ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Застосування технології blockchain для забезпечення безпеки при цифровій ідентифікації пацієнтів у системах охорони здоров'я»

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ _____
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав:
здобувачка вищої освіти Олена СТОЛЯР
група ІСДМ-63

Керівник: Андрій БОНДАРЧУК
науковий ступінь, вчене звання д.т.н., професор

Рецензент:
науковий ступінь, вчене звання _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційних систем та технології

Ступінь вищої освіти Магістр

Спеціальність Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ

_____ Каміла СТОРЧАК
«_____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Столяр Олена Валентинівна _____
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Застосування технології blockchain для забезпечення безпеки при цифровій ідентифікації пацієнтів у системах охорони здоров'я

керівник кваліфікаційної роботи Андрій БОНДАРЧУК, д.т.н., професор,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» 10.2024р. №320

2. Строк подання кваліфікаційної роботи «27» грудня 2024р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, параметри технології blockchain , вимоги до систем цифрової ідентифікації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Проблеми захисту даних при цифровій ідентифікації пацієнтів у системах охорони здоров'я
Основи технології blockchain та її роль у забезпеченні безпеки даних
Застосування блокчейну для забезпечення безпеки цифрової ідентифікації пацієнтів у медицині.

5. Перелік графічного матеріалу: *презентація*

1. Різниця між централізованою системою та blockchain.
2. Зміст кожного блоку в прикладному блокчейні.
3. Процес хешування технології Blockchain.
4. Порівняння різних типів блокчейнів.
5. Приклад загальної структури розподіленого реєстру.
6. Централізована і децентралізована система.
7. DNS-IdM Architecture , uPort Architecture , Health-ID Architecture.
8. ShoCard Architecture.
9. Ключові характеристики та особливості кількох провідних систем.
10. System Architecture MedRec.
11. Приклад оркестрації системи: постачальник додає запис для нового пацієнта.
12. Структура системи Gravitate-Health.

6. Дата видачі завдання «15» жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	10.10-05.11.24	
2	Вивчення матеріалів для аналізу потреб у захисті даних у медичних системах	05.11-12.11.24	
3	Дослідження основних загроз та вразливості цифрової ідентифікації в охороні здоров'я	13.11-19.11.24	
4	Дослідження основ технології blockchain	20.11-25.11.24	
5	Огляд міжнародного досвіду застосування блокчейну	27.11-03.12.24	
6	Визначення перспектив розвитку та можливі виклики впровадження blockchain в українській медицині	04.12-10.12.24	
7	Оформлення роботи: вступ, висновки, реферат	11.12-20.12.24	
8	Розробка демонстраційних матеріалів	21.12-29.12.24	

Здобувач вищої освіти _____ Олена СТОЛЯР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Андрій БОНДАРЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 69 стор., 2 табл., 13 рис., 43 джерел.

Мета дослідження: Розробка та обґрунтування підходу до застосування blockchain-технологій для забезпечення безпеки, прозорості та ефективності цифрової ідентифікації пацієнтів у системах охорони здоров'я.

Об'єкт дослідження: Система обміну персональними даними пацієнтів у сфері охорони здоров'я.

Предмет дослідження: Програмні рішення на основі blockchain-технологій, що забезпечують конфіденційність, прозорість та захист медичної інформації в процесі цифрової ідентифікації пацієнтів.

Короткий зміст роботи: У дослідженні розглянуто проблематику захисту медичних даних та цифрової ідентифікації пацієнтів в умовах сучасних викликів кібербезпеки. Проаналізовано можливості впровадження blockchain-рішень для підвищення рівня безпеки персональної медичної інформації. Запропоновано модель інтеграції blockchain-технологій у системи охорони здоров'я, що дозволяє підвищити ефективність автентифікації пацієнтів та мінімізувати ризики витоку даних.

КЛЮЧОВІ СЛОВА: BLOCKCHAIN, ІДЕНТИФІКАЦІЇ, ДЕЦЕНТРАЛІЗАЦІЯ, КОНСЕНСУС, АРХІТЕКТУРА, СМАРТ-КОНТРАКТИ, MEDREC, GUARDTIME, E-HEALTH.

ABSTRACT

Text part of the master's qualification work: 69 pages, 13 pictures, 2 table, 43 sources.

The purpose of the work: Development and justification of an approach to applying blockchain technologies to ensure security, transparency, and efficiency in the digital identification of patients within healthcare systems.

Object of research : The system for exchanging patients' personal data in the healthcare sector.

Subject of research : Blockchain-based software solutions that ensure confidentiality, transparency, and protection of medical information during the digital identification of patients.

Summary of the work: The study addresses the issues of medical data protection and digital patient identification amidst modern cybersecurity challenges. The possibilities of implementing blockchain solutions to enhance the security of personal medical information are analyzed. A model for integrating blockchain technologies into healthcare systems is proposed, which improves the efficiency of patient authentication and minimizes the risk of data breaches.

KEYWORDS: BLOCKCHAIN, IDENTIFICATION, DECENTRALIZATION, CONSENSUS, ARCHITECTURE, SMART CONTRACTS, MEDREC, GUARDTIME, E-HEALTH.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

ПОДАННЯ

ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра (магістра)

Направляється здобувач(ка) _____ до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю _____
(код, найменування спеціальності)

освітньо-професійної програми _____
(назва)

на тему: «_____».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач(ка) _____
_____
_____
_____

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача(ки) _____ на оцінку «_____» та присвоїти йому(їй) кваліфікацію _____.

Керівник кваліфікаційної роботи _____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач(ка) *прізвище та ініціали* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою _____ _____ _____
(назва) *(підпис)* *(Ім'я, ПРІЗВ*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

на здобуття освітнього ступеня бакалавра (магістра)

здобувача(ки) вищої освіти _____
(прізвище, ім'я, по батькові)

на тему «_____»

Актуальність.

Позитивні сторони.
1.
2.
3.

Недоліки.
1.
2.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи бакалаврської (магістерської).

Висновок: *кваліфікаційна робота на здобуття ступеня бакалавра (магістра) заслуговує оцінку "_____", а здобувач(ка) _____ заслуговує присвоєння кваліфікації: ……..*

Рецензент: _____ _____
підпис *Ім'я, ПРІЗВИЩЕ*
науковий ступінь, вчене звання

ЗМІСТ

РОЗДІЛ 1 ПРОБЛЕМИ ЗАХИСТУ ДАНИХ ПРИ ЦИФРОВІЙ ІДЕНТИФІКАЦІЇ ПАЦІЄНТІВ У СИСТЕМАХ ОХОРОНИ ЗДОРОВ'Я

1.1 Аналіз потреб у захисті даних у медичних системах

Захист інформації в медичних системах є одним із ключових пріоритетів сучасної охорони здоров'я, адже в цій сфері накопичуються великі обсяги чутливих даних про пацієнтів. Особисті та конфіденційні медичні записи потребують особливого рівня захисту, оскільки їхній витік або несанкціонована модифікація можуть завдати значної шкоди як пацієнтам, так і медичним установам. У зв'язку зі зростанням цифровізації та посиленням кіберзагроз виникає нагальна потреба у впровадженні новітніх технологічних рішень, спрямованих на забезпечення надійної безпеки медичних даних.

Медичні дані є одними з найбільш чутливих типів інформації, адже вони містять детальну інформацію про стан здоров'я пацієнтів, діагнози, результати аналізів, історію лікування, а також персональні дані, такі як адреса проживання чи фінансова інформація [1]. У сучасному світі, де дедалі більше медичних закладів переходять до електронних систем управління даними, забезпечення їхнього захисту стає критично важливим завданням. Недостатній рівень безпеки цих даних може призвести до серйозних наслідків, зокрема витоку приватної інформації, фінансових втрат чи навіть загрози життю пацієнтів.

Однак сучасні медичні системи стикаються з багатьма викликами у сфері захисту даних. Постійне зростання обсягів інформації через впровадження електронних медичних записів (EMR), телемедичних платформ та носимих пристроїв (IoT) створює значний тиск на системи захисту [4].

Традиційні методи захисту, такі як централізоване зберігання даних, використання паролів чи обмеження доступу, мають значні обмеження. Вони є вразливими до внутрішніх і зовнішніх загроз через можливість зламів, помилок чи навмисного зловживання доступом. Централізована модель зберігання також створює ризик «єдиної точки відмови» – якщо центральний сервер буде зламаний чи пошкоджений, дані можуть бути втрачені або скомпрометовані [18].

У зв’язку з цим виникає потреба у нових підходах до забезпечення захисту даних у медичних системах. Технологія blockchain пропонує децентралізовану архітектуру з використанням криптографії, яка забезпечує високий рівень безпеки та прозорості. Завдяки своїй структурі блокчейн дозволяє зменшити ризики витоку даних, забезпечити надійний доступ до інформації лише авторизованим користувачам та гарантувати цілісність записів. Такий підхід є перспективним для вирішення сучасних викликів у сфері захисту медичних даних.

1.2 Сучасні методи ідентифікації та їхні обмеження

Сучасні медичні системи застосовують різноманітні способи ідентифікації для забезпечення безпеки даних пацієнтів і контролю доступу до них. Основна задача цих методів полягає у визначенні особи користувача та гарантуванні, що тільки авторизовані особи можуть мати доступ до конфіденційної інформації.

Актуальні підходи до ідентифікації часто базуються на використанні кількох факторів. Найбільш поширеними є двофакторна та трифакторна ідентифікація. Наприклад, під час двофакторної ідентифікації користувач підтверджує свою особу за допомогою знання пароля (password) та наявності персонального ідентифікатора (login). У ролі ідентифікатора можуть виступати апаратні токени, смарт-карти чи інші пристрої [21].

Апаратні токени для ідентифікації користувачів можуть бути автономними або такими, що підключаються, або USB-токенами. Автономні токени – це мобільні персональні пристрої, що не під’єднуються до комп'ютера і мають власне джерело живлення. Вони дозволяють користувачеві ідентифікувати себе на серверах, використовуючи або одноразовий пароль (токени з використанням ОТР – англ. OneTime Password), або метод запит–відповідь. Суть методу запит–відповідь полягає в наступному:

– користувач вводить свій ідентифікатор на робочій станції, яка передає його по мережі сервера;

– сервер аутентифікації генерує випадковий запит, який по мережі передається користувачеві;

– користувач вводить запит в ідентифікаційний токен;

– токен користувача за допомогою якогось алгоритму і секретного ключа користувача зашифровує цей запит і результат відображає на своєму екрані;

– користувач вводить результат на робочій станції, яка повертає його серверу; – сервер зашифровує те саме випадкове число (запит);

– при збігу результатів процес запит/відповідь в існуючій системі аутентифікації успішно завершується [21].

USB-токени являють собою пристрої, що підключаються до USB-портів і виконують двофакторну аутентифікацію. Вони також забезпечують функції шифрування даних та створення електронного цифрового підпису. На відміну від ОТР-токенів, USB-токени зазвичай не потребують додаткового серверного програмного забезпечення [27].

Смарт-карти є ще одним популярним інструментом ідентифікації. Ці карти містять вбудовані мікропроцесори для криптографічних операцій (електронний підпис, шифрування) та пам’ять для зберігання даних користувача. Для їх використання потрібен спеціальний зчитувач [27].

Інші методи, наприклад, використання штрих-кодів або пристроїв iButton, також знаходять своє застосування у медичних інформаційних системах. Штрих-коди можуть бути нанесені на медичні картки пацієнтів і слугувати унікальним ідентифікатором, тоді як iButton пристрої, завдяки своїй міцності та унікальному ID, застосовуються у більш складних умовах [24].

Біометричні системи ідентифікації включають такі методи, як розпізнавання за відбитком пальця, геометрією обличчя, сітківкою чи райдужною оболонкою ока, а також за голосом. Зокрема, ідентифікація за відбитком пальця є однією з найбільш перспективних технологій завдяки простоті використання, швидкості та надійності [14].

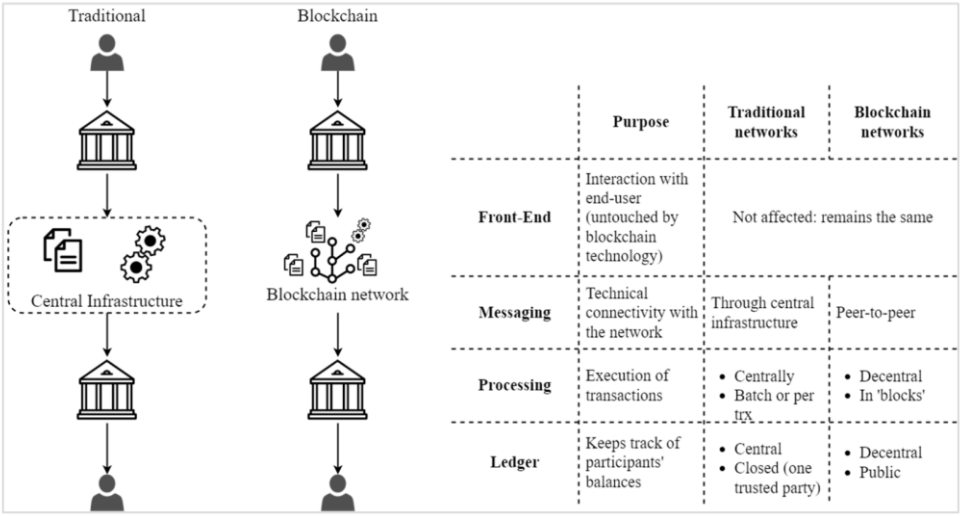
Ідентифікація за рисами обличчя (за геометрією обличчя) – один з напрямків у біометричній індустрії, що розвиваються найбільш активно. На сьогодні існує дві таких біометричних технології. В основі першої лежить спеціальне програмне забезпечення, яке отримує зображення зі звичайної веб-камери та обробляє його. На обличчі виділяються окремі об'єкти (брови, очі, ніс, губи), для кожного з яких обчислюються параметри, які повністю його визначають. При цьому багато сучасних систем будують тривимірний образ обличчя людини. Це потрібно для того, щоб уможливити ідентифікацію, наприклад, при нахилі і повороті голови, зміні виразу обличчя або макіяжі у жінок. Інша технологія заснована на ідентифікації людини за її обличчям із використанням термограми. Фотографія користувача, зроблена за допомогою спеціальної інфрачервоної камери, дозволяє отримати "карту" розташування артерій, яка у кожної людини різна. Навіть у однояйцевих близнюків артерії розташовані по-різному. Завдяки цьому надійність методу досить висока. Проте цей метод з'явився недавно і поки не набув широкого використання [14].

Незважаючи на широкий спектр сучасних методів ідентифікації, що активно впроваджуються в медичні системи для забезпечення безпеки та конфіденційності даних, їх використання має низку недоліків, які обмежують їхню ефективність та надійність. Ці обмеження впливають на функціональність систем, створюючи ризики

для безпеки й інтеграції даних. Розглянемо основні проблеми, пов’язані з сучасними методами ідентифікації.

Обмеження сучасних методів ідентифікації :

1) Централізована модель зберігання даних**:** Більшість сучасних систем ідентифікації покладаються на централізовані сервери, що створює вразливість до збоїв чи атак. У разі виходу з ладу або злому центрального сервера вся система стає недоступною або скомпрометованою (Рис 1.1)



	Purpose	Traditional networks	Blockchain networks
Front-End	Interaction with end-user (untouched by blockchain technology)	Not affected: remains the same	
Messaging	Technical connectivity with the network	Through central infrastructure	Peer-to-peer
Processing	Execution of transactions	• Centrally • Batch or per tx	• Decentral • In 'blocks'
Ledger	Keeps track of participants' balances	• Central • Closed (one trusted party)	• Decentral • Public

Рис 1.1 Різниця між централізованою системою та blockchain [39]

2) Недостатній рівень прозорості**:** Існуючі системи часто не дозволяють користувачам отримати повну інформацію про те, як обробляються їхні дані, хто має до них доступ і з якою метою. Це підриває довіру до системи ідентифікації.
3) Високий ризик компрометації даних**:** Паролі, фізичні токени й навіть біометричні дані можуть бути викрадені або зламані через недостатню захищеність інфраструктури. Це загрожує витоком конфіденційної інформації, особливо в умовах зростання кількості кібератак.
4) Невідповідність стандартів і регламентів**:** У медичній сфері відсутність універсальних стандартів для процесів аутентифікації ускладнює інтеграцію

між різними інформаційними системами, що негативно впливає на ефективність обміну даними.

5) Обмежена масштабованість**:** Багато сучасних рішень не здатні адаптуватися до зростаючого обсягу даних і кількості користувачів без значного ускладнення або підвищення витрат на інфраструктуру.
6) Залежність від стороннього програмного забезпечення**:** Більшість систем ідентифікації базуються на використанні стороннього ПЗ або обладнання, що може спричинити конфлікти сумісності, збільшення витрат та залежність від постачальників [5].

Технологія блокчейн може запропонувати вирішення багатьох із цих проблем. Завдяки децентралізованій природі та використанню смарт-контрактів, блокчейн дозволяє створювати прозорі, надійні й безпечні системи ідентифікації, які мінімізують ризики витоку даних, забезпечують довіру користувачів та легко інтегруються у глобальні медичні екосистеми. Це підкреслює необхідність упровадження інноваційних рішень, які б долали обмеження традиційних методів ідентифікації та сприяли ефективнішому захисту даних пацієнтів у медичних системах.

1.3 Основні загрози та вразливості цифрової ідентифікації в охороні здоров'я

Інтегровані медичні системи, що забезпечують збереження та обробку великих обсягів даних, висувають високі вимоги до безпеки та конфіденційності. Особливістю таких систем є необхідність підтримувати баланс між захистом приватності даних пацієнтів і їх використанням для статистичних, аналітичних і дослідницьких цілей. Хоча використання даних без прив’язки до особи мінімізує ризик для конкретного пацієнта, такі дані можуть містити важливу інформацію, яка представляє інтерес для

медичних і державних установ. Зокрема, обробка великих обсягів даних сприяє створенню точних прогнозів, розробці нових методик, тестуванню ліків, медичного обладнання та підвищенню кваліфікації медичних працівників. Однак відкритість даних створює нові виклики у сфері безпеки, які вимагають особливої уваги [7].

Медичні інформаційні системи повинні відповідати трьом ключовим вимогам: функціональність, інформаційна безпека та сумісність. Ці аспекти стають критично важливими в умовах зростаючих загроз, таких як несанкціонований доступ до даних, помилки в програмному забезпеченні, збої обладнання та людський фактор. Забезпечення балансу між цими вимогами вимагає комплексного підходу. Хоча на ранніх етапах розробки інформаційних систем акцент робився на функціональності, сьогодні безпека стала невід'ємною складовою ефективного функціонування таких систем [8].

Цифрова ідентифікація в медичних закладах значно спрощує доступ до інформації про пацієнтів, підвищує ефективність обслуговування та дозволяє зберігати великі обсяги медичних даних. Водночас вона створює нові ризики для конфіденційності, цілісності та доступності інформації [13].

Серед основних загроз можна виділити:

- збої обладнання, що призводять до втрати даних;
- помилки в роботі програмного забезпечення;
- несанкціонований доступ до баз даних;
- неналежне зберігання архівів;
- людський фактор, зокрема необережність персоналу [11].

Для забезпечення безпеки застосовуються фізичні та програмні заходи. Фізична безпека включає впровадження систем архівації та резервного копіювання даних, обмеження доступу до серверних кімнат і робочих станцій, використання відеоспостереження та ідентифікаційних карток. Програмні засоби включають антивірусні програми, системи розмежування прав доступу та контроль доступу [10].

Сучасні проблеми у сфері захисту медичних даних включають:

- невідповідність законодавства сучасним викликам інформатизації;
- недостатнє використання ліцензованих програмних рішень;
- збереження надмірного обсягу персональних даних у єдиній базі;
- відсутність контролю за діяльністю приватних операторів медичних інформаційних систем;
- низький рівень комп'ютерної грамотності серед медичних працівників;
- недотримання технічних стандартів захисту інформації [9].

У контексті вирішення цих проблем перспективною технологією є блокчейн. Вона дозволяє створювати децентралізовані бази даних із високим рівнем захисту, де кожен запис є незмінним і прозорим. Це забезпечує захист від несанкціонованих змін даних та сприяє підвищенню довіри до медичних систем. Правильна організація захисту даних допомагає уникнути витоків інформації та забезпечити високий рівень конфіденційності. Інтеграція сучасних технологій і дотримання стандартів безпеки є ключовими чинниками для підвищення ефективності та довіри до медичних інформаційних систем.

1.4 Нормативно-правові аспекти захисту даних

У сучасному світі, де цифрові технології швидко інтегруються в усі сфери життя, забезпечення захисту даних, особливо в медичному секторі, є ключовим завданням. Чутливість медичної інформації, яка включає персональні дані пацієнтів, діагнози, результати лікування та інші конфіденційні відомості [6], створює високі вимоги до їх збереження. Порушення конфіденційності або втрати медичних даних можуть мати серйозні наслідки, включаючи юридичну відповідальність, підрив довіри до медичних установ та ризик для життя пацієнтів. Тому нормативно-правове регулювання захисту даних є не лише актуальним, а й необхідним компонентом цифрової трансформації охорони здоров'я [13].

Основні нормативно-правові акти захисту даних у світі:

1. GDPR (General Data Protection Regulation) – Загальний регламент про захист даних Європейського Союзу:
    - Прийнятий у 2018 році, регламент встановлює суворі вимоги щодо збору, зберігання та обробки персональних даних.
    - Вимоги включають право користувачів на доступ до своїх даних, можливість їх видалення та інформованість про використання даних.
    - Штрафи за порушення досягають мільйонів євро, що стимулює компанії дотримуватись правил [20].
2. HIPAA (Health Insurance Portability and Accountability Act) – Закон США про захист конфіденційності медичних даних:
    - Встановлює стандарти для захисту електронних медичних записів і регламентує, як медичні установи можуть використовувати і передавати дані.
    - Передбачає жорсткі покарання за порушення конфіденційності [23].
3. Data Protection Act (DPA) у Великобританії:
    - Регулює захист персональних даних відповідно до GDPR.
    - Особливу увагу приділяє захисту даних у медичних установах та у сфері цифрових послуг [26].
4. Закони про кібербезпеку в Китаї:
    - Китай приділяє увагу як захисту конфіденційних даних, так і забезпеченню державного контролю.
    - Нові закони зобов'язують компанії зберігати дані на місцевих серверах і повідомляти про кіберзагрози [26].

В Україні захист персональних даних регулюється низкою законів та нормативних актів:

1. Закон України "Про захист персональних даних" (№ 2297-VI) [1]:

- Закон визначає правові відносини щодо захисту персональних даних і спрямований на захист права громадян на конфіденційність.
- Включає положення щодо обробки персональних даних із використанням автоматизованих засобів та на паперових носіях.

2. Закон України "Про інформацію" [2]:
   - Регламентує доступ, поширення та захист інформації в Україні.
   - Містить положення про конфіденційну інформацію, включаючи персональні дані.
3. Закон України "Про електронні довірчі послуги" [3]:
   - Регламентує питання електронного документообігу, забезпечуючи автентичність та захист електронних даних.
4. Проекти імплементації європейських стандартів (GDPR):
   - Уряд працює над гармонізацією українського законодавства з нормами ЄС у межах угоди про асоціацію.

Перспективи нормативно-правового регулювання захисту даних в Україні мають стратегічне значення, оскільки охоплюють як гармонізацію з міжнародними стандартами, так і впровадження сучасних технологій для забезпечення конфіденційності, цілісності та доступності інформації. У найближчі роки очікується суттєве вдосконалення законодавчої бази, спрямоване на вирішення таких ключових завдань:

1. Гармонізація із законодавством ЄС

Україна прагне адаптувати своє законодавство до стандартів GDPR, що дозволить ефективно інтегруватися у європейський цифровий простір, підвищити захист прав громадян на конфіденційність та спростити взаємодію з міжнародними партнерами.

2. Розвиток спеціалізованих нормативних актів у сфері охорони здоров’я [7].

Зважаючи на особливу чутливість медичних даних, передбачається ухвалення додаткових законів та підзаконних актів, які регулюватимуть їхню обробку, передачу та збереження в межах медичних інформаційних систем [5].

3. Впровадження блокчейн-технологій

Застосування блокчейну у регулюванні обігу даних відкриє нові можливості для підвищення прозорості та безпеки, адже ця технологія гарантує незмінність і автентичність даних, а також дозволяє створювати централізовані електронні реєстри [8].

4. Розробка нових стандартів кібербезпеки

Зростання кількості кіберзагроз вимагає запровадження сучасних протоколів захисту інформації та створення національних стандартів, які забезпечать ефективне попередження витоку, модифікації чи втрати даних [9].

5. Створення системи моніторингу та аудиту захисту даних

Формування регуляторних органів або посилення функцій вже існуючих структур дозволить проводити регулярний контроль за дотриманням законодавчих вимог у сфері захисту даних [8].

6. Навчання та підвищення кваліфікації кадрів

Державна підтримка програм підготовки фахівців із кібербезпеки та захисту даних сприятиме підвищенню професійного рівня та готовності реагувати на нові виклики.

У перспективі, нормативно-правове регулювання захисту даних в Україні стане більш прозорим, узгодженим із міжнародними стандартами та адаптованим до сучасних технологій, що дозволить створити надійну основу для цифрової трансформації та розвитку цифрової економіки.

Україна поступово інтегрує міжнародні стандарти захисту даних у своє законодавство. Імплементація сучасних технологій, таких як блокчейн, разом із законодавчими змінами створить міцну базу для захисту персональної інформації. Це не лише підвищить довіру громадян до цифрових послуг, але й сприятиме інтеграції України у світовий цифровий простір.

РОЗДІЛ 2 ОСНОВИ ТЕХНОЛОГІЇ BLOCKCHAIN ТА ЇЇ РОЛЬ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ДАНИХ

2.1 Основи технології blockchain: принципи роботи та ключові поняття

Ідея застосування блокчейн-технології в охороні здоров'я виникає з необхідності забезпечення безпеки та сумісності медичних даних. З розвитком Інтернету речей (IoT), численних медичних пристроїв і мобільних додатків, щодня фіксується й передається велика кількість медичних даних [26]. Це потребує ефективного управління, особливо в контексті забезпечення конфіденційності та безпеки. Блокчейн-технологія може стати вирішенням, яке забезпечить захищене зберігання та обмін медичними записами, а також гарантуватиме конфіденційність даних пацієнтів, надаючи їм право власності на свої медичні дані.

Технологія Blockchain є розподіленим реєстром, який дозволяє записувати транзакції у безпечний, прозорий і децентралізований спосіб з мінімальними витратами [31]. Блокчейн лежить в основі біткоїна — цифрової валюти, що була представлена під псевдонімом Сатоші Накамото в 2008 році. Для розуміння принципів роботи блокчейн-технології важливо ознайомитись з механізмом біткоїна, який функціонує за принципом "рівний до рівного" (peer-to-peer) і має розподілену та децентралізовану структуру. У біткоїн-системі відсутній третій посередник, і кожен учасник, що володіє біткоїном, може брати участь у мережі, читати, записувати та зберігати копії реєстрів транзакцій [26].

Учасники мережі діляться на дві групи: звичайні користувачі, які створюють транзакції з даними, і майнери, які видобувають блоки для наступного їх запису в

blockchain. Справа в тому, що створення блоку – це дуже ресурсомісткий і складний процес, ось тому далеко не всі можуть і хочуть цим займатися [26].

Дві основні проблеми системи без центрального контролю: (1) єдина точка відмови та (2) можливість подвійного витрачання. Блокчейн вирішує ці проблеми за допомогою двох основних механізмів: хеш-ланцюгового тимчасового штампу та алгоритму доказу роботи. Щоб перевірити кожну транзакцію, її необхідно зберігати в кожному вузлі мережі, а також забезпечити тимчасовий штамп для визначення її дійсності [16].

Блоки в мережі біткоїн створюються майнерами, які з'єднують нові блоки з попередніми. На Рис. 2.1 показано, як створюються блоки і як вони з'єднуються в ланцюг. Кожен блок складається з двох основних частин:

1. Зміст (Content**)**: перевірений список транзакцій, де цифрові активи можуть бути будь-якими даними, такими як біткоїн, ефіріум або медичні записи.
2. Заголовок (Header)**:** містить метадані, зокрема:
    - (a) Номер посилання на зміст блоку (Hash Root),
    - (b) Час створення блоку (Timestamp),
    - (c) Посилання на попередній блок (Prev.Hash),
    - (d) Випадкове число (nonce), яке додається до блоку відповідно до алгоритму доказу роботи [16].

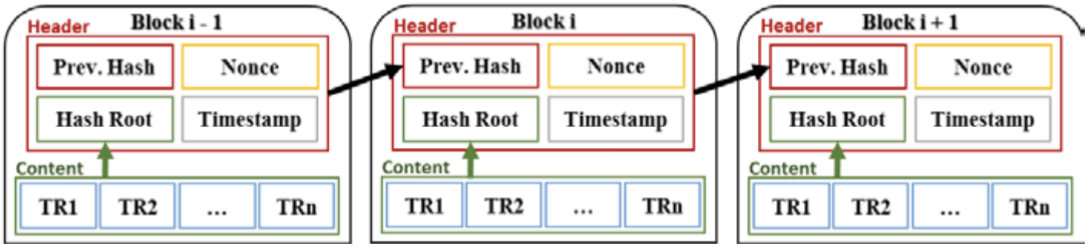


Рис 2.1 Зміст кожного блоку в прикладному блокчейні [16]

У біткоїн-блокчейні майнери використовують протокол доказу роботи для пошуку нової адреси для блоку. Вони виконують алгоритм, намагаючись знайти 32-

бітне криптографічне число, що починається з 17 нульових бітів. Коли майнер знаходить таке число, він оновлює реєстр і відправляє новий блок до всієї мережі для підтвердження. Цей процес підтвердження транзакцій називається консенсусом або доказом роботи. Завдяки складності майнінгу створення недійсних транзакцій є малоймовірним, а майнер отримує винагороду за свої зусилля [16].

Протокол доказу роботи забезпечує незмінність аудиторського сліду блокчейну. Кожен блок містить хеш попереднього, тому зміна одного блоку вимагатиме змін у всіх наступних, що потребує великих обчислювальних ресурсів (Рис 2.2) . Це робить біткоїн-блокчейн захищеним від зловмисних змін [30].

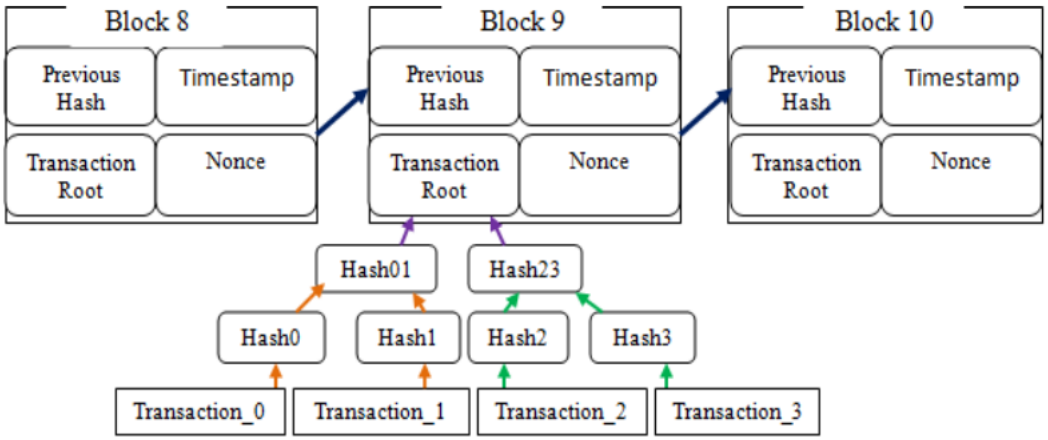


Рис.2.2 Процес хешування технології Blockchain [30]

До ключових властивостей blockchain -технології відносять :

- Децентралізація**:** відсутність єдиного контролюючого органу, що дозволяє знижувати витрати та зменшувати навантаження на сервери.
- Сталість**:** збереження транзакцій у розподілених блоках, що забезпечує узгодженість і відновлення даних у разі втрати.
- Анонімність**:** ідентичність користувачів прихована, а транзакції проводяться через згенеровані адреси.

- Прозорість та аудитованість**:** всі транзакції є доступними для перевірки, що знижує можливість шахрайства.
- Зниження часу: автоматизація та відсутність необхідності в тривалих процесах перевірки дозволяє скоротити час транзакцій [23].

Існують різні типи технологій блокчейну, такі як публічний, приватний, гібридний або консорціумний. Кожен із цих типів має свої переваги та недоліки, що впливають на оптимальні сфери їх застосування.

Публічний блокчейн – це перший тип блокчейн-технології, на основі якого були створені біткоїн та інші криптовалюти. Він сприяв популяризації технології розподіленого реєстру (DLT). Ця технологія усуває недоліки централізації, такі як брак безпеки та прозорості, розподіляючи дані в P2P-мережі замість зберігання їх у одному місці. Однак через децентралізований характер публічного блокчейну потрібен механізм для аутентифікації даних [15].

Приватний блокчейн – це мережа блокчейну, яка працює у закритому середовищі, наприклад у межах організації, або контролюється одним суб'єктом. Хоча за принципом роботи приватний блокчейн схожий на публічний у контексті P2P-зв’язків та децентралізації, він значно менший за масштабами. У приватному блокчейні його розробник з самого початку знає, хто є учасниками мережі. При цьому неможливо створити рішення з дозволами (permission-based) на публічній платформі, а користувачі залишаються повністю анонімними [19].

Гібридний блокчейн поєднує характеристики як публічного, так і приватного блокчейнів. Цей тип використовується організаціями, які хочуть отримати переваги обох технологій. Гібридний блокчейн дозволяє створити приватну систему з обмеженим доступом поряд із публічною, відкритою системою. Це забезпечує контроль над тим, хто має доступ до певних даних у блокчейні, та визначає, які саме дані будуть доступні публічно [28].

У табл. 2.1 порівнюються різні типи blockchain.

Таблиця 2.1

Порівняння різних типів блокчейнів

Тип блокчейну	Децентралізація	Пропускна здатність	Витрати	Маштабованість
Публічний блокчейн	Повна. Відсутність єдиного контролюючого органу.	Обмежена	Високі	Обмежена
Приватний блокчейн	Центральний контроль або контроль обмеженою кількістю учасників.	Висока	Низькі витрати на підтримку	Легша масштабованість завдяки централізованому контролю і меншим вимогам до обчислювальних ресурсів.
Гібридний блокчейн	Комбінація централізованих і децентралізованих елементів.	Помірна пропускна здатність	Витрати знижуються в порівнянні з публічними блокчейнами	Масштабованість гнучка: можна обробляти високі обсяги даних у певних частинах системи, зберігаючи ефективність.

Джерело: [33]

У всіх блокчейн-мережах дані зберігаються на вузлах, які належать користувачам цієї мережі. Усі учасники мають однакові права та обов'язки, що дозволяє їм виконувати будь-які дії, включаючи спроби обману інших або зміну блоків у ланцюгу. Оскільки всі знаходяться в рівних умовах, ніхто не може заборонити користувачам виконувати ці дії. В цьому контексті немає потреби в посередниках, таких як банки, державні органи, аудитори чи страхові компанії, оскільки в блокчейн-системі відсутні структури, що мають додаткові повноваження або авторитет. Усі користувачі мають рівні можливості і зобов'язання, що дозволяє уникнути необхідності звертатися за дозволом до будь-яких сторонніх організацій або установ [33].

Технологія блокчейн забезпечує захищену та децентралізовану архітектуру завдяки механізмам консенсусу (Рис. 2.3)., які є основою надійності мережі. У

контексті цифрової ідентифікації пацієнтів у системах охорони здоров’я, консенсусні алгоритми відіграють ключову роль у перевірці даних, запобіганні шахрайству та підтримці цілісності інформації в розподіленій мережі.

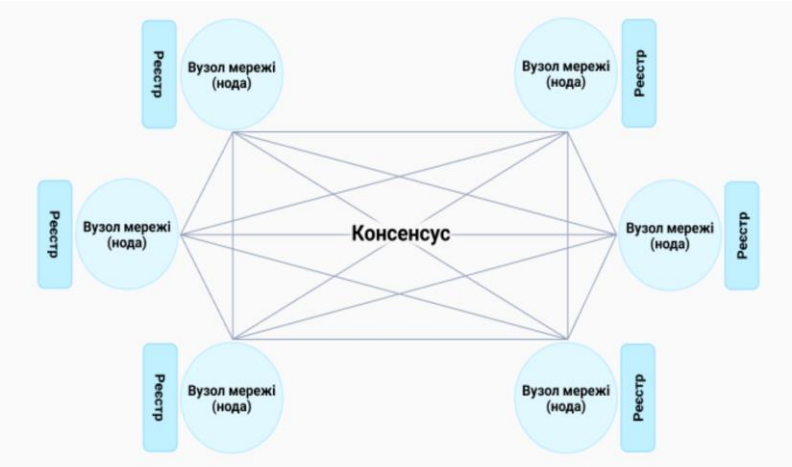


Рис. 2.3 Приклад загальної структури розподіленого реєстру [12].

Різні алгоритми консенсусу використовуються для задоволення специфічних потреб, залежно від вимог до безпеки, швидкості обробки транзакцій або витрат енергії. Наприклад:

- Proof of Work (PoW): використовується для захисту мережі від Sybil-атак за рахунок значних обчислювальних ресурсів. Однак через високі енергетичні витрати PoW не є оптимальним для застосування у сфері охорони здоров’я, де важливими є швидкість і енергоефективність.
- Proof of Stake (PoS): забезпечує вищу енергоефективність, оскільки для перевірки блоків використовується частка власності вузлів у мережі. Це підвищує довіру до учасників мережі, але може створити залежність від "багатих" учасників, що не завжди бажано у медичних системах.
- Practical Byzantine Fault Tolerance (PBFT): ідеально підходить для систем охорони здоров’я завдяки здатності ефективно працювати в середовищах із низькою затримкою та високими вимогами до безпеки. Алгоритм вимагає

узгодження 2/3 вузлів для додавання блоку, що забезпечує високу довіру до даних.

- Proof of Authority (PoA): забезпечує швидку обробку транзакцій та підходить для приватних блокчейн-систем, де учасники (наприклад, лікарі або клініки) заздалегідь ідентифіковані [30].

У системах охорони здоров'я особливу увагу слід приділяти безпеці даних пацієнтів. Алгоритми консенсусу, такі як PBFT і PoA, дозволяють реалізувати цифрову ідентифікацію пацієнтів із мінімальними затримками, одночасно зберігаючи конфіденційність інформації. Наприклад, децентралізована ідентифікація пацієнтів може включати створення смарт-контрактів, які генерують унікальний цифровий ідентифікатор пацієнта (HealthID), прив'язаний до зашифрованих даних про пацієнта, що зберігаються у захищеному хмарному середовищі [30].

Крім того, використання консенсусних алгоритмів дозволяє запобігти шахрайству та забезпечити довіру між учасниками системи охорони здоров'я: пацієнтами, лікарями та регуляторами. Відсутність центрального вузла знижує ризик компрометації даних, а застосування методів, таких як Practical Byzantine Fault Tolerance, мінімізує вразливість до зловмисних дій у мережі [30]. Таким чином, консенсусні алгоритми забезпечують надійність, масштабованість і безпеку у блокчейн-мережах, що робить їх ключовим інструментом для реалізації цифрової ідентифікації пацієнтів у сучасних системах охорони здоров'я.

Смарт-контракти є важливою складовою багатьох blockchain -систем. Вони є програмами, які автоматично виконують умови угод, безпосередньо вбудовані в blockchain. Для їх написання та виконання використовуються мови програмування, такі як Solidity (для Ethereum), Chaincode (для Hyperledger Fabric) та множина інших. Вибір конкретної мови програмування залежить від вибраного blockchain - протоколу та його особливостей [35].

Гарантування безпеки та конфіденційності в інформаційних системах є критично важливою задачею. Blockchain -технології використовують сучасні методи

шифрування та криптографії для захисту транзакцій та даних у блокчейні. Криптографія з відкритим ключем (Public-key cryptography), хеш-функції та електронний підпис – це лише деякі приклади технік, що застосовуються для гарантування безпеки. Враховуючи ці ключові аспекти, розгляд способів реалізації blockchain - технологій відкриває широкий спектр можливостей для створення надійних, безпечних та ефективних інформаційних систем.

Таким чином, Блокчейн-технологія має значний потенціал для вдосконалення системи охорони здоров’я. Її властивості – незмінність, децентралізація та криптографічна безпека – дозволяють мінімізувати ризики маніпуляцій із даними, забезпечити прозорість та конфіденційність, а також підвищити довіру до медичних систем. У поєднанні з алгоритмами консенсусу та смарт-контрактами, блокчейн може стати ключовим інструментом у цифровій трансформації охорони здоров'я.

2.2 Архітектура цифрової ідентифікації на основі блокчейну

Технологія blockchain пропонує рішення для децентралізованого управління даними та усуває необхідність довірених третіх сторін для забезпечення узгодженості інформації. Завдяки цьому блокчейн має потенціал радикально змінити цифрове суспільство, створюючи платформи без посередників, які раніше були неможливими. Від початку існування Інтернету постійно виникали виклики, пов’язані з керуванням ідентифікацією, що стосуються конфіденційності, безпеки та зручності. Зростання щоденного використання різноманітних онлайн-сервісів вимагає впровадження ефективного підходу до управління цифровою ідентифікацією (DIM). Використання блокчейн-реєстрів дає змогу зберігати й надавати доступ до певних доказів або фрагментів даних, які необхідні для перевірки атрибутів і облікових даних цифрової ідентифікації [32].

Цифрова ідентичність є актуальною концепцією в цифровому світі. Цифрова ідентичність — це набір перевірених ідентифікаторів, цифрових атрибутів і облікових даних для цифрового світу, подібних до ідентичності людини в реальному світі [34].

Керування ідентифікацією – це видача, підтримка та відкликання цифрових ідентифікаторів і облікових даних у програмах, системах і мережах. Система управління ідентифікацією – це набір технологій і процесів, які можна використовувати для управління ідентифікацією [34].

Спочатку Інтернет не був розроблений із врахуванням потреб в ідентифікації та управлінні цифровими обліковими даними. Ці функції почали формуватися лише після того, як Інтернет еволюціонував у платформу для фінансових операцій, електронної комерції, телемедицини та інших послуг у цифровій сфері. Традиційні підходи до ідентифікації, які зазвичай базуються на концепції «закритого саду», створюють чимало викликів, пов’язаних із конфіденційністю, безпекою та відсутністю сумісності між системами [33].

Найбільш поширеним методом управління користувачами в онлайн-сервісах залишається модель, що використовує централізований локальний реєстр. У цій моделі користувач реєструється безпосередньо на платформі, а постачальник послуг створює унікальний ідентифікатор і облікові дані для цього користувача. Авторизація зазвичай відбувається через пару «ім'я користувача/пароль», яка слугує основною формою ідентифікації. Такий підхід має низку недоліків: користувачі змушені запам’ятовувати велику кількість паролів для різних сервісів, що ускладнює управління ними. Як наслідок, багато хто використовує одні й ті самі паролі для декількох платформ, що значно підвищує ризики компрометації даних. У разі витоку пароля з одного облікового запису це може поставити під загрозу безпеку всіх інших акаунтів користувача [29].

Однією з найважливіших переваг блокчейну є можливість усунення необхідності в централізованих посередниках у розподілених системах. Це дає змогу сторонам здійснювати транзакції в децентралізованому середовищі без участі

центрального органу, що усуває проблему залежності від однієї точки відмови, характерної для централізованих систем. Крім того, це прискорює процес проведення операцій, оскільки усуваються затримки, пов'язані з роботою центрального органу, і зменшує витрати за рахунок відсутності комісій, які зазвичай стягує такий орган [32].

Замість централізованого управління в блокчейні використовуються механізми консенсусу, які забезпечують узгодженість даних між вузлами в розподіленій системі. Порівняння централізованих і децентралізованих систем наведено на Рис 2.4. На рисунку 1a показано кілька облікових книг, які зберігаються в центральному місці, наприклад, у Регіональній організації охорони здоров’я (RHIO). У цьому випадку RHIO відповідає за збереження даних і виступає як арбітр для вирішення суперечок щодо "актуального стану" облікової книги [27].

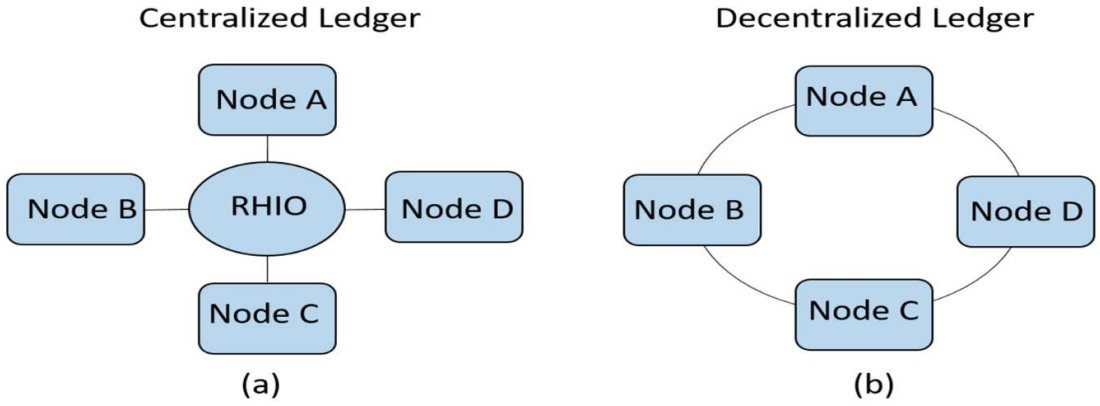


Рис. 2.4 Централізована і децентралізована система [27]

У децентралізованій системі (рисунок 1b) існує лише одна облікова книга, але всі вузли мережі мають її копію та певний рівень доступу до інформації. Для збереження цілісності даних вузли повинні досягати згоди щодо "актуального стану" облікової книги без втручання центрального органу [27].

Застосування цифрової ідентифікації до переважної більшості онлайн-сервісів сприяє підвищенню рівня довіри до систем управління ідентифікацією (IDMS). Ці системи відповідають за створення, перевірку та управління цифровими

ідентифікаторами, які дозволяють забезпечити користувачам доступ до різних платформ. Однак нинішня архітектура таких систем має свої недоліки, оскільки цифрові ідентифікатори найчастіше зберігаються в централізованих сховищах. Управління такими сховищами здійснюється однією організацією, що робить їх об'єктами підвищеної уваги для кіберзлочинців. Подібні системи можуть стати вразливими через наявність слабких місць у безпеці, що, у свою чергу, спричиняє витоки даних, крадіжку персональної інформації та порушення конфіденційності [28].

Окрім технічних загроз, централізована модель управління ідентифікацією створює ризики, пов'язані з неправильним використанням даних користувачів. Організації, які мають доступ до зібраної інформації, можуть використовувати її без відома або згоди власників. Ці виклики потребують впровадження нових підходів, які б надали користувачам більше контролю над їхніми ідентифікаційними даними [25].

Одним із таких підходів є концепція Самовизначеної Ідентичності (Self-Sovereign Identity, SSI)**,** що дає змогу користувачам самостійно управляти своєю ідентичністю. SSI дозволяє користувачам вирішувати, які дані передавати, кому і коли, надаючи повну автономію у питаннях цифрової ідентифікації. Основою для реалізації SSI є технологія блокчейн, яка відкриває можливість децентралізованого зберігання ідентифікаторів та усуває необхідність в залученні центрального посередника [33].

У межах цього дослідження розглядаються традиційні підходи до управління ідентифікацією (IdM), а також перспективи їх модернізації завдяки технології блокчейн. Сучасні децентралізовані системи, побудовані на блокчейні, орієнтовані на користувача, усувають роль посередників і забезпечують більший захист даних. Нижче наведено приклади таких рішень:

1. **Self-Sovereign Identity (SSI)**

Цей підхід надає користувачам повне право власності та контроль над своїми цифровими ідентифікаторами без залучення централізованих постачальників ідентифікації. У рамках SSI користувачі можуть самостійно вирішувати, якими

даними ділитися, з ким і в яких обставинах. Така модель сприяє конфіденційності та довіреним взаємодіям між сторонами.

uPort є яскравим прикладом реалізації SSI (Рис 2.5). Це децентралізована система ідентифікації з відкритим вихідним кодом, що базується на блокчейні Ethereum. uPort використовує низку компонентів, зокрема смарт-контракти, бібліотеки для розробників і мобільний додаток. Смарт-контракти відповідають за обробку транзакцій, а мобільний додаток дозволяє керувати ключами криптографії. Крім того, система використовує проксі смарт-контракти, які забезпечують унікальну ідентифікацію користувача [33].

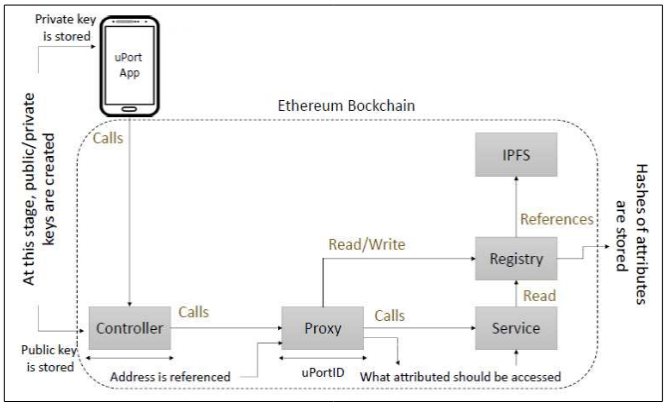


Рис 2.5 uPort Architecture [33]

Унікальність uPort полягає у використанні чотирьох основних типів смарт-контрактів:

- Проксі-контракт для пересилання транзакцій.
- Контролер-контракт, що визначає доступ до проксі-контракту.
- Контракт відновлення, який дозволяє відновлювати ідентифікацію через голосування делегатів.
- Контракт реєстрації, що відповідає за мапування атрибутів ідентифікації [33].

2. DNS-IdM

Система DNS-IdM реалізована на базі Ethereum і підтримує концепцію SSI (Рис 2.6) . Вона дозволяє користувачам реєструвати свої атрибути, які зберігаються у вигляді хешів на блокчейні. Система забезпечує процес верифікації атрибутів через смарт-контракти та дозволяє зберігати зашифровані дані на IPFS (InterPlanetary File

System). Смарт-контракт DNS виконує роль маршрутизатора для обробки верифікаційних запитів [33].

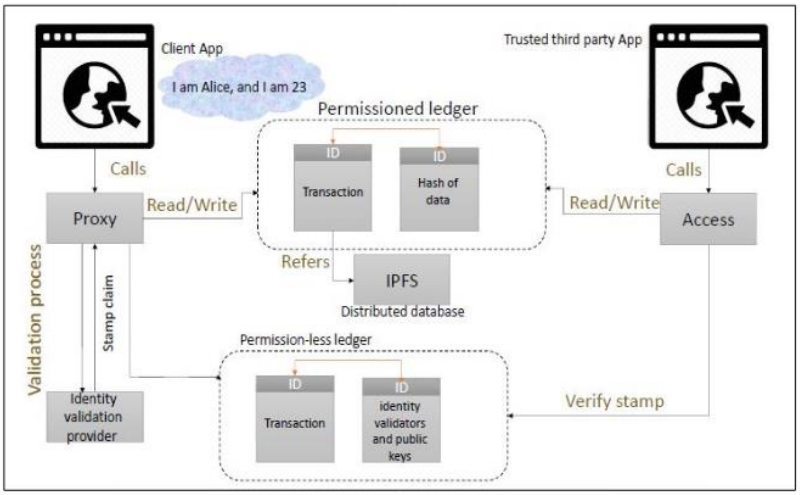


Рис 2.6 DNS-IdM Architecture [33]

3. Health-ID

Система Health-ID спеціалізується на децентралізованому управлінні ідентифікацією в галузі охорони здоров'я (Рис 2.7) . Її учасниками є пацієнти, медичні працівники та регулятори. Пацієнти отримують можливість створювати унікальні ідентифікатори, звані healthID, які зберігаються у смарт-контрактах. Медичні атрибути структуруються у форматі JSON, підписуються регуляторами та зберігаються у хмарному середовищі з додатковим хешуванням у блокчейні [33].

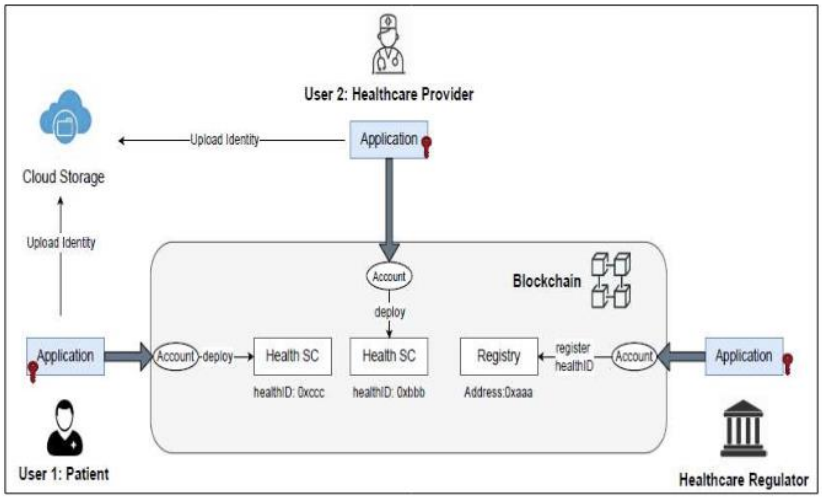


Рис 2.7 Health-ID Architecture [33]

4. Decentralized Trusted Identity (DTI)

DTI базується на довірених облікових даних, таких як паспорти або державні ID-картки. Прикладом є система **ShoCard** (Рис 2.8), яка використовує блокчейн для зв'язування ідентифікаторів користувачів із атрибутами та довіреними обліковими даними. ShoCard забезпечує перевірку ідентичності як для онлайн-сервісів, так і для офлайн-зустрічей [33].

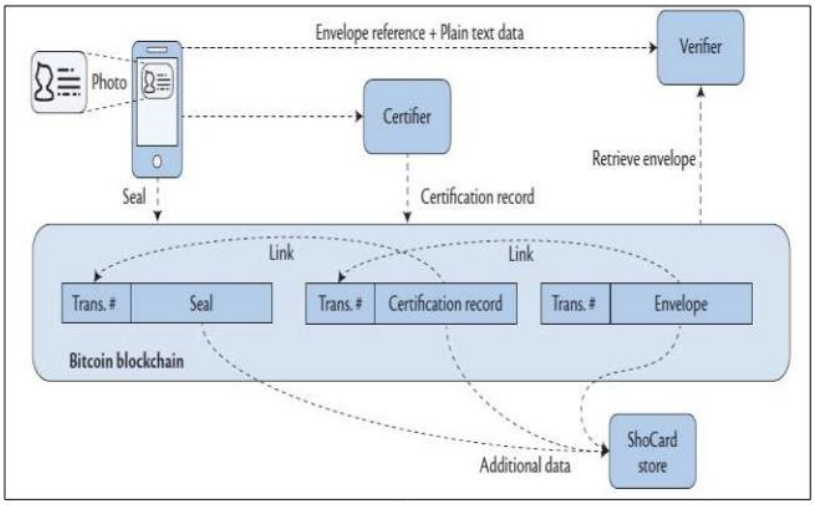


Рис 2.8 ShoCard Architecture [33]

Для більш детального порівняння різних рішень у сфері децентралізованого управління ідентифікацією (IdM), представлено таблицю 2.2, що узагальнює ключові характеристики та особливості кількох провідних систем, побудованих на основі блокчейн-технологій. Таблиця надає порівняння таких аспектів, як підхід до управління ідентифікацією, використання смарт-контрактів, рівень децентралізації, а також підходи до зберігання та верифікації даних. Ця інформація дозволяє краще зрозуміти переваги та обмеження різних технологій, що дозволяють користувачам управляти своєю цифровою ідентичністю та забезпечують високий рівень безпеки та конфіденційності [33].

Таблиця 2.2

Ключові характеристики та особливості кількох провідних систем

Ідентифікаційна система	*Підхід до децентралізації*	*Використання смарт-контрактів*	*Зберігання даних*	*Підтримка верифікації*
uPort	Повна децентралізація	Так	Ethereum, IPFS	Зовнішні перевірки, децентралізовані атрибути
DNS-IdM	Часткова децентралізація	Так	IPFS, permissioned Blockchain	Використання верифікаційних смарт-контрактів
Health-ID	Часткова децентралізація	Так	IPFS, Blockchain	Верифікація через регуляторів та медичних постачальників
ShoCard	Часткова децентралізація	Так	Blockchain	Верифікація з урядовими картками та іншими довіреними обліковими даними

Джерело : [33]

Загалом, блокчейн-технології відкривають нові можливості для децентралізованого управління ідентифікацією, що забезпечує підвищену безпеку даних та усуває необхідність у посередниках. Однак, незважаючи на їхні переваги, ці технології стикаються з рядом викликів, зокрема з питаннями масштабованості, правової невизначеності та складності впровадження. У цьому контексті новітні підходи, такі як SSI, DNS-IdM та Health-ID, демонструють потенціал для створення безпечних та автономних систем управління ідентифікацією нового покоління в охороні здоров'я.

Огляд цих інноваційних рішень дає можливість оцінити, як різні підходи до керування ідентифікацією, зокрема з використанням blockchain-технологій, можуть вирішувати сучасні проблеми безпеки та конфіденційності медичних даних. У цьому розділі буде розглянуто кілька ключових пропозицій для медичних систем, які реалізують блокчейн для ефективного керування ідентифікацією та зберігання даних. Усі обрані системи забезпечують технічну документацію, звіти та концептуальні підтвердження, що дає можливість детально оцінити їх реалізацію в реальному середовищі та вплив на надійність і конфіденційність медичних даних.

Одним із прикладів є Medilinker, який використовує Hyperledger Indy для керування ідентифікацією. Ця система інтегрує цифрові гаманці, що надають пацієнтам повний контроль над їхніми особистими даними через використання приватних ключів. Головною перевагою є те, що особисті дані не зберігаються в самому блокчейні, а передаються лише згодом, при необхідності, за допомогою цифрового підпису. Це дозволяє зберігати високий рівень конфіденційності, підтримуючи автономію користувачів та контроль над їхніми даними [20].

Інший приклад — система, що використовує Hyperledger Fabric для автентифікації та авторизації в системі EHR (електронні медичні записи). Концепція була реалізована через використання блокчейн-реєстру, що дозволяє обробляти дані від усіх лікарів у Данії, з можливістю масштабування до 100 000 транзакцій на секунду. Це демонструє, як блокчейн може бути використаний для обробки великих обсягів медичних даних при високій швидкості та надійності [38].

У роботі Sharm et al. запропоновано використання міжпланетної файлової системи та смарт-контрактів для зберігання та контролю доступу до EHR в контексті Національної схеми охорони здоров'я Індії. Вони використовують механізм доказів з нульовим знанням (ZKP), що дозволяє здійснювати автентифікацію без розкриття особистих даних. Це підвищує конфіденційність і сумісність системи, дозволяючи зберігати медичні дані пацієнтів у суворій відповідності до вимог безпеки [38].

Рішення Health-ID, представлено Javed et al., що працює на основі блокчейну Ethereum. Система вимагає від пацієнтів підтвердження особи через документи, такі як паспорт або водійське посвідчення, а постачальникам медичних послуг — перевірки через ліцензію. Система підтримує використання як централізованих, так і децентралізованих методів зберігання атрибутів посвідчення, що дозволяє пацієнтам і медичним працівникам зберігати контроль над їхніми даними [19].

Інші проекти, як Sovrin і MediBloc, зосереджуються на створенні стандартів для децентралізованої ідентифікації через використання блокчейну. Sovrin використовує попарно-псевдонімні DID і підтримує технології, як ZKP, що дозволяють забезпечити

конфіденційність і вибіркове розкриття даних. Ці проекти також активно застосовують стандарти W3C для забезпечення сумісності та інтеграції з іншими системами [18].

Зокрема, платформа MediBloc застосовує механізм дерева Merkle для зберігання медичних даних, що дозволяє здійснювати вибіркове розкриття даних з гарантією їхньої цілісності. Проект використовує блокчейн «Панацея», оптимізований для медичних даних, і дозволяє пацієнтам мати контроль над своїми медичними записами, що зберігаються у їхніх власних цифрових гаманцях [17].

Таким чином, ці приклади демонструють, як різні блокчейн-рішення можуть застосовуватися для забезпечення безпеки і конфіденційності в медичних системах, а також підкреслюють важливість використання сучасних технологій для забезпечення контролю за даними пацієнтів в умовах децентралізованих мереж.

2.3 Смарт-контракти та їх роль у цифровій ідентифікації

Концепція смарт-контрактів була вперше запропонована Ніком Сабо в 1994 році, ще до того, як існувала технологія блокчейн. Вона визначає правила та санкції щодо угоди так само, як і традиційний контракт, але також автоматично забезпечує виконання цих зобов'язань. Смарт-контракт — це фрагмент коду та даних, який розгортається на блокчейні; перший смарт-контракт разом з блокчейном був розгорнутий на Ethereum у 2015 році [29].

Смарт-контракти створюються для спрощення, автентифікації та забезпечення виконання угоди. Вони працюють за принципом логіки «if–then» [36], де задаються попередньо визначені умови, і коли ці умови виконуються, контракт автоматично виконує узгоджені завдання. Ці контракти усувають необхідність у посередниках, таких як юристи чи нотаріуси, оскільки вони забезпечують прозорість, безпеку та ефективність виконання контрактних зобов'язань [35].

Смарт-контракти відіграють важливу роль у забезпеченні безпеки, прозорості та ефективності процесів цифрової ідентифікації. Вони дозволяють автоматизувати перевірку особистості та обробку даних без потреби в посередниках, таких як адвокати або нотаріуси. Використання технології блокчейн забезпечує незмінність і безпеку записів, що є надзвичайно важливим для таких чутливих сфер, як охорона здоров'я, фінанси, урядові послуги та інші [39].

У контексті цифрової ідентифікації смарт-контракти автоматизують процеси верифікації особистих даних та забезпечують їх безпеку за допомогою технології блокчейн. Це дозволяє зменшити ризик підробки інформації або шахрайства, оскільки кожна дія, пов’язана з ідентифікацією, фіксується у вигляді транзакції, яка є незмінною та доступною для перевірки [39].

Одним з основних переваг смарт-контрактів є їх здатність забезпечувати автоматичне виконання контрактів на основі заздалегідь визначених умов. Наприклад, у сфері охорони здоров'я смарт-контракти можуть автоматично підтверджувати автентичність пацієнта перед виконанням медичних процедур або перевіркою страховки [22]. Це значно пришвидшує процеси обробки даних і дозволяє знизити час очікування, а також зменшити адміністративне навантаження.

Підвищена прозорість процесів є ще однією важливою перевагою смарт-контрактів. Завдяки використанню блокчейн-технології кожен запис або зміна даних автоматично фіксується в загальнодоступному реєстрі, що дозволяє всім учасникам процесу (пацієнтам, лікарям, страховим компаніям, органам контролю) отримувати доступ до необхідної інформації в реальному часі [23]. Це забезпечує високу прозорість і підвищує довіру серед усіх учасників, оскільки всі зміни можна відслідкувати, і це дозволяє оперативно реагувати на будь-які невідповідності або проблеми.

Ще однією важливою перевагою смарт-контрактів є підвищена безпека персональних даних, що є надзвичайно важливим у контексті сучасних вимог до конфіденційності, таких як Загальний регламент захисту даних ЄС (GDPR) або Закон

про захист здоров'я пацієнтів у США (HIPAA). Блокчейн забезпечує надійний захист даних завдяки криптографічним методам, таким як хешування та шифрування. Це дозволяє обмежити доступ до чутливих даних лише для уповноважених осіб, гарантуючи захист особистої інформації та відповідність вимогам законодавства [29]. Смарт-контракти дозволяють не лише підтверджувати особистість, але й для управління доступом до різноманітних послуг. Наприклад, пацієнти можуть використовувати смарт-контракти для управління своїми медичними записами, дозволяючи доступ лише тим медичним працівникам, які мають необхідні дозволи. Таким чином, смарт-контракти дозволяють створювати систему, в якій користувачі можуть самостійно керувати доступом до своїх даних і змінювати ці налаштування в реальному часі [29].

Для інтеграції смарт-контрактів у обмін медичною інформацією необхідно виконати кілька ключових кроків:

1. Ідентифікація варіантів використання: до них належать управління згодою пацієнта, обробка страхових претензій, управління потоком товарів і послуг та контроль за інформацією клінічних випробувань.
2. Визначення умов контракту: визначити сторони, які беруть участь, їхні ролі та обов'язки, дії, які мають бути виконані, та умови, що ініціюють ці дії.
3. Вибір блокчейн-структури: вибрати відповідну блокчейн-структуру, яка підтримує смарт-контракти та відповідає вимогам обміну медичною інформацією.
4. Розробка коду смарт-контракту: код повинен точно відображати узгоджені умови та включати відповідну логіку для виконання дій на основі попередньо визначених умов.
5. Тестування та розгортання: імітувати різні сценарії, щоб перевірити, чи веде контракт себе відповідно до очікувань за різних умов.

6. Інтеграція з існуючими системами: розробка API або інших інтерфейсів для полегшення обміну даними та комунікації між смарт-контрактом та іншими системами.
7. Забезпечення відповідності та конфіденційності: врахування регуляторних вимог та питань конфіденційності при інтеграції смарт-контрактів в обмін медичною інформацією.
8. Моніторинг і підтримка: постійний моніторинг ефективності та безпеки смарт-контракту в продуктивному середовищі [29].

Приклади використання смарт-контрактів у охороні здоров'я:

1. Управління медичними даними та цифрова ідентифікація пацієнтів: Смарт-контракти дозволяють пацієнтам отримати повний контроль над своїми медичними даними. Платформи, як Medicalchain, використовують смарт-контракти для керування доступом до медичних записів.
2. Управління згодою пацієнтів у клінічних випробуваннях: Згода пацієнта на участь у клінічних випробуваннях може бути автоматично записана у блокчейн, що забезпечує прозорість і відповідність нормативним вимогам.
3. Контроль доступу до медичних записів: Смарт-контракти застосовуються для організації доступу до медичних записів пацієнтів на основі їх цифрової ідентифікації, що дозволяє лікарям і медичним установам отримати доступ до актуальної медичної інформації.
4. Захист від підробок у фармацевтичній індустрії: Смарт-контракти використовуються для відстеження ліків через ланцюг постачання, що допомагає забезпечити автентичність медикаментів і зменшує ризик контрафактної продукції [41].

Смарт-контракти пропонуватимуть вдосконалені механізми для інтеграції різних аспектів цифрової ідентифікації, забезпечуючи високий рівень безпеки, конфіденційності та прозорості для пацієнтів, медичних установ та інших учасників. Інтеграція таких технологій сприятиме розвитку більш ефективної та безпечної

медичної інфраструктури, що дозволить зменшити витрати та покращити обслуговування пацієнтів.

2.4 Конфіденційність та захист даних

Дані пацієнтів у сфері охорони здоров’я мають виняткову цінність, тому забезпечення їхньої конфіденційності та безпеки є одним із найважливіших завдань сучасних медичних систем. Використання технології блокчейн відкриває нові можливості для революційного підходу до управління медичними даними, пропонуючи ефективні способи вирішення актуальних проблем.

Технологічні рішення, засновані на блокчейні, дозволяють пацієнтам отримати повний контроль над їхніми персональними медичними записами. Завдяки механізму приватних ключів пацієнти можуть самостійно регулювати доступ до своїх даних, визначаючи, хто, коли і в якому обсязі може їх використовувати. Це усуває необхідність зберігати інформацію у централізованих базах даних, які раніше часто ставали мішенню для кібератак. Замість цього головною умовою доступу до даних стає згода самого пацієнта. Водночас криптографічні технології, такі як методи доказів з нульовим розголошенням, дозволяють проводити аналіз даних без їхнього розкриття, забезпечуючи повну конфіденційність.

Децентралізований характер блокчейну, у поєднанні з потужними криптографічними інструментами, створює надзвичайно ефективний захист від потенційних загроз. Кожен блок даних зв’язаний із попереднім, формуючи послідовний і захищений ланцюжок, який не можна змінити без порушення його структури. Завдяки цьому будь-які спроби несанкціонованого втручання стають практично неможливими. Відсутність єдиної точки відмови унеможливлює успішну хакерську атаку на всю систему, а цілісність і достовірність даних пацієнтів залишаються гарантованими навіть за умов спроб злому [40].

Щоб забезпечити безпечний доступ до інформації, кожному пацієнту може бути присвоєна унікальна цифрова ідентифікація. Цей механізм працює на основі криптографічних ключів, які виконують роль цифрового паспорта, необхідного для автентифікації користувача та перевірки його прав доступу. Лише особи, які мають відповідний ключ, можуть отримати доступ до інформації, що повністю виключає можливість несанкціонованого використання даних [37].

Ще однією ключовою особливістю блокчейну є забезпечення прозорої хронології всіх взаємодій із медичними даними. Усі транзакції або запити на доступ до інформації маркуються унікальними часовими позначками та зберігаються у спеціальному журналі аудиту. Це дозволяє відстежувати, хто, коли і з якою метою отримував доступ до даних, забезпечуючи прозорість та відповідність міжнародним вимогам конфіденційності, таким як GDPR [38].

Для ефективної співпраці між медичними установами необхідний безпечний обмін інформацією, і блокчейн пропонує надійне рішення цієї проблеми. Використовуючи стандартизовану платформу, технологія забезпечує передачу даних між авторизованими сторонами без ризику їх витоку чи порушення конфіденційності. Незалежно від використовуваних IT-систем, авторизовані користувачі можуть безпечно обмінюватися важливою інформацією, сприяючи ефективному функціонуванню медичних установ.

Попри очевидні переваги, використання блокчейну стикається з низкою викликів. Однією з найважливіших проблем є необхідність надійного захисту приватних ключів, адже їх втрата може призвести до втрати доступу до інформації. Також виникають питання масштабованості криптографічних рішень для обслуговування великих систем охорони здоров’я. Крім того, дотримання нормативно-правових вимог, таких як GDPR, може ускладнити впровадження блокчейну [38]. Однак активна робота дослідників і розробників спрямована на подолання цих перешкод, створюючи можливості для реалізації майбутнього, в якому

блокчейн стане стандартом безпеки і конфіденційності даних у сфері охорони здоров’я [34].

Блокчейн – це не просто інструмент для зберігання даних, а потужна технологія, яка дозволяє пацієнтам і медичним установам працювати безпечно, прозоро та ефективно, створюючи нову еру цифрової охорони здоров’я.

РОЗДІЛ 3 ЗАСТОСУВАННЯ БЛОКЧЕЙНУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ ПАЦІЄНТІВ У МЕДИЦИНІ

3.1 Можливості блокчейну для зберігання та управління медичними даними

Технологія блокчейн відкриває широкі можливості для забезпечення безпеки та ефективного управління медичними даними. Її ключові характеристики, такі як децентралізація, незмінність, узгодженість і високий рівень захисту, дозволяють створювати надійні системи зберігання медичної інформації, уникаючи залучення централізованих органів [26]. Проте, впровадження блокчейну в медичну сферу супроводжується певними викликами, серед яких масштабованість, управління сховищами, продуктивність алгоритмів консенсусу, конфіденційність даних і регуляторні питання.

А. Масштабованість

Обсяги медичних даних постійно зростають через розвиток медичних технологій і збільшення кількості цифрових записів, таких як результати МРТ, рентгенівських знімків, електронних медичних карток тощо [24]. Технологія блокчейн зі своїми фіксованими розмірами блоків і часом їх створення стикається з проблемою повільної обробки транзакцій при великій кількості операцій. Наприклад, біткоїн має розмір блоку 1 МБ із середнім часом підтвердження 10 хвилин, тоді як Ethereum обробляє блоки за 16 секунд. У медичній сфері така затримка може бути критичною.

Для вирішення цієї проблеми пропонуються такі рішення:

- **On-chain** – обробка транзакцій безпосередньо в основному ланцюгу блокчейну.
- **Off-chain** – позаланцюгові рішення для оптимізації обробки даних.

- **Side-chain** – використання додаткових бокових ланцюгів для розподілу навантаження.
- **Child-chain** – збереження інформації в дочірніх ланцюгах із передачею результатів у батьківський ланцюг.
- **Interchain** – забезпечення зв’язку між різними ланцюгами для оптимізації роботи системи [20].

Ці рішення дозволяють оптимізувати роботу блокчейн-систем, що вже було продемонстровано в проектах, спрямованих на вдосконалення Ethereum.

Б. Проблеми безпеки та конфіденційності

Медичні дані є одними з найбільш конфіденційних видів інформації, тому їх захист є критично важливим. Блокчейн дозволяє захищати дані через використання децентралізованих систем, у яких кожна транзакція зберігається у незмінному реєстрі. Для додаткового захисту можуть використовуватися:

- Анонімні мережі, наприклад, Tor або їхні вдосконалення, що дозволяють приховати особисту інформацію пацієнтів.
- Смарт-контракти, які встановлюють суворі правила доступу до медичних записів, дозволяючи лікарям і пацієнтам ефективно контролювати дані.

Ці інструменти сприяють мінімізації ризиків витоку або несанкціонованого доступу до медичних даних [21].

В. Управління зберіганням

Медичні записи, що постійно накопичуються, створюють значне навантаження на сховища. Реєстр блокчейну містить усі транзакції, починаючи від першого блоку, і розподіляється між вузлами мережі. У медичній сфері це може призводити до надмірного споживання пам’яті, особливо якщо враховувати великий обсяг файлів, таких як рентгенівські знімки чи результати аналізів.

Для вирішення цієї проблеми пропонується використовувати:

- Розподілені сховища даних із інтеграцією блокчейн для зберігання лише хешів великих файлів.

- Активацію вузлів із різними рівнями доступу залежно від їхньої ролі в системі.

Г. Продуктивність алгоритмів консенсусу

У блокчейні медичних даних алгоритми консенсусу забезпечують узгодженість транзакцій, але зі збільшенням кількості вузлів у мережі їхня продуктивність може знижуватися. Для уникнення цих проблем у медичних системах можна використовувати адаптивні алгоритми, які поєднують ефективність із безпекою [28].

Д. Управління ресурсами

Медичні системи, побудовані на основі блокчейну, повинні забезпечувати економію ресурсів, особливо у випадках, коли транзакції генеруються постійно. Це можливо завдяки оптимізації витрат на майнінг і винагород для учасників мережі.

Е. Регуляторні та нормативні виклики

Для впровадження блокчейну в медичну сферу необхідно враховувати законодавчі вимоги та стандарти захисту даних, наприклад, GDPR у ЄС чи HIPAA у США. Розробка єдиних стандартів дозволить забезпечити сумісність і довіру до таких систем [28].

Блокчейн-технології мають значний потенціал для зберігання та управління медичними даними, але їхнє впровадження потребує вирішення технічних, економічних і регуляторних викликів. Попри це, можливості технології дозволяють створити ефективні системи, які сприяють підвищенню рівня безпеки, конфіденційності й доступності медичних даних .

3.2 Огляд міжнародного досвіду

Успішне впровадження блокчейн-технологій у сфері охорони здоров'я у різних країнах світу є важливим джерелом практичного досвіду для розробки власних рішень. Розгляд міжнародного досвіду дозволяє оцінити переваги та виклики, пов'язані із застосуванням блокчейну для збереження та управління медичними

даними. Особливий інтерес викликають системи, які забезпечують захист цифрової ідентифікації пацієнтів, зберігання та обмін медичними записами. У цьому розділі буде проаналізовано три успішні кейси:

- національна система e-Health в Естонії**,** яка є зразком інтеграції блокчейну у масштабі країни;
- проект MedRec у США**,** який демонструє інноваційний підхід до доступу та обміну медичними даними на основі блокчейн-технології;
- ініціатива Guardtime Health в Естонії**,** спрямована на захист медичних записів за допомогою блокчейну.

3.2.1 Кейс Естонії: національна система e-Health

Естонія є одним із лідерів у впровадженні електронної системи охорони здоров’я в Європі. З моменту запуску у 2008 році система e-Health пройшла значну еволюцію, додавши нові послуги, інтегруючи приватний сектор і впровадивши блокчейн для забезпечення безпеки доступу та цілісності даних. Цей досвід демонструє значний прогрес і інновації в електронній охороні здоров’я та сприяє досягненню стратегічних цілей, таких як покращення обміну інформацією, підвищення рівня безпеки даних та довіри громадян [42].

Однією з ключових умов успіху є сильна державна координація, яка об’єднала зусилля різних зацікавлених сторін і знайшла баланс між автономією пацієнтів, використанням персональних даних і суспільною вигодою. Важливу роль відіграло залучення громадян та забезпечення їхньої довіри до системи. Також значна увага приділялася цифровій грамотності та ухваленню законодавчих норм для запобігання неправомірному використанню даних [42].

У 2016 році Естонія стала першою країною, яка впровадила блокчейн для забезпечення цілісності урядових даних. Блокчейн став ключовим інструментом для вирішення кількох важливих проблем, зокрема для "забезпечення власності даних

громадян", "підвищення прозорості" та "захисту конфіденційності". Технологія блокчейн гарантує, що медичні картки пацієнтів в Естонії захищені, що записів не можна змінити без відповідного дозволу, а доступ до них можна контролювати.
Окрім цього, в Естонії також використовується блокчейн для контролю за ліками, що продаються в країні, через трекінг постачальницького ланцюга для лікарських засобів та упаковок. Це дозволяє забезпечити надійність і прозорість медичних даних та знизити ризик маніпуляцій з ними [43].

Однією з основних переваг e-Health є можливість швидкого доступу до медичних історій пацієнтів, результатів тестів та діагнозів для пацієнтів і лікарів у будь-який час і з будь-якого місця. Це не лише полегшує медичне обслуговування, а й допомагає в ліквідації черг, скороченні часу на лікування і забезпеченні ефективного використання медичних ресурсів [43].

У рамках реалізації електронних консультацій у первинній медичній допомозі, естонці можуть звертатися до лікарів через цифрові канали без необхідності особистої зустрічі, що знижує навантаження на медичних працівників і зменшує час на прийом пацієнтів. Впровадження таких послуг значно підвищує доступність медичних послуг у віддалених районах.

Завдяки блокчейн-технології, яка забезпечує безпеку даних, система e-Health в Естонії продовжує розвиватися, зберігаючи високу довіру громадян і медичних працівників до її ефективності та надійності.

Основними перевагами впровадження технології блокчейн є:

- Забезпечення надійності та цілісності медичних даних.
- Підвищення прозорості доступу до медичних записів та процедур.
- Забезпечення захисту персональних даних пацієнтів.
- Зниження внутрішніх загроз та зловживань даними [42].

У той же час важливою проблемою залишається цифрова ізоляція окремих груп населення, що може ускладнити доступ до медичних послуг для певних категорій

пацієнтів. З метою мінімізації цього ризику необхідно забезпечити належну освітню підтримку і підвищення цифрової грамотності [43].

Таким чином, досвід Естонії у впровадженні блокчейн-технологій у сфері охорони здоров'я є важливим прикладом для інших країн, що прагнуть покращити безпеку та ефективність своїх медичних систем.

3.2.2 Проект MedRec (США): доступ до медичних даних на основі blockchain

Медичні записи потребують інновацій. Дані пацієнтів часто розпорошені між різними постачальниками медичних послуг, що створює серйозні перешкоди для їх ефективного використання. Пацієнти змушені мати справу з дублюванням процедур, втратою часу та труднощами у доступі до попередніх даних. В основі цієї проблеми лежить те, що збереження медичних записів здебільшого покладається на постачальників, а не на самих пацієнтів [24].

MedRec є революційною платформою, яка використовує технологію блокчейну для оптимізації електронних медичних записів (EHR) (Рис 3.1). Ця система забезпечує децентралізований доступ до даних пацієнтів, дозволяючи різним медичним установам взаємодіяти через безпечну та прозору мережу. Важливо, що доступ до даних можливий лише за згодою самого пацієнта, що гарантує конфіденційність [24].

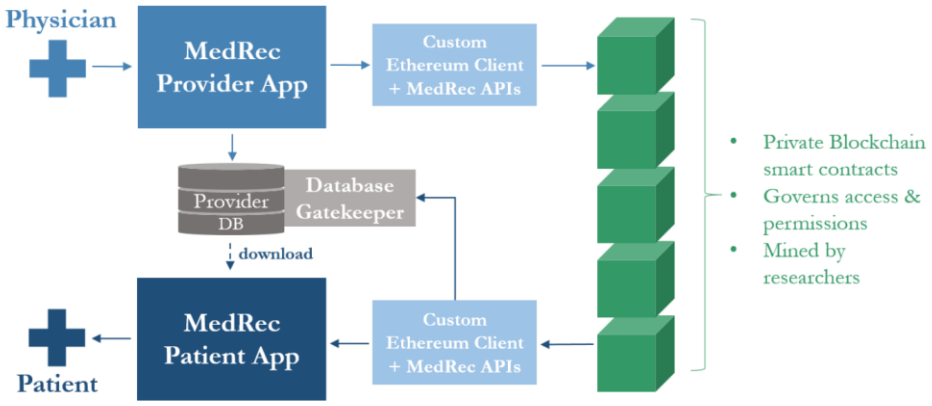


Рис. 3.1 System Architecture [24]

Основна ідея MedRec полягає у використанні розумних контрактів на базі блокчейну Ethereum. Ці смарт-контракти не зберігають медичні записи безпосередньо, а кодують метадані, які забезпечують безпечний доступ до даних, зберігаючи інформацію про власність, дозволи та цілісність даних. Завдяки цій системі можна:

- автоматично оновлювати записи пацієнтів;
- уникати дублювання процедур;
- забезпечити миттєве отримання звітів різними сторонами.

MedRec надає можливість учасникам системи управляти своїми даними через спеціальні смарт-контракти (Рис.3.2), серед яких:

1. Контракт реєстратора (Registrar Contract - RC): використовується для ідентифікації учасників системи, включаючи пацієнтів та постачальників послуг.
2. Контракт взаємин пацієнт-постачальник послуг (Patient-Provider Relationship Contract -PPR): зберігає інформацію про доступ до записів та дозволи між пацієнтами та медичними закладами.
3. Зведений контракт (Summary Contract - SC): надає єдину точку доступу до історії медичних записів, дозволяючи швидко перевіряти статус і оновлення взаємин [24].

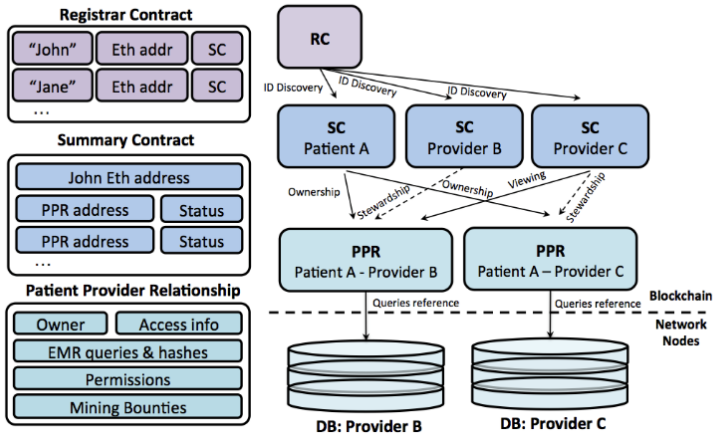


Рис 3.2 MedRec smart contracts on the blockchain and data references [24]

Розглянемо більш детально дану інформацію, що представлена вище.

RC - цей глобальний контракт відображає ідентифікаційні рядки учасників на їхні Ethereum-адреси (еквівалент публічного ключа). Використовуються ідентифікаційні рядки, а не безпосередньо криптографічні публічні ключі, що дозволяє застосовувати вже існуючі форми ідентифікації. Політики, закодовані в контракті, можуть регулювати процес реєстрації нових ідентифікацій або зміну прив’язки існуючих. Реєстрацію ідентифікацій можна обмежити, дозволивши її лише сертифікованим установам [24].

PPR - укладається між двома вузлами в системі, коли один вузол зберігає та керує медичними записами іншого. У нашому випадку йдеться про відносини між медичним постачальником і пацієнтом, але цей підхід можна застосувати до будь-якої взаємодії між двома сторонами, яка передбачає управління даними. PPR визначає набір вказівників на дані та відповідні дозволи на доступ, які ідентифікують записи, що зберігаються постачальником. Кожен вказівник складається з рядка запиту, який, виконуючись у базі даних постачальника, повертає підмножину даних пацієнта. До рядка запиту додається хеш цієї підмножини даних, щоб гарантувати, що дані не були змінені в джерелі [24].

Додаткова інформація вказує, де саме можна отримати доступ до бази даних постачальника в мережі, наприклад, через ім'я хоста та порт у стандартній мережевій топології. Запити на дані та пов'язана інформація створюються постачальником і оновлюються, коли додаються нові записи. Щоб пацієнти могли ділитися своїми даними з іншими, у системі реалізовано словник (хеш-таблицю), який зіставляє адреси користувачів із переліком додаткових запитів. Кожен запит дозволяє визначити частину даних пацієнта, до яких сторонній користувач отримує доступ.

Слід зазначити, що використання універсальних рядків дозволяє легко інтегрувати цю систему з будь-якими базами даних, які підтримують текстові запити. Це дає змогу зручно впроваджувати рішення у вже існуючу інфраструктуру

зберігання даних постачальників. У той же час пацієнти отримують точний контроль над доступом до своїх медичних записів, обираючи, які саме частини даних вони готові надати.

SC - цей контракт функціонує як шлях з підказками для учасників системи, що дозволяє їм знаходити історію своїх медичних записів. Він містить список посилань на контракти відносин пацієнт-постачальник (PPR), що представляють усі попередні та поточні взаємодії учасника з іншими вузлами в системі. Пацієнти, наприклад, матимуть в своєму Зведеному контракті посилання на всі медичні заклади, з якими вони мали справу. Постачальники послуг, в свою чергу, ймовірно, матимуть посилання на пацієнтів, яких вони обслуговують, а також на треті сторони, з якими пацієнти дозволили обмін даними [24].

Зведений контракт зберігається в розподіленій мережі, надаючи важливі функції резервного копіювання та відновлення. Пацієнти можуть залишати систему та знову до неї приєднуватися кілька разів, на довільний період, і завжди відновлювати доступ до своєї історії, завантажуючи останній блокчейн з мережі. Блокчейн реєструється та зберігається, поки в мережі є вузли, що беруть участь.

З метою забезпечення цілісності та доступності медичних записів, дана система також включає механізм для відновлення відсутніх або пошкоджених даних. Втрачені або неповні дані можна відновити з мережі в будь-який час, використовуючи Summary Contract (SC) кожного вузла. Це дозволяє користувачам (пацієнтам та постачальникам послуг) швидко відновлювати доступ до необхідної інформації, навіть якщо певні записи були втрачені або видалені з локальних баз даних [24].

Компоненти вузлів системи спроектовані таким чином, щоб забезпечити їх інтеграцію з існуючою інфраструктурою електронних медичних записів (EHR). Очікується, що багато вузлів, зокрема постачальники медичних послуг, вже мають надійно керовані бази даних пацієнтів на серверах, підключених до мережі. Архітектура системи включає чотири основні програмні компоненти: Backend Library, Ethereum Client, Database Gatekeeper та EHR Manager. Ці компоненти можуть бути

розгорнуті на серверах, утворюючи розподілену систему, що функціонує узгоджено (Рис. 3.3). Прототип, розроблений для цієї системи, демонструє інтеграцію з базою даних SQLite та забезпечує управління через веб-інтерфейс користувача. Важливо зазначити, що будь-які реалізації бекенду постачальника послуг та інтерфейсу користувача можуть взаємодіяти в рамках системи, завдяки модульному протоколу, визначеному через блокчейн-контракти [24].

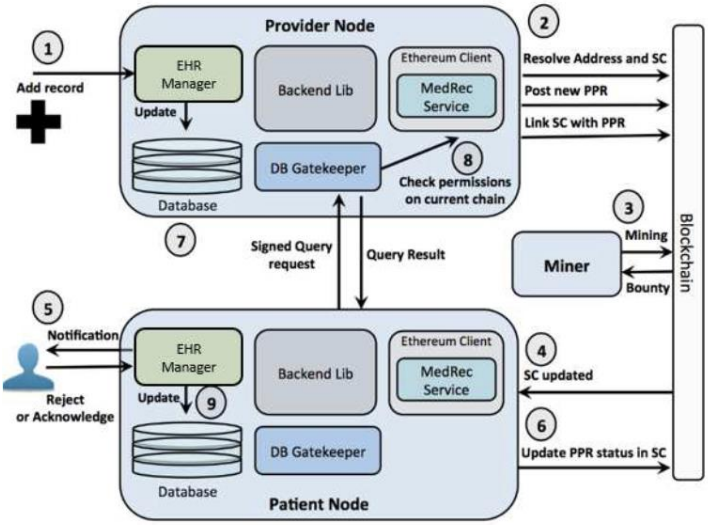


Рис 3.3 Приклад оркестрації системи: постачальник додає запис для нового пацієнта [24]

Вузли пацієнтів мають ту саму архітектуру компонентів, що й вузли постачальників. Реалізація цих компонентів може здійснюватися на локальних комп’ютерах або мобільних пристроях. Локальні бази даних пацієнтів можуть бути реалізовані як легкі бази даних, що зберігають медичні дані лише тимчасово (як кеш). Втрачені або відсутні дані можуть бути отримані з мережі в будь-який час за допомогою Summary Contract відповідного вузла [24].

Backend Library (Бібліотека бекенду) - є основним компонентом, який спрощує роботу системи, абстрагуючи взаємодії з блокчейном. Ця бібліотека надає API, який керує підкапотними деталями комунікації з блокчейном, дозволяючи програмам управління записами та їх інтерфейсам користувача уникати безпосереднього взаємодії з складною частиною блокчейну. Одним із основних викликів при взаємодії

з блокчейном є забезпечення того, щоб транзакції успішно приймалися мережею. Backend Library вирішує цю проблему автоматично, обробляючи перевірку транзакцій, включаючи випадки, коли транзакції скасовуються або затримуються.

Бібліотека бекенду (Backend Library) взаємодіє з Ethereum клієнтом для виконання низькорівневих завдань, таких як форматування та розбір протоколу Ethereum. У випадку, коли постачальник додає новий запис про пацієнта, як показано на етапах 1 і 2 в Рис 3.3, процес починається з використання Registrar Contract для визначення ідентифікаційної інформації пацієнта та її відповідного Ethereum-адреси. Потім постачальник завантажує новий PPR (Contract для взаємодії між пацієнтом і постачальником) на блокчейн, прив'язуючи його до Ethereum-адреси пацієнта. Вузол постачальника формує запит, який посилається на ці дані, і оновлює PPR. В кінці система надсилає транзакцію для асоціації нового PPR **з** Summary Contract пацієнта**,** що дозволяє пізніше знаходити запис на блокчейні [24].

Ethereum Client (Клієнт Ethereum) забезпечує повну функціональність для підключення та участі в мережі Ethereum. Він підключається до мережі peer-to-peer, кодує та надсилає транзакції та підтримує перевірену локальну копію блокчейну.

Етап 3 передбачає процес майнінгу, де учасники мережі заохочуються надавати свої обчислювальні ресурси для забезпечення надійного та поступового розвитку блокчейн-ланцюга. Стимулювання майнерів має на меті підтримку довіри до системи та її стабільність, що є критично важливим для ефективного функціонування в екосистемі охорони здоров'я. У випадку, описаному на етапах 4–6 Рис 3.3, вузол пацієнта постійно моніторить SC, і після того, як новий блок з’єднується з новим PPR, клієнт надсилає сигнал про оновлення. Пацієнт отримує сповіщення і може прийняти чи відхилити нову комунікацію, що оновить Summary Contract відповідно. Якщо комунікацію прийнято, система автоматично запитує нові медичні дані, використовуючи інформацію в PPR для пошуку сервера Database Gatekeeper постачальника [24].

Database Gatekeeper (Пропускник бази даних) є офлайн інтерфейсом доступу до локальної бази даних вузла, який регулюється дозволами, збереженими на блокчейні. Цей сервер прослуховує запити на доступ до даних з клієнтів у мережі, що містять запит на виконання та посилання на блокчейн-основний PPR, який підтверджує права доступу. Запит підписується криптографічно видавцем, що дозволяє пропускнику перевірити ідентичність. Після перевірки підпису пропускник перевіряє контракти на блокчейні, щоб впевнитися, що запитуюча адреса має дозвіл на доступ до даних. Якщо перевірка пройшла успішно, пропускник виконує запит на локальній базі даних і повертає результат клієнту [24].

Етапи 7–9 в Рис 3.3 демонструють, як пацієнт отримує особисті дані з вузла постачальника. Компоненти також підтримують доступ третіх осіб: пацієнт може вибрати дані для спільного доступу і оновити відповідний PPR, включаючи адресу третьої особи та запит. В разі необхідності, вузол пацієнта може визначити адресу третьої особи через Registrar Contract на блокчейні. Потім вузол пацієнта зв’язує існуючий PPR з постачальником до Summary Contract третьої особи. Третя особа автоматично отримує сповіщення про нові дозволи і може слідувати посиланню для отримання необхідної інформації [24].

EMR Manager (Менеджер електронних медичних записів) інтегрує всі раніше згадані компоненти в єдину систему для управління електронними медичними записами. Ця програма виводить дані з локальних SQLite баз даних для перегляду, надає сповіщення про оновлення та пропонує можливості для спільного доступу та отримання даних. Інтерфейс користувача спроектовано таким чином, щоб він був інтуїтивно зрозумілим, чітким і інформативним, згідно з кращими практиками, такими як ті, що визначені в конкурсі Blue Button Міністерства у справах ветеранів США [24].

Проєкт MedRec є інноваційною системою, яка сприяє розвитку прецизійної медицини та зручному доступу до медичних даних, водночас вирішуючи проблему централізованого зберігання даних, що є вразливим до кіберзагроз і витоків

інформації. Використовуючи блокчейн-технології, MedRec надає можливість децентралізованого зберігання даних, що гарантує безпечний, контролюваний доступ до медичних записів з боку пацієнта, а також дозволяє забезпечити їх координоване використання між різними учасниками медичної екосистеми, такими як лікарі, постачальники послуг, фармацевтичні компанії та страхові організації.

Завдяки відкритим API, система MedRec має потенціал для інтеграції з іншими медичними платформами та IT-інфраструктурами, що відповідають сучасним стандартам безпеки та конфіденційності. Це дозволяє створити масштабовану систему для обміну медичними даними, що відповідає вимогам національних стандартів у сфері охорони здоров'я, зокрема рекомендаціям ONC (Office of the National Coordinator for Health Information Technology), спрямованим на підтримку розвитку стандартів та забезпечення безпечного обміну даними [24].

Проєкт активно розвивається та вже взаємодіє з ключовими гравцями в медичній галузі, такими як лікарні, медичні організації, страхові компанії та державні установи, з метою збору вимог до функціональності та розширення сценаріїв використання. Серед таких учасників — Міністерство у справах ветеранів США, медичні установи, фармацевтичні компанії та інші. Це дає можливість адаптувати систему MedRec до потреб реальних користувачів та забезпечити її подальший розвиток.

Для вдосконалення системи та її безпеки в планах є проведення додаткових етапів тестування, включаючи аудит безпеки та тестування на проникнення, а також програми заохочення виявлення помилок. Це дозволить значно підвищити надійність системи та забезпечити високий рівень захисту медичних даних.

3.2.3 Guardtime Health (Естонія): захист медичних записів

Guardtime — це естонський стартап, який використовує блокчейн-технології для захисту як публічних, так і приватних даних, забезпечуючи їх верифікацію та

цілісність. Компанія розробила систему, що використовує математичний доказ для перевірки коректності даних, мереж, систем і процесів через так звану KSI Blockchain. Ця технологія вже знайшла своє застосування у захисті медичних записів в Естонії, де Guardtime уклала угоду з урядом країни для забезпечення безпеки 1 мільйона медичних записів за допомогою своїх інноваційних рішень.

У межах цієї угоди, компанія співпрацює з Управлінням електронної охорони здоров'я Естонії та Управлінням інформаційних систем Естонії, що дозволяє забезпечити захист державних даних та інтеграцію з національною медичною інфраструктурою. Ключова перевага такої технології полягає в використанні децентралізованої блокчейн-архітектури, яка гарантує безпечне зберігання та перегляд медичних даних без необхідності створення централізованої бази даних. Це дає змогу зменшити ризики витоків інформації та атаки на дані, що особливо важливо в умовах сучасних кіберзагроз.

Естонія є однією з найбільш розвинених цифрових країн у світі, і саме тут технологія Guardtime була активно впроваджена. Громадяни Естонії користуються смарт-картками, що зберігають їх медичні дані та дають доступ до понад 1000 державних послуг. Завдяки цьому, всі медичні записи можуть бути безпечно перевірені та доступні як для пацієнтів, так і для медичних працівників або інших відповідальних осіб [43].

Використання блокчейну в системі зменшує внутрішні загрози для даних, що робить інформацію про пацієнтів більш безпечною. Інтеграція таких технологій у сферу охорони здоров’я дозволяє зменшити ризики несанкціонованого доступу та забезпечити високий рівень конфіденційності.

Guardtime розробила нову платформу як послугу Blockchain-as-a-Service (BCaaS)**,** яка дозволяє забезпечити безпеку медичних даних у реальному часі. Основною метою цієї платформи є захист віддалених сегментів медичної інфраструктури, таких як амбулаторії та пацієнти, що знаходяться на реабілітації. Це

досягається через створення схем кібер-фізичної безпеки, що включають семантичне моделювання контекстів безпеки та конфіденційності.

Проект передбачає використання таких основних компонентів:

- Аутентифікація та авторизація: Для забезпечення безпеки використовуються посилені послуги аутентифікації та авторизації через безпечні пристрої IoT, засновані на апаратному забезпеченні та біометричній аутентифікації.
- Криптографічний сервер: Для забезпечення безпеки даних реалізовано симетричну криптографію, хешування, генерацію випадкових чисел, а також генерацію простих чисел і ключів.
- Система підписання та верифікації: Вона забезпечує цілісність даних на всіх етапах їх обробки та зберігання [43].

Ці компоненти дозволяють створювати надійну та безпечну інфраструктуру для обміну медичними даними та їх захисту від несанкціонованого доступу.

Guardtime пропонує інтеграцію своїх технологій в існуючу медичну інфраструктуру, що дозволяє державним органам, медичним установам та пацієнтам здійснювати безпечний доступ до даних та здійснювати необхідні перевірки. Платформа також передбачає створення цифрової медичної карти для кожного пацієнта, що дозволяє зберігати та верифікувати всі медичні дані.

Завдяки таким технологіям, система Guardtime Health забезпечує високий рівень безпеки та прозорості у збереженні медичних записів, що робить її одним із провідних рішень для захисту медичних даних у глобальному контексті.

Guardtime планує подальшу інтеграцію з іншими важливими компонентами медичної інфраструктури, розширюючи можливості платформи для обміну та захисту медичних даних. Вони продовжують активно співпрацювати з органами охорони здоров'я, страхування та урядами, щоб удосконалювати свою систему та покращувати доступ до надійної медичної інформації [43].

У контексті подальшого розвитку цифрових рішень для охорони здоров'я, Gravitate-Health є ще одним прикладом того, як інноваційні технології можуть

перетворити управління медичними даними на ще більш безпечний і зручний процес (Рис. 3.4). Подібно до Guardtime, Gravitate-Health орієнтована на інтеграцію новітніх цифрових інструментів, таких як блокчейн, для покращення доступу до надійної медичної інформації [42].

Gravitate-Health розробляє цифрову платформу, яка дозволяє пацієнтам, медичним працівникам і установам швидко отримувати та перевіряти медичні дані в режимі реального часу. Це рішення спрямоване на створення безпечного, зручного та доступного середовища для управління медичними записами, що є важливим кроком у розвитку цифрової трансформації охорони здоров'я.

Так само, як і технологія Guardtime**,** Gravitate-Health прагне забезпечити цілісність і безпеку медичних даних за допомогою інноваційних підходів, таких як створення цифрових медичних карт та інтеграція з іншими системами охорони здоров'я. Технології, розроблені Gravitate-Health, мають потенціал забезпечити високий рівень доступності та прозорості медичних записів, одночасно мінімізуючи ризики несанкціонованого доступу та маніпуляцій з даними [42].

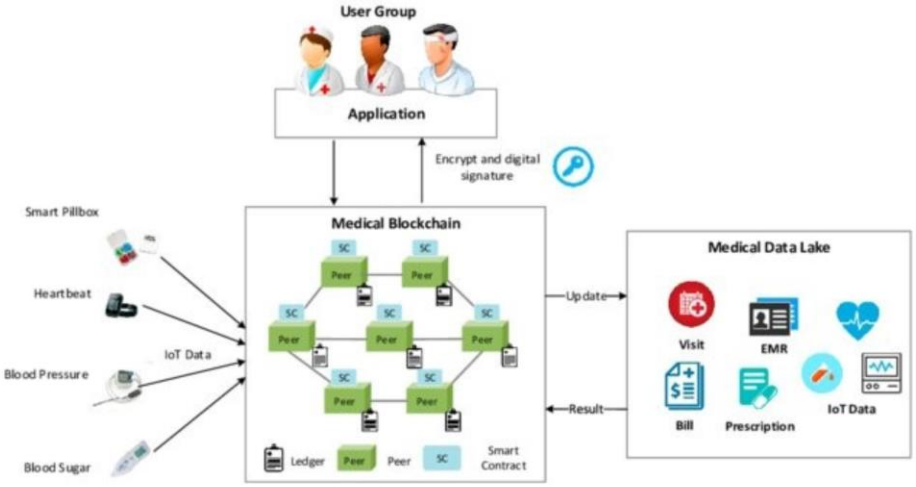


Рис. 3.4 Структура системи Gravitate-Health [42]

Таким чином, Guardtime Health представляє собою потужний інструмент для забезпечення безпеки медичних даних, що відповідає сучасним вимогам конфіденційності та захисту інформації. Технологія блокчейн, яку використовує

компанія, може стати основою для побудови нових стандартів безпеки та доступу до медичних даних на глобальному рівні.

3.3 Перспективи розвитку та можливі виклики впровадження блокчейну в українській медицині

Впровадження інноваційних інформаційних технологій у медичну сферу є важливою складовою реформи охорони здоров'я в Україні. Однією з таких технологій є блокчейн, який може значно покращити ефективність роботи медичних закладів, зменшити ризики шахрайства та забезпечити більшу прозорість і безпеку обробки медичних даних. В даному розділі ми проаналізуємо кроки, які вже були зроблені в Україні для впровадження інформаційних технологій в медичній сфері, можливості застосування блокчейн-технологій, основні перспективи розвитку, виклики та пропозиції для подальшого розвитку цієї технології в українському охороні здоров'я.

В Україні вже реалізуються кілька ініціатив, спрямованих на автоматизацію медичних процесів і забезпечення доступу до медичних даних у електронному вигляді. Одним із таких кроків є створення електронної системи охорони здоров'я (ЕСОЗ), яка забезпечує автоматизацію обліку медичних послуг і управління інформацією про охорону здоров'я. ЕСОЗ включає центральну базу даних, що належить Національній службі здоров'я України (НСЗУ), і медичні інформаційні системи (МІС), що дозволяють зберігати і передавати дані в електронному вигляді. Завдяки цій системі медичні заклади можуть зберігати інформацію в цифровому форматі, що дозволяє покращити якість надання медичних послуг та пришвидшити процес прийняття рішень [5].

Особливу увагу в системі ЕСОЗ приділено захисту даних. Використовуються кваліфіковані електронні підписи (КЕП), принципи GDPR для зберігання медичних та персональних даних окремо, а також blockchain-подібні алгоритми для забезпечення

цілісності даних. Це дозволяє забезпечити надійний захист персональних медичних записів та створити прозору систему обміну даними [5].

Україна має можливість використати міжнародний досвід країн, де вже успішно застосовуються блокчейн-технології в медицині. Наприклад, в Естонії у 2016 році був запущений проект e-health, що дозволив створити загальний реєстр даних пацієнтів. Цей проект продемонстрував ефективність блокчейну для зберігання та обміну медичними даними, забезпечуючи високий рівень безпеки і прозорості. У Великій Британії був реалізований проект Medicalchain для безпечного зберігання особистих даних пацієнтів за допомогою блокчейн. Крім того, у Франції розробляється платформа MedicalDAO.io для консультування пацієнтів з використанням блокчейну та штучного інтелекту. Україна може не тільки перейняти найкращі практики з цих країн, але й адаптувати їх до своїх умов, враховуючи специфіку національної медичної системи.

Блокчейн може стати основою для низки інноваційних рішень у медичній сфері, серед яких:

- Єдиний реєстр медичних карт пацієнтів**.** Блокчейн дозволить створити систему для зберігання медичних даних пацієнтів, доступ до яких буде мати лише уповноважений медичний персонал. Це дозволить зменшити кількість втрачених або недостовірних медичних записів.
- Відстеження поставок медикаментів**.** Використання блокчейну в ланцюгах постачання дозволить забезпечити прозорість поставок ліків і медичних засобів, що допоможе уникнути шахрайства і спекуляцій.
- Електронні рецепти та направлення. Блокчейн може бути використаний для зберігання і передачі електронних рецептів та направлень, що дозволить лікарям та пацієнтам швидше обмінюватися інформацією і спростить процес отримання медичних послуг.

- Медична телемедицина**.** Завдяки використанню блокчейну можна забезпечити безпечний обмін медичними даними для дистанційних консультацій та лікування через телемедичні платформи [8].

Можливі виклики впровадження блокчейн-технологій у медичну сферу України є багатогранними і потребують уважного підходу до вирішення кожного з них. Ось кілька ключових проблем, які можуть виникнути:

- Технічні та інфраструктурні труднощі**.** В Україні на даний момент ще не створено достатньо розвиненої інфраструктури для ефективного впровадження блокчейн-технологій у медичну сферу. Це включає в себе як недостатню швидкість інтернет-з'єднання в деяких регіонах, так і обмежений доступ до необхідних серверів та потужностей для підтримки блокчейн-мережі. Водночас, блокчейн-системи потребують високого рівня технічної підтримки та постійного оновлення програмного забезпечення.
- Недостатня правова база і регулювання**.** Україна не має повністю сформованої нормативно-правової бази для регулювання використання блокчейн-технологій у медицині. Це може стати серйозним бар'єром для успішного впровадження цієї технології, оскільки необхідно визначити, як зберігати і обробляти персональні медичні дані, забезпечити їх конфіденційність, а також визначити, хто має доступ до цих даних і як контролювати цей процес. Без чітких законодавчих норм існує ризик виникнення правових проблем та конфліктів.
- Опір з боку медичних установ та персоналу**.** Зміна звичних процесів в медичних закладах може викликати опір з боку медичних працівників. Блокчейн-технології потребують нових підходів до зберігання та обміну даними, що може виглядати складним і незвичним для лікарів та медсестер, які звикли працювати з традиційними системами. Навчання та переконання персоналу у необхідності таких змін можуть бути довготривалими та ресурсозатратними процесами.
- Фінансова складність впровадження**.** Впровадження блокчейн-технологій потребує значних фінансових витрат на розробку, підтримку і адаптацію

інфраструктури. Оскільки технології, що забезпечують надійний рівень безпеки та ефективності, потребують великих вкладень на початковому етапі, виникає питання про те, як держава та приватні медичні установи будуть фінансувати ці інвестиції. З огляду на обмежений бюджет держави та медичних установ, залучення додаткових ресурсів через партнерства або міжнародні гранти може бути єдиним можливим шляхом.

- Інтеграція з існуючими системами**.** Україні вже є розвинута електронна система охорони здоров'я (ЕСОЗ), і для того, щоб блокчейн інтегрувався в цю систему, необхідно буде провести масштабні роботи з адаптації і модифікації існуючих платформ. Враховуючи технічні обмеження та необхідність забезпечення сумісності між різними інформаційними системами, це може бути складним і тривалим процесом, що потребує додаткових ресурсів та експертних знань [9].

Таким чином, кожен із цих викликів потребує детального аналізу та комплексного підходу до вирішення, зокрема через розробку законодавчих ініціатив, інвестицій у технічну інфраструктуру, а також програми навчання та підтримки медичних працівників.

Рекомендації та кроки для впровадження блокчейн-технологій в українську медицину:

- Розробка та адаптація законодавчої бази**.** Оскільки законодавчі та нормативні акти України ще не повністю охоплюють питання використання блокчейн-технологій у медицині, важливо розпочати роботу над розробкою чіткої правової бази. Це включає прийняття законів, що регулюють захист персональних даних, питання конфіденційності медичної інформації та визначення механізмів контролю за доступом до таких даних. Законодавчі ініціативи повинні враховувати міжнародні стандарти, такі як GDPR, для забезпечення безпеки та конфіденційності даних пацієнтів.
- Покращення інфраструктури та технічної бази**.** Для успішного впровадження блокчейн-технологій в медичну сферу необхідно значно покращити технічну

інфраструктуру країни. Це включає в себе розширення мережі високошвидкісного інтернету, розвиток хмарних технологій та забезпечення доступу до потужних серверів для обробки та зберігання медичних даних. Держава повинна сприяти розвитку IT-інфраструктури та залучати інвестиції в технологічні стартапи, які спеціалізуються на розробці блокчейн-рішень для медицини.

- Проведення пілотних проектів**.** Важливо почати з пілотних проектів, які дозволять протестувати ефективність блокчейн-рішень у конкретних медичних установах або регіонах. Це може включати впровадження єдиного реєстру пацієнтів, створення цифрових медичних карток або тестування платформ для відстеження постачань ліків. Пілотні проекти допоможуть виявити потенційні проблеми на ранніх етапах і дозволять адаптувати технології до специфічних потреб української медичної системи.
- Навчання та підготовка медичного персоналу**.** Важливим кроком є забезпечення підготовки медичних працівників до роботи з новими технологіями. Це передбачає організацію тренінгів, вебінарів і курсів для лікарів, медсестер та адміністративного персоналу. Необхідно забезпечити розуміння того, як працює блокчейн, як здійснюється доступ до даних пацієнтів через цифрові медичні картки і як це покращить якість надання медичних послуг. Така підготовка допоможе зменшити опір змінам і сприяти швидкому впровадженню нових технологій у медичних установах.
- Залучення міжнародних партнерів та консалтингових компаній**.** Україна може використовувати досвід інших країн, які вже впровадили блокчейн у медичну сферу. Потрібно налагоджувати партнерства з міжнародними організаціями та технологічними компаніями, що спеціалізуються на розробці блокчейн-рішень для медицини. Консультації з таких експертів допоможуть уникнути можливих помилок та прискорять процес інтеграції блокчейн-технологій в українську медицину.

- Інтеграція з існуючими медичними інформаційними системами. Важливим кроком для успішного впровадження блокчейн-технологій є інтеграція з вже існуючими медичними інформаційними системами (МІС). Це дозволить забезпечити безперервний обмін даними між різними медичними установами та зберігати їх у блокчейні, що підвищить довіру до медичних записів. Інтеграція має бути здійснена таким чином, щоб не порушити звичні робочі процеси медичних установ і забезпечити плавний перехід до нової системи.
- Забезпечення фінансування та державної підтримки**.** Для успішного впровадження блокчейн-технологій необхідне фінансування, яке може бути частково надане державою через програми підтримки інновацій у сфері охорони здоров'я. Важливо залучити як державні, так і приватні інвестиції для розвитку та реалізації таких проектів. Держава також повинна стимулювати участь місцевих ІТ-компаній та стартапів у розробці рішень, що відповідають вимогам медичної системи.
- Оцінка результатів та коригування стратегії**.** Після впровадження пілотних проектів важливо здійснювати постійну оцінку результатів та ефективності блокчейн-рішень. Збір даних про успішність їх застосування в реальних умовах дозволить зробити коригування та вдосконалити технології. Оцінка ефективності також дозволить визначити, які аспекти потрібно доопрацювати або адаптувати, щоб забезпечити ще більшу безпеку та ефективність системи.

Впровадження блокчейн-технологій в українську медицину відкриває широкі перспективи для покращення безпеки медичних даних, прозорості в управлінні постачанням медикаментів, а також підвищення ефективності медичних послуг. Однак для успішного впровадження цієї технології необхідно подолати низку технічних, правових і фінансових викликів. При належній підтримці з боку держави, міжнародній співпраці та підготовці кадрів, блокчейн може стати важливим інструментом для модернізації медичної системи України.

Таким чином, впровадження блокчейн-технологій в українську медицину вимагатиме комплексного підходу, поетапного впровадження та тісної співпраці між державними органами, медичними установами та IT-компаніями. Ретельно продумана стратегії та підтримка з боку усіх учасників процесу дозволять значно покращити ефективність та безпеку медичних послуг в Україні.