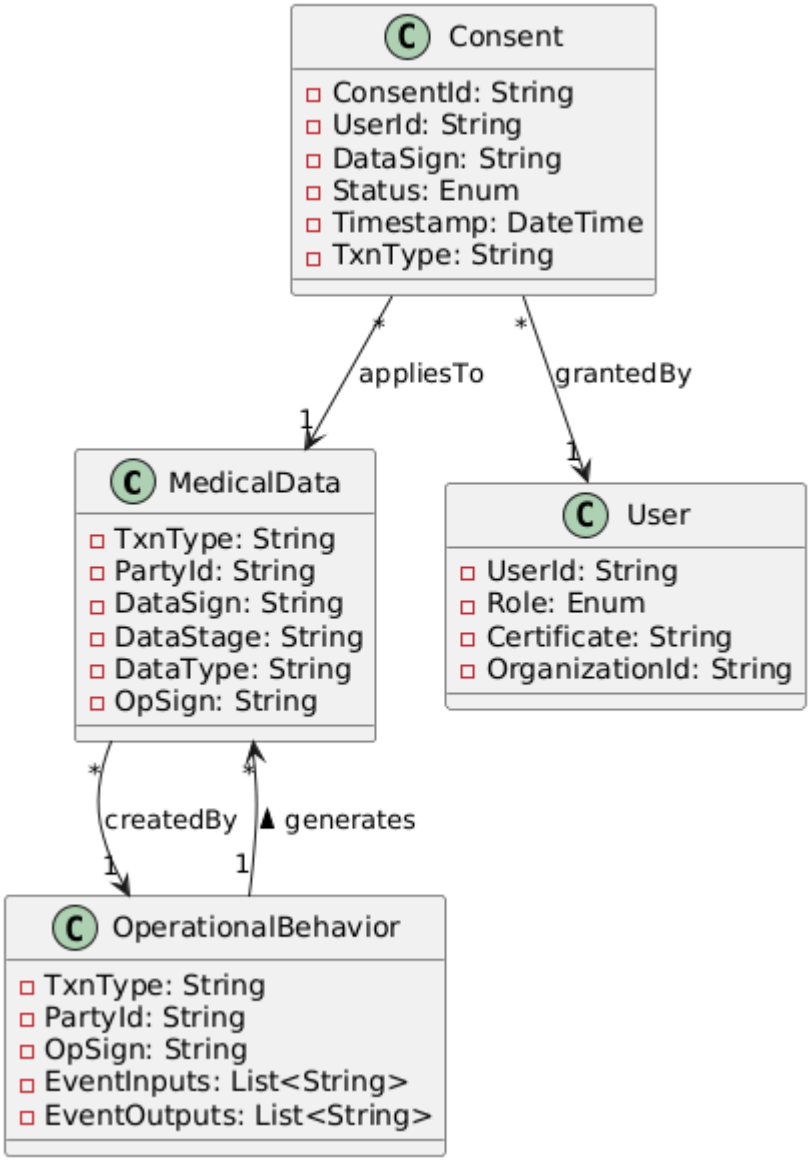

Рисунок 3.6 – Структура даних системи

Таблиці 3.1 – Опис атрибутів сутностей моделі

Сутність	Атрибут	Тип	Опис
1	2	3	4
MedicalData	TxnType	String	Тип транзакції (data).
	PartyId	String	Ідентифікатор організації-учасника.

Продовження таблиці 3.1

1	2	3	4
	DataSign	String	Унікальний підпис/хеш медичних даних.
	DataStage	String	Стадія обробки (raw, processed тощо).
	DataType	String	Формат даних (файл, БД, API).
	OpSign	String	Ідентифікатор операції, що породила ці дані.
OperationalBehavior	TxnType	String	Тип транзакції (operation).
	PartyId	String	Ідентифікатор організації-ініціатора.
	OpSign	String	Унікальний ідентифікатор операції.
	EventInputs	List<String>	Список DataSign вхідних даних.
	EventOutputs	List<String>	Список DataSign вихідних результатів.
User	UserId	String	Унікальний ідентифікатор користувача.

Продовження таблиці 3.1

1	2	3	4
	Role	Enum (Patient, Doctor, Admin, Auditor)	Роль користувача у системі.
	Certificate	String	Криптографічний сертифікат або публічний ключ.
	OrganizationId	String	Організація, до якої належить користувач.
Consent	ConsentId	String	Унікальний ідентифікатор згоди.
	UserId	String	Посилання на користувача, який надає згоду.
	DataSign	String	Посилання на об’єкт MedicalData, що є предметом згоди.
	Status	Enum (Given, Revoked)	Статус згоди.
	Timestamp	DateTime	Час надання або відкликання згоди.
	TxnType	String	Тип транзакції (наприклад, consent).

Загалом, запропонована структура забезпечує високий рівень простежуваності, контрольованості та відповідності принципам етичного поводження з персональними даними. Усі зв’язки моделі мають чітке семантичне обґрунтування та логічну відповідність вимогам до розподілених систем обміну медичними даними.

Концепція Data Lineage, або історії змін даних, у системах управління медичною інформацією, реалізованих на основі технологій розподіленого реєстру, виконує критично важливу функцію забезпечення простежуваності, достовірності та цілісності медичних записів протягом усього їх життєвого циклу. У запропонованій моделі, реалізованій у контексті Hyperledger Fabric, Data Lineage реалізується як послідовність зв’язаних транзакційних дій, які формують граф взаємозв’язку між первинними даними, операціями та результатами обробки (рисунок 3.7).

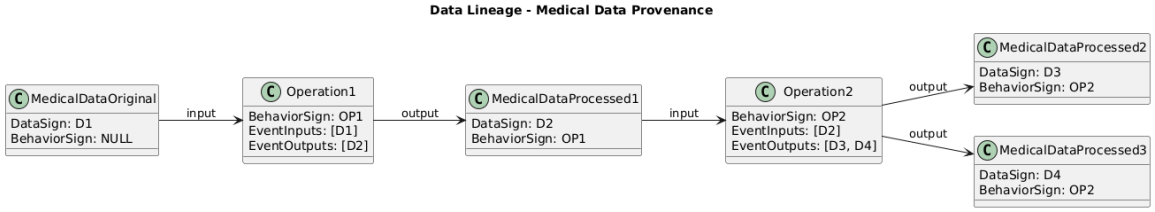

Рисунок 3.7 - Граф взаємозв’язку між первинними даними, операціями та результатами обробки

На логічному рівні, кожна одиниця медичних даних (MedicalData) має унікальний підпис (DataSign), який виступає криптографічним ідентифікатором конкретного об’єкта. Якщо запис є первинним, тобто ще не був оброблений у межах жодної транзакції, атрибут BehaviorSign, що вказує на породжуючу операцію, залишається порожнім (NULL). У цьому випадку об’єкт вважається джерелом походження (data origin).

Будь-яка транзакція, яка обробляє або модифікує медичні дані, представлена у системі як об’єкт типу OperationalBehavior. Така транзакція

має унікальний ідентифікатор (BehaviorSign), та містить два основних компоненти: вхідні дані (EventInputs) і вихідні дані (EventOutputs), представлені у вигляді масивів DataSign. Таким чином, транзакція формує відображення даних до і даних після виконання певної операції, створюючи причинно-наслідкові зв’язки.

Наприклад, якщо первинний запис D1 є вхідним для транзакції OP1, яка породжує новий запис D2, то між D1 і D2 утворюється односпрямований зв’язок через OP1. Якщо ж D2 пізніше стає вхідним у транзакцію OP2, яка породжує D3 та D4, ланцюг змін продовжується. Така структура природно утворює орієнтований ациклічний граф (DAG), що дозволяє точно простежити шлях перетворення даних від початкового стану до будь-якого похідного.

У сукупності ця модель підтримує реалізацію таких функцій, як:

- трасування походження даних (provenance tracking) — встановлення джерела кожного елементу даних;
- аудит змін — фіксація часу, авторства, обґрунтування кожної операції;
- валідація достовірності — перевірка того, що дані не були змінені поза дозволеними каналами;
- формування історії обробки — необхідна функція в клінічних дослідженнях та регуляторному контролі.

Завдяки використанню атрибутів DataSign і BehaviorSign, які зберігаються у блокчейні, забезпечується незмінність і криптографічна доказовість кожної одиниці даних та кожної дії над нею. Це особливо важливо в умовах правового регулювання медичної діяльності, де кожна зміна має бути верифікованою та зворотно простежуваною.

У результаті, концепція Data Lineage у блокчейн-системі не лише сприяє підвищенню рівня довіри до цифрових медичних записів, але й створює об’єктивну інформаційну основу для прийняття клінічних, адміністративних або правових рішень.

У сучасних інформаційних системах, що функціонують у сфері охорони здоров’я, одним із ключових аспектів є забезпечення повної простежуваності змін медичних даних. Це особливо критично в умовах багатостороннього доступу, де беруть участь пацієнти, лікарі, адміністратори, аудитори та автоматизовані служби. Для забезпечення достовірності, незмінності та юридичної підтверджуваності походження кожного інформаційного об'єкта доцільно використовувати DAG-модель історії змін (Data Lineage DAG).

Основою цієї моделі є орієнтований ациклічний граф (DAG — Directed Acyclic Graph). У теоретичному контексті, DAG — це структура графу, яка складається з вершин і спрямованих ребер, де жоден цикл не може бути утворений. Інакше кажучи, неможливо почати з деякої вершини, слідувати по напрямку стрілок і повернутись до тієї самої вершини. Така властивість є надзвичайно важливою для відображення процесів перетворення або обробки даних, які відбуваються односторонньо в часі — тобто від минулого до майбутнього.

Основою цієї моделі є орієнтований ациклічний граф (DAG — Directed Acyclic Graph). У теоретичному контексті, DAG — це структура графу, яка складається з вершин і спрямованих ребер, де жоден цикл не може бути утворений. Інакше кажучи, неможливо почати з деякої вершини, слідувати по напрямку стрілок і повернутись до тієї самої вершини. Така властивість є надзвичайно важливою для відображення процесів перетворення або обробки даних, які відбуваються односторонньо в часі — тобто від минулого до майбутнього.

У запропонованій медичній блокчейн-системі кожен об’єкт MedicalData є вершиною DAG, а кожна транзакція або операція OperationalBehavior, яка змінює ці дані, є окремим вузлом логіки перетворення (рисунок 3.8). Зв’язки між вузлами реалізуються через пари:

- EventInputs — набір DataSign, що були використані як вхідні дані для операції;

- EventOutputs — набір DataSign, що були сформовані як результат цієї операції.

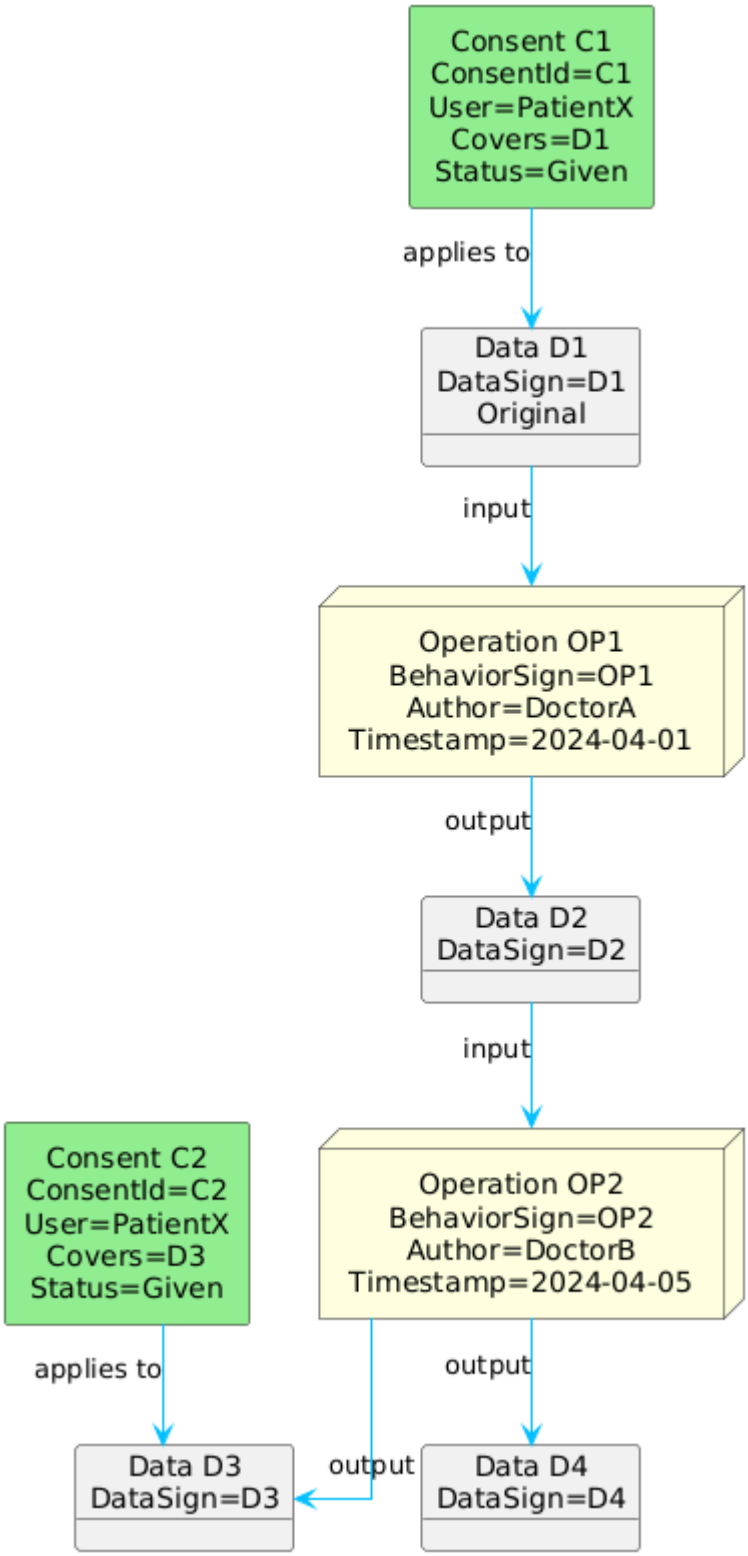

Рисунок 3.8 - DAG-модель змін даних

Таким чином, якщо Data D1 є початковим записом (із BehaviorSign =

NULL), він може бути використаний в операції OP1, яка створює новий запис D2. Далі D2 може бути перетворений за допомогою іншої транзакції OP2 у записи D3 і D4. В результаті цього виникає ланцюг перетворення даних, у якому кожен новий запис пов’язаний з попередніми на підставі визначених транзакцій, а весь ланцюг не містить циклів, що забезпечує однозначну історію змін.

На практиці DAG-модель:

- гарантує, що кожен запис має лише одного безпосереднього "батька", що виключає неоднозначність походження;
- дозволяє будувати запити на відновлення повної історії походження будь-якого запису (data provenance);
- сприяє реалізації аудиту, оскільки вся інформація про час, автора операції, використовувані і створені дані зберігається у вузлах графа;
- забезпечує контроль доступу та згоди через асоціацію вузлів даних з об’єктами типу Consent, які відображають правовий статус кожного елементу.

У розширеній моделі також враховується інформація про ініціаторів змін (авторів транзакцій) та час виконання операцій, що дозволяє впроваджувати хронологічну простежуваність. Кожен вузол OperationalBehavior містить поля Author і Timestamp, що робить можливим формування темпоральних запитів і аналіз змін у динаміці.

Крім того, до DAG інтегруються об’єкти типу Consent, що встановлюють або обмежують доступ до певних DataSign. Це дозволяє поєднати технічну трасування з правовими аспектами обробки персональних даних.

4 ДОСЛІДЖЕННЯ ПРОТОТИПУ СИСТЕМИ ЗБЕРІГАННЯ ТА ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

4.1 Експериментальна платформа

Для перевірки ефективності створеної платформи управління медичними даними було проведено серію експериментів, що включали завантаження, запитування та простеження джерел медичних даних у блокчейн-мережі. Проведення експериментів охоплювало аналіз експериментального середовища, структури вхідних даних, а також оцінювання отриманих результатів.

Експериментальне середовище було реалізовано на базі трьох віртуальних серверів, розгорнутих у хмарному середовищі AWS EC2.

Конфігурації серверів наведено у таблиці 4.1.

Таблиця 4.1 - Апаратне середовище

№ сервера	Призначення	Операційна система	Процесор	Оперативна пам’ять	Диск (SSD)	Мережева пропускна здатність
1	2	3	4	5	6	7
1	Orderer-кластер	Ubuntu 20.04	32 ядер	64 ГБ	500 ГБ	1 Гбіт/с
2	Peer-вузли лікарень	Ubuntu 20.04	16 ядер	64 ГБ	500 ГБ	1 Гбіт/с
3	Peer-вузли лікарень + медична хмара	Ubuntu 20.04	16 ядер	64 ГБ	500 ГБ	1 Гбіт/с

Для розгортання блокчейн-мережі, реалізації смарт-контрактів, керування сертифікатами та проведення тестування використовувався наступний програмний стек.

Таблиця 4.2 - Програмне середовище

Назва програмного забезпечення	Версія	Призначення
1	2	3
Docker	20.0	Контейнеризація компонентів системи
Hyperledger Fabric	2.4	Побудова блокчейн-мережі
Fabric-CA	1.5	Керування цифровими сертифікатами
Caliper	0.5	Вимірювання продуктивності блокчейн-мережі
Apache JMeter	5.6.3	Генерація навантаження та тестування запитів
Node.js	Остання стабільна	Розробка клієнтських застосунків і логіки взаємодії з мережею
Golang	1.8+	Розробка смарт-контрактів
Shell-скрипти	—	Автоматизація процесів розгортання

У рамках експерименту було розгорнуто сім організацій, що брали участь у симуляції взаємодії у сфері охорони здоров’я:

- 1 регуляторна організація (контроль доступу, аудит);

- 1 організація медичної хмари (централізоване сховище);
- 5 лікарень (розподілені учасники обміну даними).

Кожна організація мала три вузли типу peer, які брали участь у збереженні блоків, перевірці транзакцій та забезпеченні децентралізованої структури мережі. Кластер Orderer, відповідальний за узгодження транзакцій, було розгорнуто на сервері з найбільшою обчислювальною потужністю.

Розподіл організацій між серверами відображено на рисунку 4.1.

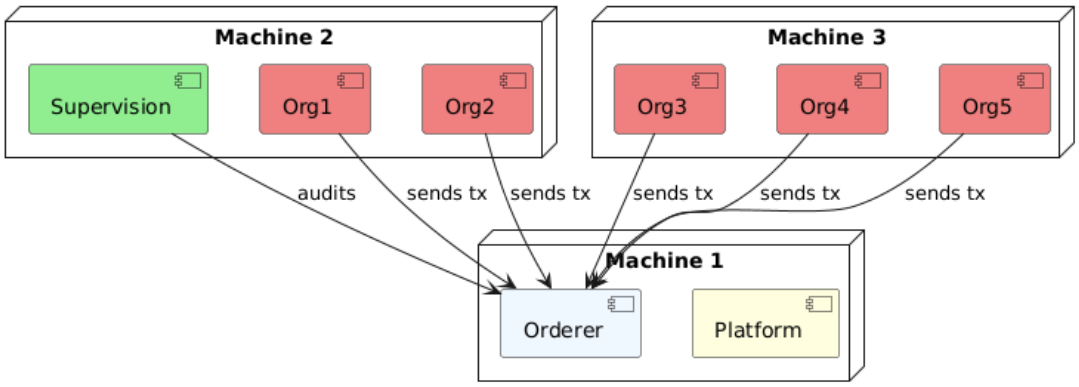

Рисунок 4.1 – Діаграма розгортання експериментальної платформи

Діаграма розгортання (рисунок 4.1) моделює фізичне розміщення ключових компонентів Hyperledger Fabric у межах системи. Вузли мережі логічно поділені на три машини:

- Machine 1 виконує функції інфраструктури, зокрема обробку консенсусу через компонент Orderer та роботу з API або SDK через модуль Platform. Саме тут агрегуються транзакції;
- Machine 2 слугує вузлом організаційної участі й нагляду, містить дві повноцінні організації (Org1, Org2) та компонент Supervision, який може виконувати функції аудитора, сертифікаційного органу (CA) або адміністрування консенсусу;
- Machine 3 об'єднує три організації (Org3, Org4, Org5), які ймовірно, беруть участь у мережі як endorsers, або забезпечують спеціалізовану обробку/читання транзакцій.

Логічні зв’язки вказують на взаємодію кожної організації з ордеринг-сервісом (Orderer), що відображає типову схему взаємодії Fabric peer-вузлів із ordering-сервісом для обробки транзакцій.

4.2 Експериментальні данні

У рамках верифікації ефективності запропонованої платформи для управління конфіденційною медичною інформацією було сформовано експериментальний набір даних, який за структурою та обсягом відповідає типовим сценаріям використання в інформаційних системах охорони здоров’я. Дані було згенеровано штучно з метою забезпечення конфіденційності, однак вони відповідають загальноприйнятим стандартам представлення медичної інформації, зокрема HL7 та FHIR.

Експериментальні дані включали персоналізовані відомості про пацієнтів, історії хвороб, діагностичні результати, лікарські призначення, а також запити на доступ до медичних записів з боку різних організацій. Враховано також часову динаміку подій та взаємозв’язки між об’єктами, що дозволяє відтворити умови функціонування децентралізованої медичної системи в реальному часі.

Загальний обсяг експериментального набору склав понад 500 000 записів, які охоплюють понад 5 000 умовно унікальних пацієнтів, кілька сотень лікарів та десятки установ різного профілю. Дані подані у форматах JSON, XML та, частково, DICOM, що дозволяє адаптувати їх до потреб як внутрішнього зберігання в блокчейн-мережі, так і зовнішніх децентралізованих сховищ типу IPFS.

Характеристики та структура експериментальних даних узагальнені у таблиці 4.3.

Таблиця 4.3 – Опис експериментальних даних

Тип даних	Кількість записів	Формат	Примітки
1	2	3	4
Пацієнти	5 000	JSON	Основні відомості та медична історія
Призначення лікарів	12 000	JSON/XML	Рецепти, плани лікування, консультації
Діагностичні результати	7 500	JSON/DICOM	Дані аналізів, зображення, висновки
Запити доступу	15 000	JSON	Запити від різних організацій системи

Такий підхід до формування експериментальних даних дозволяє не лише здійснити функціональне тестування розроблених компонентів, але й провести якісну оцінку їх масштабованості, продуктивності та стійкості до зміни умов навантаження.

4.3 Аналіз результатів дослідження

4.3.1 Дослідження продуктивності із завантаження та запитів даних

З метою оцінки продуктивності побудованої блокчейн-платформи управління медичною інформацією було проведено серію експериментів із завантаженням і запитом даних. Основною метою дослідження було вивчення впливу кількості організацій у мережі на ключові показники продуктивності, зокрема: швидкість надсилання запитів (Send Rate),

максимальну затримку (Max Latency), мінімальну та середню затримки (Min / Avg Latency), а також пропускну здатність (Throughput).

Для тестування використовувався інструмент Hyperledger Caliper, у якому було налаштовано 10 віртуальних працівників (workers), які здійснили 100 000 випадкових операцій із завантаження та запитів медичних і поведінкових даних. Тестування проводилося на блокчейн-мережах із різною кількістю організацій (від 3 до 7). Після п’яти ітерацій кожного тесту було отримано усереднені результати (таблиця 4.4).

Таблиця 4.4 - Результати завантаження медичних даних

Кількість організацій	Send Rate (TPS)	Throughput (TPS)	Max Latency (c)	Avg Latency (c)
1	2	3	4	5
3	1361.7	1349.3	2.05	0.11
7	794.7	782.8	2.28	0.37

Результати експериментів свідчать, що із збільшенням кількості організацій спостерігається стабільна тенденція до зменшення показників пропускної здатності (TPS). Зокрема, для завантаження медичних даних при 3 організаціях throughput становив 1349,3 TPS, а при 7 організаціях – 782,8 TPS. Аналогічно зменшився send rate з 1361,7 до 794,7 TPS. При цьому максимальна затримка зросла з 2,05 с до 2,28 с, а середня – з 0,11 с до 0,37 с (таблиця 4.4). Схожі результати були зафіксовані і для поведінкових даних. Так, при збільшенні кількості організацій з 3 до 7 throughput зменшився з 1247,1 до 778,6 TPS, а середня затримка зросла з 0,10 с до 0,37 с (Таблиця 4.5).

Таблиця 4.5 - Результати завантаження поведінкових даних

Кількість організацій	Send Rate (TPS)	Throughput (TPS)	Max Latency (c)	Avg Latency (c)
1	2	3	4	5
3	1256.3	1247.1	2.03	0.10
7	789.9	778.6	2.04	0.37

У разі виконання запитів до медичних даних, спостерігалася аналогічна тенденція: throughput зменшився з 1603,2 TPS до 1179,9 TPS, а середня затримка зросла з 0,09 с до 0,26 с. Поведінкові дані демонстрували схожі показники зниження, зокрема throughput зменшився з 1599,8 до 1173,8 TPS, а середня затримка зросла з 0,09 до 0,27 с (Таблиці 4.6-4.7).

Таблиця 4.6 - Результати запитів до поведінкових даних

Кількість організацій	Send Rate (TPS)	Throughput (TPS)	Max Latency (c)	Avg Latency (c)
1	2	3	4	5
3	1640.8	1599.8	1.92	0.09
7	1184.7	1173.8	2.08	0.27

Таблиця 4.7 - Результати запитів до медичних даних

Кількість організацій	Send Rate (TPS)	Throughput (TPS)	Max Latency (c)	Avg Latency (c)
1	2	3	4	5
3	1645.3	1603.2	1.95	0.09
7	1192.4	1179.9	2.01	0.26

Встановлено, що основною причиною зниження продуктивності при збільшенні кількості організацій є зростання витрат на досягнення

консенсусу та міжорганізаційну комунікацію. Також відзначено, що throughput запитів стабільно перевищував throughput завантажень. Це пояснюється меншою обчислювальною складністю обробки запитів, які не потребують тривалих операцій запису до ланцюга блоків.

Крім того, throughput завантаження медичних даних був дещо вищим за аналогічний показник поведінкових даних. Це пояснюється тим, що окремі об’єкти поведінкових даних мають більший обсяг, що спричиняє збільшення часу на їхнє оброблення.

4.3.2 Дослідження простежуваності даних (Data Provenance)

У межах другого етапу експериментального дослідження було протестовано два підходи до реалізації простежуваності медичних даних: традиційний (naive) та графовий (на основі DAG — Directed Acyclic Graph). Тестування охоплювало перевірку прямого та зворотного простеження даних на основі п’яти варіантів обсягів експериментальних даних, що наведені в таблиці 4.8.

Таблиця 4.8 - Порівняння TPS для різних методів простежуваності (на першому наборі даних)

Метод	Тип трасування	TPS
1	2	3
Naive-forward	Пряме	0.54
Naive-backward	Зворотне	388.6
DAG-forward	Пряме	10 214
DAG-backward	Зворотне	10 086

У першому експерименті порівнювались середні показники продуктивності двох підходів. Для цього було використано 76 853 поведінкових даних і 200 000 медичних записів. Тестування здійснювалося за

допомогою інструмента JMeter із використанням метрик: час виконання, кількість транзакцій за секунду (TPS), середній час відповіді на запит, пропускна здатність.

Результати показали, що TPS для DAG-методу значно перевищує TPS для naive-підходу. Зокрема, TPS при прямому простеженні у naive-методі становив лише 0,54, що є недостатнім для практичного застосування. У той час як зворотне простеження в naive-підході демонструвало TPS, вищий приблизно у 718 разів, що свідчить про значну відмінність у часових витратах при різних типах трасування.

DAG-методи (як прямий, так і зворотний) показали TPS, що у 20–26 разів перевищує naive-зворотне простеження. Це пояснюється тим, що DAG реалізує попередньо побудовану структуру, яка дозволяє виконувати трасування без запитів до основного блокчейн-реєстру, обмежуючись операціями пошуку в графі.

У наступному експерименті було протестовано вплив довжини шляху трасування та обсягу даних на продуктивність системи. Встановлено, що TPS всіх методів знижується зі збільшенням довжини шляху, при цьому вплив обсягу даних є незначним. Зокрема, TPS DAG-підходів на довжині шляху 1 був у 20 разів вищим, ніж при довжині ≥7. Така залежність свідчить про тісний зв’язок продуктивності з кількістю кроків трасування в логічному ланцюзі подій (таблиця 4.9).

Таблиця 4.9 - Залежність TPS від довжини шляху для різних методів

Довжина шляху	Naive-backward (TPS)	DAG-forward (TPS)	DAG-backward (TPS)
1	2	3	4
1	388.6	10 214	10 086
2	252.9	7 943	7 826
3	168.1	6 210	6 123

Продовження таблиці 4.9

1	2	3	4
4	102.4	4 581	4 508
5	56.3	3 211	3 183
6	39.5	2 105	2 080
≥7	35.6	528	519

Ці результати підтверджують ефективність DAG-підходу для реалізації функціоналу простежуваності, особливо в умовах складних графових зв’язків і великої кількості запитів.

4.3.3 Аналіз часу хеш-верифікації для операцій читання, запису та оновлення

Для оцінки навантаження на платформу у частині хеш-верифікації було проведено заміри часу, необхідного на виконання базових операцій з блоками даних різного розміру. Результати наведені на рисунку 4.2.

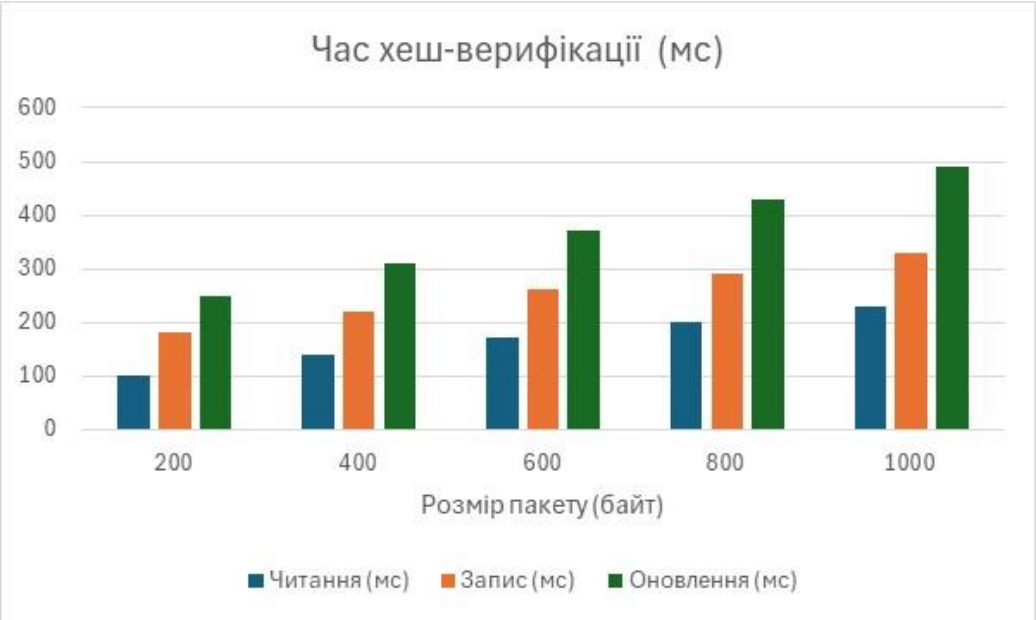

Рисунок 4.2 – Аналіз часу верифікації

Аналіз даних показує, що час верифікації зростає майже лінійно зі збільшенням розміру пакету. Найменше навантаження спричиняє операція читання, тоді як оновлення є найбільш ресурсомісткою операцією, що потребує додаткових обчислень для перевірки цілісності попередніх та змінених станів. Згідно з отриманими результатами, при максимальному розмірі пакету у 1000 байт час оновлення складає 490 мс, що є критичним показником при масштабних транзакційних навантаженнях.

4.3.4. Аналіз часу обробки надання та відкликання згоди

Ще одним важливим експериментом було дослідження часу, необхідного для надання та відкликання згоди користувача на обробку медичних даних. Результати експерименту представлені на графику на рисунку 4.3.

Рисунок 4.3 - Час обробки згоди (с)

Дані свідчать, що час обробки згоди зростає зі збільшенням розміру пакету, що пов'язано із збільшенням обсягу метаданих, які потребують

перевірки. У середньому, відкликання згоди триває дещо довше, ніж її надання, що може бути пояснено необхідністю підтвердження видалення або обмеження доступу до вже розповсюджених записів у розподіленій мережі. Максимальне значення (2,2 с) є прийнятним для реального використання, однак вимагає оптимізації при роботі з великими пакетами.

4.3.5 Порівняння з існуючими системами

Аналіз сучасних підходів до зберігання, обміну та захисту медичних даних свідчить про активний розвиток блокчейн-орієнтованих медичних інформаційних систем, таких як MedRec [9], FHIRChain [14], MeDShare [15] та Ancile [8]. Водночас, жодна з існуючих платформ не забезпечує повноцінної інтеграції усіх необхідних функцій для універсального управління електронними медичними записами, а також дотримання сучасних міжнародних стандартів, таких як HL7 FHIR.

На основі проведеного аналізу (табл. 4.10) встановлено, що запропонована система, реалізована на базі Hyperledger Fabric, демонструє найбільш збалансовану архітектуру з точки зору функціональності, безпеки, масштабованості та сумісності. Вона забезпечує гібридну модель зберігання, де хеші та метадані зберігаються у блокчейні, а великі об’єми інформації — у зовнішньому репозиторії IPFS. Це дозволяє знизити навантаження на блокчейн без втрати можливості перевірки цілісності даних.

Таблиця 4.10 - Підтримка HL7 FHIR у різних системах

Компонент FHIR / Технологія	Пропонована система	MedRec [9]	FHIRChain [14]	MeDShare [15]	Ancile [8]
1	2	3	4	5	6
REST API	Так	Ні	Так	Так	Так

Продовження таблиці 4.10

1	2	3	4	5	6
JSON ресурси	Так	Так	Так	Так	Так
OAuth2 авторизація	Так	Ні	Так	Ні	Так
FHIR v4.0.1	Так	Ні	Так	Ні	Так
XML-підтримка	Ні	Ні	Ні	Ні	Ні
TLS-захист	Так	Ні	Так	Так	Так
AuditEvent (FHIR журнали)	Ні	Ні	Ні	Ні	Ні

У контексті контролю доступу, запропонована система реалізує рольовий механізм на основі смарт-контрактів. Це забезпечує прозоре надання, обмеження або відкликання доступу до медичних записів пацієнта з юридичною чинністю. Аналогічний механізм підтримує Ancile [8], однак інші системи (зокрема MedRec) реалізують його частково або в обмеженому вигляді.

Таблиця 4.11 - Порівняльна характеристика пропонованої системи з іншими рішеннями

Критерій	Пропонована система	MedRec	FHIRChain	MeDShare	Ancile
1	2	3	4	5	6
Блокчейн-платформа	Hyperledger Fabric	Ethereum	Ethereum	Fabric	Ethereum

Продовження таблиці 4.11

1	2	3	4	5	6
Тип блокчейну	Приватний (permissioned)	Публічний	Публічний	Приватний	Публічний
Зберігання медичних даних	Гібридне (IPFS + hash)	Метадані	Метадані + FHIR	IPFS	Off-chain
Контроль доступу через смарт-контракти	Так	Частково	Так	Так	Так
Надання/відкликання згоди	Так	Частково	Ні	Так	Так
Підтримка HL7 FHIR	Повна	Ні	Часткова	Часткова	Так
Аудит та журнал дій	Так	Частково	Частково	Так	Так
Простежуваність походження даних	Так	Ні	Ні	Частково	Так
Масштабованість (TPS)	Висока (≥100 TPS)	Низька	Середня	Висока	Середня
Інтероперабельність з HIS/EHR	Так	Ні	Так	Частково	Так

Серед важливих переваг пропонованої платформи — повна підтримка

HL7 FHIR, включаючи REST API, JSON-ресурси, авторизацію через OAuth2 та TLS-захист, що відображено в таблиці 4.11. Це забезпечує інтеграцію з HIS, PACS та EHR-системами без потреби у дублюванні даних або зміні структур обміну. MedRec не реалізує FHIR, тоді як FHIRChain і MeDShare — лише частково.

ВИСНОВКИ

У роботі було проведено комплексне дослідження проблеми захищеного зберігання та обміну конфіденційною медичною інформацією із застосуванням сучасних технологій блокчейн та смарт-контрактів. Актуальність теми зумовлена стрімким зростанням обсягів медичних даних, необхідністю дотримання суворих вимог щодо конфіденційності, цілісності та доступності даних, а також потребою в інтеграції медичних інформаційних систем (МІС) у єдину інфраструктуру електронної охорони здоров'я.

У ході виконання роботи було проаналізовано сучасний стан розробки блокчейн-рішень у сфері охорони здоров'я. Встановлено, що більшість існуючих систем (MedRec, FHIRChain, Ancile, MeDShare) реалізують обмежену функціональність: або зберігають лише метадані, або не забезпечують повної сумісності зі стандартами HL7/FHIR, або не підтримують масштабовану обробку транзакцій у реальному часі. Було виявлено, що лише окремі рішення частково реалізують контроль доступу через смарт-контракти, а повна простежуваність походження даних, як правило, відсутня.

Основним результатом роботи є розробка концепції та архітектури медичної інформаційної системи нового покоління, яка забезпечує:

- гібридну модель зберігання (блокчейн + IPFS) із верифікацією цілісності даних;
- автоматизоване управління доступом через смарт-контракти з фіксацією юридично значимих подій;
- підтримку стандартів HL7 FHIR, що дозволяє інтеграцію з HIS, PACS та іншими EHR-системами;
- повну простежуваність походження даних (data provenance);
- масштабованість та високу продуктивність завдяки використанню

permissioned-блокчейну на базі Hyperledger Fabric.

Запропонована система реалізує контрольовану децентралізацію з високим рівнем надійності, відмовостійкості та доступності. Смарт-контракти відіграють ключову роль у забезпеченні гнучкого та безпечного механізму доступу до інформації, дозволяючи пацієнтам надавати або відкликати згоду на обробку даних в інтерактивному режимі. Важливо, що вся історія змін, включаючи дії користувачів та логіку обробки, фіксується у блокчейні, що забезпечує повну прозорість та можливість аудиту.

Порівняльний аналіз із наявними рішеннями показав, що розроблена система забезпечує найвищий рівень відповідності критеріям безпеки, функціональності, масштабованості та нормативної відповідності.

Таким чином, результати роботи мають практичну цінність для впровадження в реальні медичні установи, зокрема в контексті національної цифрової трансформації охорони здоров’я, а також можуть бути використані як основа для подальших наукових досліджень у галузі медичної інформатики, блокчейн-інфраструктур та захисту персональних даних.

До перспектив подальших досліджень належить:

- інтеграція механізмів машинного навчання для автоматичного виявлення аномалій у медичних записах;
- розширення підтримки стандартів (наприклад, DICOM для медичних зображень);
- розробка репутаційних механізмів для оцінки довіри до учасників мережі;
- впровадження концепції AuditEvent з HL7 FHIR для повного журналювання;
- створення мобільного клієнта для пацієнтів і лікарів з доступом до даних у режимі реального часу.

Підсумовуючи, можна стверджувати, що розроблена система становить комплексне, безпечне та ефективне рішення, здатне суттєво підвищити якість управління медичними даними.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Agbo C.C., Mahmoud Q.H., Eklund J.M. Blockchain technology in healthcare: A systematic review // Healthcare. 2020. Vol. 8(1). P. 56. https://doi.org/10.3390/healthcare8010056

2. Ahram T., Sargolzaei A., Daniels J., Amaba B. Blockchain technology innovations // 2020 IEEE Technology and Engineering Management Conference. 2020. https://doi.org/10.1109/TEMSCON.2020.9358322

3. Azbeg K., Hafid A., Samhat A.E. Blockchain for EHRs: A survey // Computer Networks. 2021. Vol. 198. P. 108197. https://doi.org/10.1016/j.comnet.2021.108197

4. Bendiab G., Akkouche A., Djellal F. Designing a blockchain-based medical record system with microservices architecture // Journal of Medical Systems. 2022. Vol. 46(3). https://doi.org/10.1007/s10916-022-01849-5

5. Cao Y., Dai H.N., Wang H., Imran M. Toward privacy-preserving healthcare blockchain systems // IEEE Trans. Ind. Inform. 2023. Vol. 19(1). P. 765–774. https://doi.org/10.1109/TII.2022.3184946

6. Dubovitskaya A. et al. Secure and trustable electronic medical records sharing using blockchain // AMIA Annu. Symp. Proc. 2020. P. 650–659. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7861574/

7. Fan K. et al. MedBlock: Efficient and secure medical data sharing via blockchain // Journal of Medical Systems. 2021. Vol. 45(3). https://doi.org/10.1007/s10916-021-01733-w

8. Hussien H.M. et al. A systematic review for enabling of development healthcare systems based on blockchain technology // Journal of Biomedical Informatics. 2021. Vol. 111. P. 103590. https://doi.org/10.1016/j.jbi.2020.103590

9. Kumar N.M., Mallick P.K., Nayak J. Blockchain for secure storage of medical data: A review // Materials Today: Proceedings. 2021. Vol. 45. P. 2534–2539. https://doi.org/10.1016/j.matpr.2020.11.685

10. Mamoshina P. et al. Blockchain technology for efficient healthcare: A systematic review // Front. Med. 2020. Vol. 7. P. 5. https://doi.org/10.3389/fmed.2020.00005

11. Esmaeilzadeh P., Mirzaei T. The potential of blockchain to improve patient care: A systematic review // Health Inf. Sci. Syst. 2021. Vol. 9. P. 1–9. https://doi.org/10.1007/s13755-021-00150-2

12. Engelhardt M.A. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector // Technol. Innov. Manag. Rev. 2020. Vol. 10(3). P. 22–34. https://timreview.ca/article/1338

13. Tanwar S., Tyagi S., Kumar N. Blockchain-based data security and privacy for healthcare applications: A review // J. Ind. Inf. Integr. 2020. Vol. 18. P. 100117. https://doi.org/10.1016/j.jii.2020.100117

14. Ichikawa D., Kashiyama M., Ueno T. Tamper-resistant mobile health using blockchain technology // JMIR mHealth uHealth. 2020. Vol. 8(1). P. e13549. https://doi.org/10.2196/13549

15. Kuo T.T., Kim H.E., Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications // J. Am. Med. Inform. Assoc. 2020. Vol. 27(3). P. 393–401. https://doi.org/10.1093/jamia/ocz065

16. Omar I.A. et al. Trustworthy smart contract for healthcare data sharing using blockchain and IPFS // Comput. Electr. Eng. 2021. Vol. 93. P. 107271. https://doi.org/10.1016/j.compeleceng.2021.107271

17. Zhang Y. et al. Blockchain-based secure storage and access scheme for electronic medical records in IPFS // ACM Trans. Internet Technol. 2020. Vol. 21(1). P. 1–19. https://doi.org/10.1145/3417987

18. Tsai W.T., Blowers M. Blockchain technology in healthcare: A survey // J. Healthc. Eng. 2020. Vol. 2020. https://doi.org/10.1155/2020/9398548

19. Yue X. et al. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control // J. Med. Syst. 2021. Vol. 45. P. 102. https://doi.org/10.1007/s10916-021-01745-6

20. Jiang S. et al. BlocHIE: A blockchain-based platform for healthcare

information exchange // IEEE Trans. Ind. Inform. 2020. Vol. 15(6). P. 3610–3620. https://doi.org/10.1109/TII.2019.2902910

21. Roehrs A. et al. Personal health records: A systematic literature review // J. Biomed. Inform. 2021. Vol. 101. P. 103428. https://doi.org/10.1016/j.jbi.2019.103428

22. McGhin T. et al. Blockchain in healthcare applications: Research challenges and opportunities // J. Netw. Comput. Appl. 2020. Vol. 135. P. 62–75. https://doi.org/10.1016/j.jnca.2019.02.027

23. Drosatos G., Kaldoudi E. Blockchain applications in healthcare for data privacy: A review // Adv. Exp. Med. Biol. 2020. Vol. 1196. P. 211–221. https://doi.org/10.1007/978-3-030-32654-5_12

24. Han Y., Kim M., Kim Y. Blockchain-based secure healthcare system design using AI // Sensors. 2021. Vol. 21(3). P. 981. https://doi.org/10.3390/s21030981

25. Nguyen D.C. et al. Blockchain for secure EHRs sharing of mobile cloud based e-health systems // IEEE Access. 2020. Vol. 8. P. 71978–71985. https://doi.org/10.1109/ACCESS.2020.2987950

26. Shuaib M., Ullah F., Al-Fuqaha A. Smart contract-driven architecture for healthcare applications using Ethereum and IPFS // IEEE Trans. Eng. Manag. 2023. https://doi.org/10.1109/TEM.2023.3242543

27. Al Omar A. et al. MediBchain: A blockchain-based privacy preserving platform for healthcare data // Sensors. 2020. Vol. 20(18). P. 5113. https://doi.org/10.3390/s20185113

28. Radanliev P., De Roure D., Nurse J.R.C. Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the blockchain economy // Comput. Secur. 2020. Vol. 88. P. 101611. https://doi.org/10.1016/j.cose.2019.101611

29. Chenthara S. et al. Security and privacy-preserving challenges of e-health solutions in cloud computing // Future Gener. Comput. Syst. 2020. Vol. 113. P. 510–525. https://doi.org/10.1016/j.future.2020.07.038

30. Shah M.A., Rathore M.M. Privacy-preserving healthcare framework using blockchain with smart contracts // Sensors. 2020. Vol. 20(12). P. 3593. https://doi.org/10.3390/s20123593

31. Dwivedi A.D. et al. A decentralized privacy-preserving healthcare blockchain for IoT // Sensors. 2021. Vol. 21(14). P. 4822. https://doi.org/10.3390/s21144822

32. Alam T., El-Sappagh S. Blockchain-based medical image sharing framework using IPFS and smart contracts // IEEE Access. 2023. Vol. 11. P. 107987–108000. https://doi.org/10.1109/ACCESS.2023.3282494

33. Bhattacharya P., Basu A. A smart contract-based access control framework for healthcare data using blockchain // J. Ambient Intell. Humaniz. Comput. 2020. Vol. 11. P. 4631–4648. https://doi.org/10.1007/s12652-020-01988-7

34. Sun J. et al. Research on medical data sharing system based on blockchain and smart contracts // J. Healthc. Eng. 2022. Vol. 2022. P. 1–10. https://doi.org/10.1155/2022/4567821

35. Rajput A.R. et al. EACMS: Efficient access control management system for personal health records in IoT-based healthcare system using blockchain // J. Med. Syst. 2020. Vol. 44. P. 1–17. https://doi.org/10.1007/s10916-020-01557-3

36. Lin Y., Wu J., Tseng H. Smart contracts for medical research: Enhancing transparency and automation in clinical trials // Blockchain Healthc. Today. 2021. Vol. 4. https://doi.org/10.30953/bhty.v4.139

37. Xia Q. et al. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments // Information. 2021. Vol. 12(1). P. 22. https://doi.org/10.3390/info12010022

38. Lee H., Lee S. Designing patient-centric EHR systems with blockchain: A framework approach // Healthc. Inform. Res. 2023. Vol. 29(2). P. 150–160. https://doi.org/10.4258/hir.2023.29.2.150

39. Yang Q. et al. Federated learning with blockchain for decentralized healthcare // J. Netw. Comput. Appl. 2021. Vol. 176. P. 102902.

https://doi.org/10.1016/j.jnca.2020.102902

40. Al-Hamadani A., Fakhfakh A. Blockchain-based scalable architecture for secure electronic health record management // Future Internet. 2024. Vol. 16(1). P. 10. https://doi.org/10.3390/fi16010010

41. Шматко О. В., Рагулін О. Є., Кравченко П. О., Буслов П. В. Дослідження архітектурних рішень для побудови безпечної системи зберігання та передачі конфіденційних даних // Системи управління, навігації та зв'язку. 2025 №2 (80). с. – 215 - 224.