Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:

ДОСЛІДЖЕННЯ МЕТОДІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЦІЛІСНОСТІ ДАНИХ В МЕРЕЖАХ

Виконав

студент групи БІКСм-1-24-1.4д

Кордилевський Макарій Станіславович
(прізвище, ім’я, по батькові)

_____
(підпис)

Науковий керівник
к.в.н, доцент

Аносов Андрій Олександрович

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Кордилевському Макарію Станіславовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів та розробка рекомендацій щодо застосування технології блокчейну для забезпечення безпеки та цілісності даних в мережах;

   керівник: Аносов Андрій Олександрович,

   затверджені наказом ректора від «___»____ 20___ року №__.
2. Термін подання студентом роботи «___»_____ 20___ р.
3. Вихідні дані до роботи:
   3.1 науково-технічна та нормативна література з теми дослідження;
   3.2 методи: системний аналіз, порівняльний аналіз;
4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):
   4.1 Проаналізувати теоретичні основи технології блокчейн, типи блокчейн-мереж та механізми консенсусу;
   4.2 Дослідити проблеми забезпечення цілісності даних у сучасних мережах та обмеження традиційних методів захисту;
   4.3 Систематизувати існуючі блокчейн-платформи та проаналізувати їх можливості для корпоративних застосувань;
   4.4 Сформувати критерії вибору блокчейн-платформи для забезпечення цілісності критичних даних;
   4.5 Провести порівняльний аналіз блокчейн-платформ та обґрунтувати вибір оптимального рішення;
   4.6 Розробити концептуальну архітектуру системи та практичні рекомендації щодо впровадження.
5. Перелік графічного матеріалу:
   5.1 Презентація доповіді, виконана в Microsoft PowerPoint.
6. Дата видачі завдання «___»_____ 20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання		
2.	Аналіз літератури		
3.	Обґрунтування вибору рішення		
4.	Збір даних		
5.	Виконання та оформлення розділу 1.		
6.	Виконання та оформлення розділу 2.		
7.	Виконання та оформлення розділу 3.		
8.	Вступ, висновки, реферат		
9.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції		
10.	Оформлення та друк текстової частини роботи		
11.	Оформлення презентацій		
12.	Отримання рецензій		
13.	Попередній захист роботи		
14.	Захист в ЕК		

Студент _____ _____
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ _____
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів та розробці рекомендацій щодо застосування технології блокчейну для забезпечення безпеки та цілісності даних в мережах.

Робота складається зі вступу, 3 розділів, що містять 16 рисунків та 15 таблиць, висновків та списку використаних джерел, що містить 338 найменувань. Загальний обсяг роботи становить 121 сторінок, з яких 4 сторінок займають ілюстрації і таблиці на окремих аркушах, а також додатки, перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження є процеси забезпечення безпеки та цілісності даних у корпоративних мережах з використанням технології блокчейн.

Предметом дослідження є методи та засоби застосування технології блокчейн для захисту даних від несанкціонованої модифікації, забезпечення прозорості операцій та протидії внутрішнім загрозам в інформаційних системах.

Метою роботи є дослідження методів застосування технології блокчейн для забезпечення безпеки та цілісності даних у мережах, а також розробка практичних рекомендацій щодо вибору та впровадження блокчейн-рішень на прикладі інформаційної системи медичної установи.

Наукова новизна одержаних результатів полягає в тому, що в роботі систематизовано критерії вибору блокчейн-платформи для забезпечення цілісності даних у корпоративних мережах, проведено комплексний порівняльний аналіз блокчейн-платформ з урахуванням вимог до конфіденційності, продуктивності та антикорупційного потенціалу, обґрунтовано переваги платформи Hyperledger Fabric для корпоративних застосувань, розроблено рекомендації щодо інтеграції блокчейн-рішень з існуючими інформаційними системами.

Галузь застосування. Запропоновані методи та рекомендації можуть бути використані організаціями різних галузей при прийнятті рішень щодо впровадження блокчейн-технологій для забезпечення цілісності критичних даних, підвищення прозорості операцій та протидії внутрішнім загрозам в інформаційних системах.

Ключові слова: БЛОКЧЕЙН, ЦІЛІСНІСТЬ ДАНИХ, ІНФОРМАЦІЙНА БЕЗПЕКА, БЕЗПЕКА МЕРЕЖ, HYPERLEDGER FABRIC, СМАРТ-КОНТРАКТИ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, РОЗПОДІЛЕНИЙ РЕЄСТР, МЕХАНІЗМИ КОНСЕНСУСУ, ЗАХИСТ ІНФОРМАЦІЇ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ – Інформаційна безпека

РД – Розподілений реєстр

DLT – (Distributed Ledger Technology) Технологія розподіленого реєстру

PoW – (Proof of Work) Доказ виконаної роботи

PoS – (Proof of Stake) Доказ частки володіння

PBFT – (Practical Byzantine Fault Tolerance) Практична візантійська відмовостійкість

DPoS – (Delegated Proof of Stake) Делегований доказ частки

PoA – (Proof of Authority) Доказ повноважень

PoH – (Proof of History) Доказ історії

PoET – (Proof of Elapsed Time) Доказ минулого часу

SHA-256 – (Secure Hash Algorithm 256-bit) Алгоритм безпечного хешування 256-біт

Keccak-256 – Алгоритм хешування Keccak 256-біт

ECC – (Elliptic Curve Cryptography) Криптографія на еліптичних кривих

RSA – (Rivest-Shamir-Adleman) Алгоритм шифрування Рівеста-Шаміра-Адлемана

ECDSA – (Elliptic Curve Digital Signature Algorithm) Алгоритм цифрового підпису на еліптичних кривих

AES-256 – (Advanced Encryption Standard 256-bit) Розширений стандарт шифрування 256-біт

TLS – (Transport Layer Security) Безпека транспортного рівня

PKI – (Public Key Infrastructure) Інфраструктура відкритих ключів

CA – (Certificate Authority) Центр сертифікації

EVM – (Ethereum Virtual Machine) Віртуальна машина Ethereum

dApp – (Decentralized Application) Децентралізований додаток

API – (Application Programming Interface) Інтерфейс програмування додатків

SDK – (Software Development Kit) Набір засобів розробки програмного забезпечення

JSON – (JavaScript Object Notation) Нотація об'єктів JavaScript

XML – (Extensible Markup Language) Розширювана мова розмітки

REST – (Representational State Transfer) Передача репрезентативного стану

HTTP – (Hypertext Transfer Protocol) Протокол передачі гіпертексту

SQL – (Structured Query Language) Мова структурованих запитів

ЛІС – Лабораторна інформаційна система

МІС – Медична інформаційна система

РІС – Радіологічна інформаційна система

ЕМК – Електронна медична картка

eHealth – Електронна система охорони здоров'я

HL7 – (Health Level Seven) Стандарт обміну медичними даними сьомого рівня

FHIR – (Fast Healthcare Interoperability Resources) Швидкі ресурси взаємодії в охороні здоров'я

DICOM – (Digital Imaging and Communications in Medicine) Цифрові зображення та комунікації в медицині

PACS – (Picture Archiving and Communication System) Система архівування та передачі зображень

HIPAA – (Health Insurance Portability and Accountability Act) Закон про переносимість і підзвітність медичного страхування

GDPR – (General Data Protection Regulation) Загальний регламент захисту даних

DPIA – (Data Protection Impact Assessment) Оцінка впливу на захист даних

RBAC – (Role-Based Access Control) Контроль доступу на основі ролей

ABAC – (Attribute-Based Access Control) Контроль доступу на основі атрибутів

ACE – (Attribute-Based Credentials for Ethereum) Облікові дані на основі атрибутів для Ethereum

MSP – (Membership Service Provider) Постачальник служби членства

PDC – (Private Data Collection) Колекція приватних даних

КЕП – Кваліфікований електронний підпис

ISO/IEC – (International Organization for Standardization / International Electrotechnical Commission) Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія

ДСТУ – Державні стандарти України

NIST – (National Institute of Standards and Technology) Національний інститут стандартів і технології

ENISA – (European Union Agency for Cybersecurity) Агентство Європейського Союзу з кібербезпеки

КМУ – Кабінет Міністрів України

ЄС – Європейський Союз

EU – (European Union) Європейський Союз

DeFi – (Decentralized Finance) Децентралізовані фінанси

NFT – (Non-Fungible Token) Невзаємозамінний токен

IBC – (Inter-Blockchain Communication) Міжблокчейнова комунікація

SSI – (Self-Sovereign Identity) Самостійна ідентичність

ПО – Програмне забезпечення

IoT – (Internet of Things) Інтернет речей

AWS – (Amazon Web Services) Веб-сервіси Amazon

S3 – (Simple Storage Service) Проста служба зберігання

CAPEX – (Capital Expenditure) Капітальні витрати

OPEX – (Operational Expenditure) Операційні витрати

CPU – (Central Processing Unit) Центральний процесор

RAM – (Random Access Memory) Оперативна пам'ять

SSD – (Solid State Drive) Твердотільний накопичувач

GB – (Gigabyte) Гігабайт

PDF – (Portable Document Format) Портативний формат документів

EEA – (Enterprise Ethereum Alliance) Альянс корпоративного Ethereum

HSD – (Hyperledger Software Development) Розробка програмного забезпечення Hyperledger

ATOM – Криптовалюта мережі Cosmos

CBDC – (Central Bank Digital Currency) Цифрова валюта центрального банку

ВСТУП

Проблема захисту інформації та забезпечення цілісності даних супроводжує людство протягом усієї його історії. Від глиняних табличок Месопотамії, які зберігали торгові записи та державні акти, до середньовічних архівів із сургучними печатками та підписами нотаріусів - люди завжди шукали способи захистити важливу інформацію від підробки, несанкціонованого доступу та випадкового знищення. Кожна епоха створювала власні механізми довіри: особисті печатки королів, нотаріальне засвідчення документів, банківські сейфи та державні реєстри.

Цифрова революція кінця XX - початку XXI століття кардинально змінила підходи до зберігання та обробки інформації. Перехід від паперових носіїв до електронних баз даних відкрив безпрецедентні можливості для обміну інформацією, проте водночас створив нові, раніше невідомі загрози. Централізовані системи зберігання даних, попри всі технічні засоби захисту, виявилися вразливими до кібератак, внутрішніх зловживань та корупційних маніпуляцій. Адміністратор бази даних, який має необмежений доступ до системи, технічно здатен модифікувати будь-які записи, включаючи журнали аудиту власних дій.

Революційним рішенням цієї фундаментальної проблеми стала технологія блокчейн, концепція якої була запропонована у 2008 році невідомим автором під псевдонімом Сатоші Накамото. Вперше в історії людства з'явилася можливість створювати розподілені реєстри, де жоден учасник системи не має можливості одноосібно змінити записані дані. Незмінність записів забезпечується не адміністративними заходами чи довірою до окремих осіб, а математичними алгоритмами криптографії та механізмами консенсусу.

Актуальність теми. За даними дослідження компанії IBM Security [1], середня вартість витоку даних у 2024 році досягла рекордних 4,88 мільйона доларів США, що на 10% більше порівняно з попереднім роком. Особливо вразливою виявилася сфера охорони здоров'я, де середня вартість одного інциденту становить 9,77 мільйона доларів - найвищий показник серед усіх галузей протягом 14 років поспіль. При цьому 35% інцидентів пов'язані з внутрішніми загрозами - діями

співробітників організації, які мають легітимний доступ до систем.

Згідно зі звітом Transparency International [2], Україна посідає 104 місце зі 180 країн за індексом сприйняття корупції, що свідчить про високий рівень корупційних ризиків у державних та приватних установах. Медична сфера залишається однією з найбільш корумпованих галузей: підробка медичних довідок, незаконний продаж персональних даних пацієнтів, маніпуляції з документацією закупівель - ці явища завдають значної шкоди як окремим громадянам, так і суспільству загалом.

Дослідження ринку блокчейн-технологій компанією Grand View Research [3] прогнозує зростання глобального ринку блокчейн з 17,46 мільярда доларів у 2023 році до 825,93 мільярда доларів до 2032 року із середньорічним темпом зростання (CAGR) 52,8%. Сектор охорони здоров'я визначено як один із найперспективніших напрямів застосування технології, оскільки блокчейн здатен вирішити критичні проблеми галузі: забезпечити цілісність медичних записів, прозорість ланцюгів постачання медикаментів та захист персональних даних пацієнтів.

Більшість організацій, що працюють з критичними даними, стикаються з низкою системних проблем:

- неможливість гарантувати незмінність записів у централізованих базах даних;
- вразливість до інсайдерських загроз та зловживань з боку привілейованих користувачів;
- відсутність прозорих механізмів аудиту, захищених від маніпуляцій;
- складність забезпечення відповідності вимогам регуляторів щодо захисту персональних даних;
- недостатня інтероперабельність між різними інформаційними системами.
- Вищеперелічене підтверджує актуальність дослідження методів застосування технології блокчейн для забезпечення безпеки та цілісності даних у мережах.

Мета роботи полягає у дослідженні методів застосування технології блокчейн для забезпечення безпеки та цілісності даних у мережах, а також розробці

практичних рекомендацій щодо вибору та впровадження блокчейн-рішень. Для досягнення цієї мети в роботі необхідно вирішити такі завдання:

- проаналізувати теоретичні основи технології блокчейн, типи блокчейн-мереж та механізми консенсусу;
- дослідити проблеми забезпечення цілісності даних у сучасних мережах та обмеження традиційних методів захисту;
- систематизувати існуючі блокчейн-платформи та проаналізувати їх можливості для корпоративних застосувань;
- сформувати критерії вибору блокчейн-платформи для забезпечення цілісності критичних даних;
- провести порівняльний аналіз блокчейн-платформ та обґрунтувати вибір оптимального рішення;
- розробити концептуальну архітектуру системи та практичні рекомендації щодо впровадження.

Виходячи з цього**, об'єктом дослідження** є процеси забезпечення безпеки та цілісності даних у корпоративних мережах з використанням технології блокчейн. Предметом дослідження є методи та засоби застосування технології блокчейн для захисту даних від несанкціонованої модифікації, забезпечення прозорості операцій та протидії внутрішнім загрозам в інформаційних системах. Як практичний приклад для апробації запропонованих методів обрано інформаційну систему приватної медичної установи України.

Методи дослідження. Для вирішення поставлених завдань використано комплекс методів: аналіз та синтез - для дослідження теоретичних основ блокчейн-технології; порівняльний аналіз - для оцінювання блокчейн-платформ за визначеними критеріями; системний підхід - для розробки архітектури запропонованого рішення; методи оцінки ризиків за стандартами ISO/IEC 27005:2022 та ДСТУ ISO/IEC 27002 - для аналізу загроз інформаційній безпеці.

Наукова новизна одержаних результатів. Наукова новизна полягає у систематизації критеріїв вибору блокчейн-платформи для забезпечення цілісності даних у корпоративних мережах з урахуванням антикорупційного потенціалу

технології; проведенні комплексного порівняльного аналізу блокчейн-платформ Bitcoin, Ethereum та Hyperledger Fabric у контексті вимог до конфіденційності, продуктивності та регуляторної відповідності; обґрунтуванні переваг платформи Hyperledger Fabric для корпоративних застосувань та розробці рекомендацій щодо інтеграції блокчейн-рішень з існуючими інформаційними системами.

Теоретичне та практичне значення полягає в обґрунтуванні доцільності використання блокчейн-технологій для вирішення проблем централізованих систем зберігання даних, розробці методичних рекомендацій щодо вибору блокчейн-платформи та архітектурних рішень для забезпечення цілісності критичних даних в умовах підвищених корупційних ризиків.

Галузь застосування. Результати роботи можуть бути використані організаціями різних галузей - медичними установами, фінансовими організаціями, державними органами та підприємствами - при прийнятті рішень щодо впровадження блокчейн-технологій для забезпечення цілісності даних, підвищення прозорості операцій та протидії внутрішнім загрозам, а також як матеріал для використання у навчальному процесі закладів вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації».

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

У тезах «Збірнику тез конференції «Безпека інформаційно-комунікаційних систем - 2025»»

https://fitm.kubg.edu.ua/informatsiya/naukova-diialnist/konferentsii-fakultetu/2646-bezpeka-informatsiino-komunikatsiinykh-system.html

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ

1.1. Основи технології блокчейн

1.1.1. Що таке блокчейн? Базове визначення

Сучасний цифровий світ переживає справжню трансформацію підходів до зберігання та передачі інформації. Одним із найбільш революційних технологічних рішень останнього десятиліття стала технологія блокчейн, яка докорінно змінює уявлення про довіру в цифрових системах. За своєю суттю, блокчейн являє собою розподілену базу даних, що складається з безперервного ланцюжка блоків, кожен з яких містить певну інформацію та криптографічно пов'язаний із попереднім [1].

Якщо говорити простіше, то блокчейн можна порівняти з величезною книгою записів, копії якої одночасно зберігаються на тисячах або навіть мільйонах комп'ютерів по всьому світу. Кожен новий запис додається на нову сторінку (блок), а сторінки скріплюються між собою таким чином, що змінити будь-яку з них, не порушивши цілісності всієї книги, практично неможливо. Саме ця особливість робить технологію надзвичайно привабливою для забезпечення безпеки даних.

Історія блокчейну бере свій початок у 2008 році, коли невідома особа або група осіб під псевдонімом Сатоші Накамото опублікувала документ під назвою «Bitcoin: A Peer-to-Peer Electronic Cash System» [2]. У цій роботі було описано принципово нову архітектуру для створення децентралізованої електронної грошової системи. Проте з часом стало зрозуміло, що потенціал блокчейну виходить далеко за межі криптовалют і охоплює практично будь-які сфери, де важливі прозорість, безпека та незмінність записів.

На технічному рівні блокчейн функціонує як однорангова (peer-to-peer) мережа, де кожен учасник (вузол) має рівні права та зберігає повну або часткову копію всього ланцюжка даних. Відсутність центрального сервера чи адміністратора означає, що жоден окремий суб'єкт не контролює систему повністю, а рішення приймаються колективно за допомогою спеціальних алгоритмів консенсусу.

1.1.2. Ключові властивості блокчейну

Розуміння фундаментальних властивостей блокчейну має критичне значення для оцінки його придатності до вирішення конкретних завдань інформаційної безпеки. Серед основних характеристик цієї технології варто виділити чотири ключові: децентралізацію, незмінність, прозорість та криптографічну захищеність [3].

Децентралізація є, мабуть, найбільш визначальною рисою блокчейну. На відміну від традиційних баз даних, де існує єдиний центр управління та зберігання інформації, блокчейн розподіляє ці функції між усіма учасниками мережі. Така архітектура усуває так звану «єдину точку відмови» (single point of failure), адже навіть якщо частина вузлів вийде з ладу або буде скомпрометована, мережа продовжить функціонувати. Крім того, децентралізація знижує ризики цензури та несанкціонованого втручання, оскільки для маніпуляції даними зловмиснику довелося б контролювати значну частину всієї мережі.

Незмінність (immutability) даних забезпечується завдяки криптографічному зв'язку між блоками. Кожен блок містить хеш попереднього, тому будь-яка спроба змінити інформацію в одному з блоків призведе до зміни його хешу, що автоматично розірве ланцюжок і буде негайно виявлено іншими учасниками мережі. Ця властивість робить блокчейн ідеальним інструментом для створення аудиторських журналів та систем, де важливо гарантувати, що дані не були підроблені після їх запису.

Прозорість проявляється в тому, що всі транзакції є видимими для учасників мережі. У публічних блокчейнах кожен може переглянути історію всіх операцій від самого початку існування системи. Звичайно, ступінь прозорості може варіюватися залежно від типу мережі - приватні блокчейни можуть обмежувати доступ до інформації, однак принцип відкритості для авторизованих учасників залишається незмінним.

Криптографічна захищеність базується на використанні сучасних криптографічних примітивів: хеш-функцій, асиметричної криптографії та цифрових підписів.

1.1.3. Як працює блокчейн? Покрокове пояснення

Процес додавання нової інформації до блокчейну складається з кількох послідовних етапів, кожен з яких має критичне значення для забезпечення безпеки та цілісності всієї системи [4].

На першому етапі користувач ініціює транзакцію - це може бути передача криптовалюти, реєстрація документа, зміна стану смарт-контракту або будь-яка інша операція, передбачена конкретною блокчейн-платформою. Транзакція підписується приватним ключем ініціатора, що засвідчує його особу та дозволяє в майбутньому верифікувати авторство операції.

Підписана транзакція розповсюджується по мережі та потрапляє до так званого «пулу очікування» (mempool), де накопичуються транзакції, які ще не були включені до блоку. Спеціальні вузли мережі - майнери або валідатори, залежно від механізму консенсусу - відбирають транзакції з пулу та формують з них новий блок.

Рис. 1.1 «Покрокова діаграма процесу додавання транзакції до блокчейну: від створення транзакції через валідацію до включення в блок»

Після формування блоку настає етап досягнення консенсусу. Мережа повинна колективно погодитися з тим, що новий блок є валідним і може бути доданий до ланцюжка. Конкретний механізм цього процесу залежить від протоколу - це може бути доказ виконаної роботи (Proof of Work), доказ частки (Proof of Stake) або один із багатьох інших алгоритмів консенсусу.

Коли консенсус досягнуто, новий блок криптографічно зв'язується з попереднім шляхом включення хешу останнього блоку до заголовка нового. Оновлений ланцюжок розповсюджується по всій мережі, і кожен вузол додає новий блок до своєї локальної копії бази даних. З цього моменту транзакції, включені до блоку, вважаються підтвердженими та стають частиною незмінної історії.

1.1.4. Структура блоку

Кожен блок у блокчейні має чітко визначену внутрішню структуру, розуміння якої допомагає глибше усвідомити механізми забезпечення безпеки цієї технології. Загалом блок складається з двох основних компонентів: заголовка (header) та тіла (body) [5].

Заголовок блоку містить метадані, необхідні для підтримання цілісності ланцюжка:

- Хеш попереднього блоку - це криптографічний відбиток заголовка попереднього блоку, який створює нерозривний зв'язок між усіма елементами ланцюжка. Саме цей компонент забезпечує властивість незмінності, оскільки зміна будь-якого блоку вимагала б перерахунку хешів усіх наступних блоків.
- Корінь дерева Меркла (Merkle Root) - це єдиний хеш, який узагальнює всі транзакції, включені до блоку. Він обчислюється шляхом послідовного хешування пар транзакцій до отримання одного кореневого значення. Така структура дозволяє ефективно перевіряти наявність конкретної транзакції без необхідності завантаження всього блоку.
- Мітка часу (timestamp) фіксує приблизний час створення блоку. Хоча точність цієї мітки може варіюватися, вона забезпечує хронологічне впорядкування подій у мережі.

— Nonce - випадкове число, яке використовується в алгоритмах типу Proof of Work для знаходження хешу, що відповідає заданим критеріям складності.

— Цільова складність (difficulty target) визначає вимоги до хешу блоку, які повинен виконати майнер для успішного додавання блоку до ланцюжка.

Тіло блоку містить власне корисне навантаження - список транзакцій, які були включені до цього блоку. Кількість транзакцій обмежується розміром блоку, який різниться залежно від конкретної платформи. Наприклад, у Bitcoin максимальний розмір блоку становить близько 1-4 МБ, тоді як Ethereum використовує динамічний ліміт на основі витраченого газу.

Рис. 1.2 «Структури блоку з візуалізацією заголовка (хеш попереднього блоку, Merkle Root, timestamp, nonce) та тіла (список транзакцій)»

Таблиця 1.3

Основні компоненти структури блоку

Компонент	**Розташування**	**Призначення**	**Типовий розмір**
Хеш попереднього блоку	Заголовок	Зв'язок з попереднім блоком	32 байти
Корінь Меркла	Заголовок	Узагальнення всіх транзакцій	32 байти
Мітка часу	Заголовок	Фіксація часу створення	4 байти
Nonce	Заголовок	Вирішення задачі PoW	4 байти
Номер версії	Заголовок	Ідентифікація протоколу	4 байти
Транзакції	Тіло	Корисне навантаження	Змінний

1.1.5. Криптографічні основи блокчейну

Безпека блокчейну нерозривно пов'язана з криптографічними методами, які лежать в його основі. Без надійної криптографії вся концепція розподіленого реєстру втратила б сенс, адже саме вона забезпечує цілісність даних, автентифікацію учасників та захист від несанкціонованих модифікацій [6].

Хеш-функції відіграють центральну роль у функціонуванні блокчейну. Криптографічна хеш-функція - це математичний алгоритм, який перетворює вхідні дані довільної довжини на вихідне значення фіксованого розміру (хеш або дайджест). Для застосування в блокчейні хеш-функція повинна мати кілька критичних властивостей:

— Детермінованість - однакові вхідні дані завжди дають однаковий результат.

— Односторонність - за хешем практично неможливо відновити вихідні дані.

— Стійкість до колізій - надзвичайно складно знайти два різні набори даних з однаковим хешем.

— Лавинний ефект - незначна зміна вхідних даних кардинально змінює вихідний хеш.

Найпоширенішою хеш-функцією в блокчейн-системах є SHA-256 (Secure Hash Algorithm 256-bit), розроблена Національним інститутом стандартів і технологій США. Вона використовується, зокрема, у Bitcoin та багатьох інших платформах. Ethereum застосовує модифікований варіант під назвою Keccak-256 [7].

Асиметрична криптографія (криптографія з відкритим ключем) забезпечує механізм ідентифікації учасників мережі та підтвердження авторства транзакцій. Кожен користувач блокчейну володіє парою математично пов'язаних ключів:

— Приватний ключ - секретне число, яке повинно зберігатися в абсолютній таємниці. Він використовується для підписування транзакцій та є, по суті, єдиним доказом права власності на активи в блокчейні.

— Публічний ключ - похідне значення, яке можна вільно розповсюджувати. На його основі формується адреса користувача в мережі, а також здійснюється верифікація цифрових підписів.

Більшість блокчейн-платформ використовують криптографію на еліптичних кривих (Elliptic Curve Cryptography, ECC), зокрема криву secp256k1. Порівняно з традиційним алгоритмом RSA, ECC забезпечує аналогічний рівень безпеки при значно менших розмірах ключів, що критично важливо для ефективності розподілених систем [8].

Цифрові підписи створюються шляхом хешування повідомлення та шифрування отриманого хешу приватним ключем відправника. Одержувач може перевірити підпис, використовуючи публічний ключ підписувача - якщо розшифрований хеш збігається з хешем отриманого повідомлення, підпис вважається дійсним. Цей механізм гарантує дві важливі властивості: автентичність (повідомлення справді походить від заявленого відправника) та цілісність (повідомлення не було змінено після підписання).

Дерево Меркла (Merkle Tree) - це структура даних, яка дозволяє ефективно та безпечно верифікувати вміст великих масивів даних. Воно будується знизу вгору: спочатку хешуються окремі транзакції (листя дерева), потім хеші об'єднуються попарно та хешуються знову, і так до отримання єдиного кореневого хешу (Merkle Root).

Рис. 1.4 «Візуалізація дерева Меркла: піраміда з хешами транзакцій на нижньому рівні, проміжними хешами посередині та кореневим хешем на вершині»

Перевага цієї структури полягає в можливості так званого «спрощеного підтвердження платежу» (Simplified Payment Verification, SPV). Для доведення включення конкретної транзакції до блоку не потрібно завантажувати весь блок - достатньо надати лише «шлях Меркла», тобто ланцюжок хешів від транзакції до кореня. Це особливо важливо для легких клієнтів, що працюють на пристроях з обмеженими ресурсами.

1.2. Типи блокчейн-мереж

1.2.1. Публічні блокчейни (Public/Permissionless)

Публічні блокчейни втілюють початкову філософію технології, закладену ще в оригінальному документі Накамото - повну відкритість та відсутність централізованого контролю. У таких мережах будь-хто може стати учасником без попередньої реєстрації чи отримання дозволу: читати дані, надсилати транзакції та навіть брати участь у процесі валідації блоків [9].

Яскравими прикладами публічних блокчейнів є Bitcoin та Ethereum. Ці мережі функціонують на основі економічних стимулів - учасники, які підтримують інфраструктуру (майнери або валідатори), отримують винагороду у вигляді криптовалюти за свою роботу. Така модель забезпечує стійкість системи без необхідності довіри до будь-якого центрального органу.

Основні переваги публічних блокчейнів включають максимальну децентралізацію, стійкість до цензури та високий рівень прозорості. Водночас вони мають суттєві обмеження: низьку пропускну здатність (Bitcoin обробляє лише 7-10 транзакцій на секунду), високе споживання енергії для мереж на базі Proof of Work, а також потенційні проблеми з конфіденційністю, оскільки всі транзакції є публічно доступними.

Для корпоративних застосувань публічні блокчейни часто виявляються надто повільними та недостатньо контрольованими. Проте вони залишаються оптимальним вибором для сценаріїв, де важлива максимальна відкритість та незалежність від будь-яких організацій.

1.2.2. Приватні блокчейни (Private/Permissioned)

На протилежному кінці спектру розташовані приватні блокчейни, які функціонують під контролем єдиної організації. Доступ до таких мереж суворо обмежений - читати дані, надсилати транзакції та брати участь у валідації можуть лише авторизовані користувачі [10].

Приватний блокчейн можна уявити як внутрішню корпоративну базу даних, яка використовує блокчейн-архітектуру для забезпечення незмінності та аудиторського сліду. Типовими прикладами є Hyperledger Fabric у приватній

конфігурації або Corda для специфічних бізнес-процесів.

Основні переваги цього типу мереж - висока швидкість транзакцій (тисячі операцій на секунду), повний контроль над правами доступу та можливість швидкого внесення змін до протоколу. Організація-оператор визначає, хто може бути валідатором, які дані є видимими для різних категорій користувачів та як вирішуються суперечки.

Однак приватні блокчейни частково жертвують ключовими перевагами технології. Централізований контроль означає наявність єдиної точки довіри, а отже, й потенційної точки відмови. Крім того, оператор теоретично може змінювати або видаляти дані, що підриває концепцію незмінності. Критики іноді називають приватні блокчейни «розподіленими базами даних із зайвими ускладненнями», ставлячи під сумнів доцільність їх використання порівняно з традиційними рішеннями.

1.2.3. Консорціумні блокчейни (Consortium/Federated)

Консорціумні блокчейни займають проміжну позицію між публічними та приватними варіантами. Контроль над такою мережею розподілений між групою попередньо визначених організацій, які спільно відповідають за валідацію транзакцій та підтримку інфраструктури [11].

Ця модель особливо добре підходить для галузей, де кілька конкуруючих компаній мають спільний інтерес у підтриманні єдиного джерела правди, але жодна з них не готова довірити контроль одному учаснику. Показовими прикладами є банківські консорціуми для міжбанківських розрахунків, мережі для відстеження ланцюгів постачання або платформи для обміну медичними даними між клініками.

До переваг консорціумних блокчейнів належать баланс між ефективністю та децентралізацією, швидше досягнення консенсусу порівняно з публічними мережами, а також збереження певного рівня розподілу довіри. Кілька незалежних валідаторів забезпечують взаємний контроль, унеможливлюючи односторонні маніпуляції.

Серед недоліків варто відзначити складність координації між учасниками консорціуму - питання управління, розподілу витрат та вирішення конфліктів

можуть суттєво ускладнювати впровадження. Крім того, консорціумні мережі все ще є менш децентралізованими, ніж публічні, що робить їх вразливими до змови між валідаторами.

1.2.4. Гібридні блокчейни

Гібридні блокчейни намагаються поєднати найкращі характеристики приватних та публічних мереж в єдиній архітектурі. Такі системи зазвичай мають приватний рівень для конфіденційних операцій та публічний рівень для забезпечення прозорості й незмінності критичних даних [12].

Типовий сценарій використання гібридного блокчейну може виглядати наступним чином: організація веде внутрішній облік у приватній мережі, де швидкість та конфіденційність є пріоритетами, але періодично «якорить» хеші своїх внутрішніх блоків до публічного блокчейну (наприклад, Bitcoin або Ethereum). Це дозволяє отримати незалежне підтвердження часу та цілісності даних без розкриття їх змісту.

Перевагами гібридного підходу є гнучкість у налаштуванні рівнів доступу, можливість масштабування приватного рівня без обмежень публічних мереж, а також отримання переваг обох моделей. Водночас гібридні архітектури складніші у проектуванні та підтримці, вимагають ретельного продумування взаємодії між рівнями та можуть створювати додаткові вектори атак.

1.2.5. Порівняльна таблиця типів блокчейнів

Для систематизації розглянутих характеристик різних типів блокчейн-мереж доцільно подати їх у вигляді порівняльної таблиці, що дозволить наочно продемонструвати ключові відмінності.

Таблиця 1.5

Порівняльна характеристика типів блокчейн-мереж

Характеристика	**Публічний**	**Приватний**	**Консорціумний**	**Гібридний**
Доступ до читання	Відкритий для всіх	Обмежений	Обмежений або частково відкритий	Налаштовується
Право на запис	Відкрите	Обмежене	Обмежене	Налаштовується

Валідація блоків	Будь-який учасник	Оператор мережі	Члени консорціуму	Комбіноване
Швидкість транзакцій	Низька (7-30 TPS)	Висока (1000+ TPS)	Середня-висока (100-1000 TPS)	Залежить від конфігурації
Рівень децентралізації	Максимальний	Мінімальний	Середній	Середній
Енергоспоживання	Високе (PoW)	Низьке	Низьке	Залежить від конфігурації
Прозорість	Повна	Обмежена	Часткова	Гнучка
Приватність	Низька	Висока	Середня-висока	Налаштовується
Типові приклади	Bitcoin, Ethereum	Hyperledger Fabric	R3 Corda, Quorum	Dragonchain
Сфери застосування	Криптовалюти, DeFi	Корпоративні системи	Міжгалузева взаємодія	Комплексні рішення

Вибір конкретного типу блокчейну залежить від специфіки завдання, вимог до продуктивності, рівня довіри між учасниками та регуляторних обмежень. Не існує універсально найкращого варіанту - кожен тип має свої сильні сторони та обмеження, які необхідно враховувати при проектуванні системи.

1.3. Механізми консенсусу

1.3.1. Що таке консенсус і навіщо він потрібен?

Консенсус у контексті розподілених систем - це процес досягнення згоди між учасниками мережі щодо поточного стану спільної бази даних. У традиційних централізованих системах це питання не виникає: єдиний сервер визначає, яка інформація є правильною, і всі клієнти довіряють його рішенням. Проте в децентралізованих мережах, де немає центрального арбітра, необхідний механізм для координації дій незалежних вузлів [13]

Проблема досягнення консенсусу в розподілених системах далеко не тривіальна. Вона тісно пов'язана з так званою «задачею візантійських генералів» - класичною проблемою комп'ютерних наук, сформульованою Леслі Лампортом у 1982 році. Задача описує ситуацію, коли група учасників повинна координувати свої дії, при цьому деякі з них можуть бути зрадниками та свідомо передавати хибну інформацію.

Блокчейн-системи вирішують цю проблему за допомогою спеціальних алгоритмів консенсусу, які забезпечують узгодженість даних навіть за наявності недобросовісних учасників. Ідеальний механізм консенсусу повинен гарантувати:

— Узгодженість - усі чесні вузли погоджуються з однаковим станом реєстру.

— Живучість - система продовжує функціонувати та обробляти нові транзакції.

— Стійкість до атак - зловмисники не можуть нав'язати хибний стан мережі.

— Децентралізацію - жоден окремий учасник не контролює процес.

На практиці різні алгоритми консенсусу по-різному балансують між цими вимогами, жертвуючи одними характеристиками заради покращення інших.

1.3.2. Proof of Work (PoW) – доказ виконаної роботи

Proof of Work став першим механізмом консенсусу, успішно застосованим у масштабній децентралізованій системі - саме він лежить в основі Bitcoin та став моделлю для багатьох наступних криптовалют. Концептуально PoW вимагає від учасників, що претендують на створення нового блоку, виконати певну обчислювальну роботу, яка потребує значних ресурсів, але результат якої легко перевірити [14].

Рис. 1.6 «Процес майнінгу в PoW: майнер перебирає значення nonce, поки не знайде хеш, що задовольняє умову складності»

Технічно це реалізується через пошук числа nonce, при якому хеш заголовка блоку буде меншим за визначене цільове значення. Оскільки хеш-функції є односторонніми, єдиний спосіб знайти відповідний nonce - це перебирати варіанти, поки не буде отримано допустимий результат. Складність цієї задачі автоматично регулюється протоколом для підтримання заданого часу генерації блоку (близько 10 хвилин для Bitcoin).

Безпека PoW базується на тому, що чесні майнери колективно контролюють більшість обчислювальної потужності мережі. Для успішної атаки зловмиснику довелося б перевершити цю потужність, що вимагає колосальних інвестицій в обладнання та електроенергію. Знамените «правило 51%» означає, що атакуючий, який контролює більше половини хешрейту мережі, теоретично може переписувати історію транзакцій.

Головним недоліком PoW є енергоспоживання. За різними оцінками, мережа Bitcoin споживає електроенергію на рівні невеликої країни - близько 120-150 ТВт·год на рік. Це викликає обґрунтовану критику з екологічних позицій та обмежує масштабованість системи. Крім того, поступова централізація майнінгу у

великих пулах та регіонах з дешевою електроенергією підриває початкову ідею децентралізації.

1.3.3. Proof of Stake (PoS) – доказ частки

Proof of Stake виник як альтернатива енергоємному PoW, пропонуючи принципово інший підхід до вибору валідаторів блоків. Замість конкуренції обчислювальною потужністю, PoS використовує економічні стимули - право на створення блоку надається пропорційно до кількості криптовалюти, яку учасник «заморозив» як заставу (стейк) [15].

Логіка PoS полягає в тому, що учасники з великою часткою в мережі найбільше зацікавлені в її коректному функціонуванні. Спроба маніпуляції призведе до втрати застави та знецінення їхніх активів. Валідатори обираються за псевдовипадковим алгоритмом, де ймовірність вибору зростає зі збільшенням стейку, але не є детерміністичною.

Найбільш знаковою подією для PoS став перехід Ethereum з Proof of Work у вересні 2022 року (так званий «The Merge»). Ця міграція зменшила енергоспоживання мережі приблизно на 99,95%, продемонструвавши життєздатність PoS для великих публічних блокчейнів [16].

Переваги PoS включають радикальне зниження енергоспоживання, нижчий поріг входу для валідаторів (не потрібно дороге обладнання) та теоретично кращу децентралізацію. Водночас критики вказують на ризик «багатіють ще більше багаті» (large stakers отримують непропорційно більше винагороди), а також на складніші моделі безпеки порівняно з простотою PoW.

1.3.4. Practical Byzantine Fault Tolerance (PBFT)

PBFT (Практична візантійська відмовостійкість) - це класичний алгоритм консенсусу, адаптований для блокчейн-систем, особливо для приватних та консорціумних мереж. На відміну від імовірнісних механізмів на кшталт PoW, PBFT забезпечує детерміністичну фіналізацію - щойно блок підтверджено, він гарантовано залишиться частиною канонічного ланцюжка [17].

Алгоритм працює в три етапи: pre-prepare (лідер пропонує блок), prepare (валідатори обмінюються підготовчими повідомленнями) та commit (остаточне

підтвердження). Для досягнення консенсусу необхідна згода щонайменше 2/3+1 валідаторів, що робить систему стійкою до візантійських відмов до третини учасників.

Перевагами PBFT є висока швидкість фіналізації (секунди замість хвилин), низьке енергоспоживання та детермінований результат. Проте алгоритм погано масштабується - кількість повідомлень зростає квадратично з числом валідаторів, що робить його непридатним для мереж з тисячами вузлів. Тому PBFT та його варіації (IBFT, Tendermint) використовуються переважно в permissioned-середовищах з обмеженою кількістю відомих учасників.

1.3.5. Інші механізми консенсусу

Окрім трьох основних механізмів, існує ціла низка альтернативних підходів, кожен з яких намагається оптимізувати певні аспекти досягнення консенсусу.

Delegated Proof of Stake (DPoS) - варіант PoS, де власники токенів голосують за обмежену кількість делегатів, які безпосередньо валідують блоки. Це значно підвищує швидкість (EOS досягає тисяч TPS), але за рахунок більшої централізації. Критики порівнюють DPoS з представницькою демократією, де реальна влада концентрується в руках нечисленної еліти [18].

Proof of Authority (PoA) - механізм для приватних мереж, де право валідації надається наперед визначеним авторитетним вузлам. Ці вузли ідентифіковані та несуть репутаційну відповідальність за свої дії. PoA забезпечує максимальну швидкість, але повністю жертвує децентралізацією.

Proof of History (PoH) - інновація від Solana, яка не є самостійним механізмом консенсусу, а скоріше криптографічним способом доведення часу. PoH дозволяє валідаторам погоджуватися щодо порядку подій без постійного обміну повідомленнями, що драматично прискорює роботу мережі [19].

Proof of Elapsed Time (PoET) - розроблений Intel механізм для Hyperledger Sawtooth, який використовує захищене апаратне середовище (SGX) для чесного випадкового вибору лідера. Кожен вузол «засинає» на випадковий час, і перший, хто прокинеться, отримує право створити блок.

1.3.6. Порівняльна таблиця механізмів консенсусу

Таблиця 1.7

Порівняльна характеристика механізмів консенсусу

Характеристика	PoW	PoS	DPoS	PBFT	PoA
Енергоспоживання	Дуже високе	Низьке	Низьке	Низьке	Низьке
Пропускна здатність	7-30 TPS	15-100 TPS	1000+ TPS	1000-10000 TPS	1000+ TPS
Час фіналізації	10-60 хв	10-15 хв	Секунди	Секунди	Секунди
Децентралізація	Висока	Середня-висока	Низька-середня	Низька	Мінімальна
Стійкість до атак	51% хешрейту	51% стейку	51% голосів	1/3 валідаторів	Компрометація валідаторів
Масштабованість	Низька	Середня	Висока	Обмежена	Висока
Типові платформи	Bitcoin, Litecoin	Ethereum 2.0, Cardano	EOS, TRON	Hyperledger Fabric	POA Network, xDai

Вибір механізму консенсусу визначається конкретними вимогами до системи. Для максимальної безпеки та децентралізації підходить PoW або PoS; для корпоративних рішень з високими вимогами до швидкості - PBFT або PoA; для публічних блокчейнів з акцентом на продуктивність - DPoS або комбіновані підходи.

1.4. Проблема забезпечення цілісності даних в сучасних мережах

1.4.1. Цілісність даних як критичний аспект інформаційної безпеки

Інформаційна безпека традиційно розглядається через призму тріади CIA: конфіденційність (Confidentiality), цілісність (Integrity) та доступність (Availability). Хоча всі три компоненти є важливими, саме цілісність даних набуває особливого значення в контексті сучасних цифрових систем, де рішення все частіше приймаються на основі даних без безпосередньої участі людини [20].

Цілісність даних означає гарантію того, що інформація залишається точною, повною та незмінною протягом усього життєвого циклу - від моменту створення до архівування чи знищення. Порушення цілісності може мати катастрофічні наслідки: спотворені медичні записи можуть призвести до помилкового лікування, маніпуляції з фінансовими даними - до мільйонних втрат, а фальсифікація виробничих параметрів - до аварій та людських жертв.

Важливо розрізняти два аспекти цілісності: фізичну та логічну. Фізична цілісність стосується збереження даних на носіях - захисту від пошкодження, втрати чи випадкового знищення. Логічна цілісність забезпечує коректність даних з точки зору бізнес-логіки та правил - їх несуперечливість, відповідність визначеним форматам та обмеженням. Блокчейн-технології адресують переважно логічну цілісність, хоча розподіленість мережі опосередковано сприяє й фізичній захищеності.

1.4.2. Загрози цілісності даних

Сучасні організації стикаються з широким спектром загроз, здатних порушити цілісність їхніх даних. Ці загрози можна класифікувати за джерелом походження на зовнішні та внутрішні [21].

Зовнішні загрози включають:

— Кібератаки - зловмисники можуть модифікувати дані через експлуатацію вразливостей програмного забезпечення, SQL-ін'єкції, атаки на ланцюг постачання тощо. За даними звіту ENISA Threat Landscape 2024, кількість кібератак продовжує зростати, при цьому атаки на цілісність даних становлять значну частку інцидентів [22].

— Програми-вимагачі (ransomware) - окрім шифрування даних з метою викупу, сучасні версії часто викрадають та загрожують оприлюдненням чи модифікацією інформації. Статистика свідчить, що середня вартість відновлення після атаки ransomware перевищує 1,8 мільйона доларів США.

— Атаки «людина посередині» (Man-in-the-Middle) - перехоплення та модифікація даних під час передачі між системами, особливо актуальні для незашифрованих каналів зв'язку.

Внутрішні загрози часто є навіть більш небезпечними:

— Інсайдерські загрози - співробітники з легітимним доступом можуть навмисно або випадково модифікувати критичні дані. За різними оцінками, від 60% до 80% інцидентів безпеки пов'язані з внутрішніми акторами.

— Помилки персоналу - ненавмисні дії користувачів чи адміністраторів, такі як випадкове видалення записів, некоректне оновлення баз даних або помилки при міграції даних.

— Збої обладнання та програмного забезпечення - апаратні несправності, помилки в коді, некоректна робота систем резервного копіювання можуть призводити до непоміченого пошкодження даних.

1.4.3. Проблеми централізованих систем зберігання даних

Традиційна архітектура інформаційних систем базується на централізованій моделі, де всі дані зберігаються в єдиному сховищі під контролем одного суб'єкта. Хоча така модель має свої переваги (простота управління, ефективність запитів), вона створює фундаментальні проблеми для забезпечення цілісності [23].

Єдина точка відмови - централізований сервер або база даних стає критичним вузлом, відмова якого може призвести до втрати всіх даних. Навіть при наявності резервних копій відновлення може бути тривалим і неповним.

Концентрація довіри - користувачі змушені повністю довіряти оператору централізованої системи. Немає незалежного способу переконатися, що дані не були змінені адміністратором. Ця проблема особливо гостра в ситуаціях потенційного конфлікту інтересів або корупції.

Привабливість для атакуючих - централізовані сховища є очевидними цілями

для кіберзлочинців, адже компрометація одного сервера надає доступ до всього масиву даних. Історія знає численні приклади масштабних витоків саме з централізованих систем.

Складність аудиту - перевірка того, що дані не були модифіковані, вимагає довіри до журналів аудиту, які самі зберігаються в тій же централізованій системі та можуть бути підроблені разом з основними даними.

1.4.4. Обмеження традиційних методів захисту цілісності

Для захисту цілісності даних організації традиційно застосовують комплекс технічних та організаційних заходів. Проте кожен із цих методів має суттєві обмеження, які стають критичними в умовах сучасного ландшафту загроз [24].

Контрольні суми та хеш-функції дозволяють виявити випадкові пошкодження даних, але не захищають від навмисної модифікації. Зловмисник, який має доступ до системи, може змінити дані та перерахувати контрольну суму, не залишаючи слідів.

Системи контролю доступу обмежують коло осіб, які можуть модифікувати дані, проте не вирішують проблему зловживань з боку авторизованих користувачів. Крім того, облікові записи можуть бути скомпрометовані, а права доступу - надані помилково.

Журнали аудиту фіксують історію операцій з даними, однак у централізованих системах самі журнали можуть бути підроблені. Адміністратор з достатніми привілеями здатний видалити чи модифікувати записи про свої дії.

Резервне копіювання захищає від втрати даних, але не від їх непомітної модифікації. Якщо спотворення не було вчасно виявлено, пошкоджені дані потраплять і до резервних копій.

Цифрові підписи забезпечують автентичність та цілісність окремих документів, але не створюють незмінного аудиторського сліду та не захищають від ситуацій, коли підписант сам є джерелом загрози. Усі ці обмеження вказують на потребу в принципово новому підході до забезпечення цілісності - такому, що не залежить від довіри до єдиного центрального суб'єкта та забезпечує криптографічно гарантовану незмінність записів.

1.5. Блокчейн як рішення для забезпечення цілісності даних

1.5.1. Як блокчейн вирішує проблеми традиційних систем

Технологія блокчейн пропонує елегантне рішення багатьох проблем, притаманних централізованим системам зберігання даних. Її архітектурні особливості створюють середовище, в якому цілісність інформації забезпечується не довірою до окремих суб'єктів, а математичними та криптографічними гарантіями [25].

Ключова інновація блокчейну полягає в усуненні необхідності центрального арбітра. Замість того щоб покладатися на один сервер чи організацію, система розподіляє функції зберігання та верифікації між безліччю незалежних учасників. Навіть якщо частина з них діє недобросовісно, консенсусні механізми забезпечують коректність загального стану мережі.

Порівняно з традиційними підходами, блокчейн надає:

- Незалежну верифікацію - будь-який учасник може самостійно перевірити весь ланцюжок даних, не довіряючи заявам інших сторін.
- Криптографічний захист історії - зміна минулих записів вимагає перерахунку всіх наступних блоків, що є обчислювально нездійсненним.
- Розподілене зберігання - копії даних існують на багатьох вузлах, усуваючи єдину точку відмови.
- Вбудований аудиторський слід - хронологічна послідовність блоків автоматично створює незмінний журнал усіх операцій.

1.5.2. Незмінність даних в блокчейні

Незмінність (immutability) є, мабуть, найважливішою властивістю блокчейну з точки зору забезпечення цілісності даних. Вона означає, що одного разу записана інформація не може бути видалена чи модифікована без виявлення цього факту всіма учасниками мережі [26].

Технічно незмінність забезпечується криптографічним зв'язком між блоками. Кожен блок містить хеш свого попередника, створюючи безперервний ланцюжок залежностей. Спроба змінити будь-який запис призведе до зміни хешу відповідного блоку, що, своєю чергою, зробить недійсним посилання в наступному блоці, і так

далі до кінця ланцюжка.

Рис. 1.8 «Демонстрація незмінності: два ланцюжки блоків - оригінальний та зі спробою модифікації, де видно розрив хешів»

Для успішної модифікації історичних даних атакуючому довелося б:

— Змінити цільовий запис у потрібному блоці.

— Перерахувати хеш цього блоку.

— Оновити посилання в наступному блоці та перерахувати його хеш.

— Повторити процес для всіх наступних блоків.

— Зробити це швидше, ніж чесна частина мережі додає нові легітимні блоки.

— Переконати більшість вузлів прийняти підроблений ланцюжок.

У великих публічних мережах на кшталт Bitcoin або Ethereum такий сценарій є практично нездійсненним через колосальні обчислювальні чи економічні витрати, необхідні для контролю більшості мережевих ресурсів.

1.5.3. Прозорість та аудит операцій

Прозорість блокчейну радикально змінює підхід до аудиту інформаційних систем. У традиційних централізованих системах аудитор змушений довіряти журналам, наданим самою організацією, не маючи можливості незалежно підтвердити їх повноту та достовірність. Блокчейн усуває цю залежність [27].

У публічних блокчейнах вся історія транзакцій від самого початку існування мережі є відкритою для перегляду. Спеціалізовані сервіси (блок-експлорери) дозволяють досліджувати будь-яку транзакцію, відстежувати рух коштів, перевіряти баланси адрес. Ця радикальна прозорість унеможливлює приховування операцій чи маніпуляції з історією.

Для корпоративних застосувань, де повна відкритість може бути небажаною, приватні та консорціумні блокчейни дозволяють налаштувати рівні доступу. Проте навіть у таких системах авторизовані аудитори отримують можливість незалежної верифікації, не покладаючись на дані, надані перевіряною стороною.

Практичні переваги для аудиту включають:

— Автоматичну фіксацію часу - кожна операція має криптографічно підтверджену мітку часу.
— Неможливість вибіркового видалення - не можна сховати окремі «незручні» транзакції.
— Відстежуваність - можливість прослідкувати походження будь-якого запису.
— Зниження витрат на верифікацію - автоматизована перевірка замість трудомістких ручних процедур.

1.5.4. Децентралізація як фактор безпеки

Децентралізована архітектура блокчейну створює безпрецедентний рівень стійкості до різноманітних загроз - як технічних, так і антропогенних. Відсутність єдиного центру контролю фундаментально змінює модель загроз [28].

Стійкість до відмов - навіть якщо значна частина вузлів вийде з ладу через технічні причини, стихійні лиха чи цілеспрямовані атаки, мережа продовжить функціонувати. Географічний розподіл вузлів забезпечує додаткову стійкість до регіональних катастроф.

Захист від цензури - жоден окремий суб'єкт не може заблокувати або скасувати транзакції. Навіть якщо уряд чи корпорація вимагають видалення певної інформації, це технічно неможливо без контролю над переважною більшістю мережі.

Усунення інсайдерської загрози - в децентралізованій системі немає

привілейованого адміністратора з необмеженим доступом. Компрометація окремих вузлів не надає зловмиснику можливості маніпулювати всією базою даних.

Незалежність від довіри - учасники не зобов'язані довіряти один одному чи будь-якому центральному органу. Коректність системи гарантується математикою та економічними стимулами, а не репутацією чи правовими угодами.

1.5.5. Смарт-контракти для автоматизації політик безпеки

Смарт-контракти являють собою програмний код, що зберігається в блокчейні та автоматично виконується при настанні визначених умов. Ця технологія, вперше повноцінно реалізована в Ethereum, відкриває широкі можливості для автоматизації політик інформаційної безпеки [29].

Схема 1.9 "Робота смарт-контракту: вхідні умови →
логіка контракту → автоматичне виконання дій"

На відміну від традиційних програм, смарт-контракти успадковують властивості блокчейну: їх код є незмінним після розгортання, виконання - детермінованим та верифікованим, а результати - прозорими для всіх учасників. Це робить їх ідеальним інструментом для ситуацій, де важлива автоматизація без

можливості маніпуляцій.

Приклади застосування смарт-контрактів для безпеки даних:

— Автоматичний контроль доступу - смарт-контракт може перевіряти права запитувача та надавати доступ до даних лише за виконання визначених умов.
— Управління життєвим циклом даних - автоматичне архівування або знищення інформації після спливу визначеного терміну.
— Умовне розкриття - дані стають доступними лише після настання певних подій (наприклад, завершення угоди або отримання оплати).
— Багатопідписні схеми - критичні операції вимагають підтвердження від кількох незалежних сторін.

Водночас смарт-контракти мають і обмеження: помилки в коді можуть призводити до серйозних вразливостей (як продемонстрував злам DAO у 2016 році), а незмінність означає неможливість виправлення багів після розгортання без складних процедур міграції.

1.6. Огляд існуючих блокчейн-платформ

1.6.1. Bitcoin

Bitcoin, створений у 2009 році, є першою та найбільш відомою блокчейн-платформою у світі. Хоча спочатку його розробляли виключно як децентралізовану платіжну систему, принципи, закладені в Bitcoin, стали фундаментом для всієї індустрії та залишаються еталоном безпеки і децентралізації [30].

Рис. 1.10 «Логотип «Bitcoin»

З технічного боку Bitcoin використовує механізм консенсусу Proof of Work, де майнери змагаються за право створення нового блоку шляхом розв'язання обчислювально складної криптографічної задачі. Середній час генерації блоку становить близько 10 хвилин, а максимальний розмір блоку - приблизно 1-4 МБ (з урахуванням SegWit), що обмежує пропускну здатність мережі до 7-10 транзакцій на секунду.

Для забезпечення цілісності даних Bitcoin пропонує так званий механізм OP_RETURN, який дозволяє включати до транзакцій до 80 байт довільних даних. Хоча це здається обмеженням, насправді цього достатньо для запису хешів документів або посилань на зовнішні сховища. Проекти на кшталт Proof of Existence використовують цю можливість для створення незмінних міток часу для документів.

Сильними сторонами Bitcoin є неперевершена безпека (найбільший хешрейт серед усіх блокчейнів), максимальна децентралізація та понад 15 років успішного функціонування без серйозних компрометацій. Обмеження включають низьку пропускну здатність, високу вартість транзакцій у періоди завантаження та відсутність повноцінної підтримки смарт-контрактів.

1.6.2. Ethereum

Ethereum, запущений у 2015 році Віталіком Бутеріним та командою розробників, розширив концепцію блокчейну далеко за межі простих грошових переказів. Ключовою інновацією стала повноцінна віртуальна машина Ethereum (EVM), здатна виконувати довільний програмний код - смарт-контракти [31].

Рис. 1.11 «Логотип Ethereum»

У вересні 2022 року Ethereum здійснив історичний перехід з Proof of Work на Proof of Stake (подія, відома як «The Merge»). Це радикально знизило енергоспоживання мережі (за оцінками, на 99,95%) та змінило економічну модель валідації. Наразі мережа обробляє близько 15-30 транзакцій на секунду в базовому шарі, хоча рішення другого рівня (Layer 2) значно підвищують ефективну пропускну здатність.

Для застосувань у сфері безпеки даних Ethereum пропонує найрозвиненішу екосистему смарт-контрактів. Мова програмування Solidity дозволяє створювати складні децентралізовані додатки (dApps) для управління доступом, верифікації документів, ведення аудиторських журналів тощо. Стандарти токенів (ERC-20, ERC-721) забезпечують інтероперабельність між різними проектами.

Переваги Ethereum включають потужну екосистему розробників, широкий вибір інструментів та бібліотек, активну спільноту та постійний розвиток. Серед недоліків - відносно висока вартість газу для складних операцій, виклики масштабованості (які вирішуються через шардинг та L2-рішення) та залишкові ризики безпеки смарт-контрактів.

1.6.3. Hyperledger Fabric

Hyperledger Fabric - це модульна блокчейн-платформа корпоративного класу, розроблена під егідою Linux Foundation. На відміну від публічних блокчейнів, Fabric проектувався спеціально для потреб бізнесу та приватних мереж, де учасники є відомими і частково довіряють один одному [32].

Рис. 1.12 «Логотип Hyperledger Fabric»

Архітектура Fabric базується на концепції каналів (channels) - приватних підмереж всередині загальної інфраструктури. Учасники одного каналу бачать лише транзакції цього каналу, що забезпечує конфіденційність бізнес-операцій. Смарт-контракти в Fabric називаються chaincode і можуть бути написані на популярних мовах програмування: Go, JavaScript, Java.

Механізм консенсусу в Fabric є підключуваним модулем - організація може обрати алгоритм залежно від вимог (Raft, Kafka, або спеціалізовані BFT-рішення). Типова пропускна здатність становить тисячі транзакцій на секунду, що робить платформу придатною для високонавантажених бізнес-процесів.

Сфери застосування Hyperledger Fabric включають управління ланцюгами постачання, фінансові сервіси, охорону здоров'я, державне управління. Серед відомих впроваджень - мережа Food Trust від IBM для відстеження походження продуктів харчування та TradeLens для глобальної логістики.

1.6.4. R3 Corda

R3 Corda позиціонується як «блокчейн для бізнесу» і має суттєві архітектурні відмінності від класичних блокчейн-платформ. Фактично Corda є розподіленим реєстром (DLT), який запозичує ключові концепції блокчейну, але оптимізований для корпоративних фінансових застосувань [33].

Рис.1.13 «Логотип R3 Corda»

Головна особливість Corda - принцип «need-to-know»: дані транзакції бачать лише безпосередньо задіяні сторони, а не всі учасники мережі. Це фундаментально відрізняє Corda від більшості блокчейнів, де всі вузли зберігають повну копію реєстру. Такий підхід забезпечує конфіденційність та відповідність регуляторним вимогам фінансової галузі.

Смарт-контракти в Corda написані на мовах JVM (переважно Kotlin або Java) і можуть включати юридичні тексти для забезпечення зв'язку з правовою системою. Платформа підтримує концепцію «оракулів» для інтеграції зовнішніх даних та нотаріальних сервісів для запобігання подвійним витратам.

R3 Corda активно використовується у фінансовому секторі для торгівлі цінними паперами, страхування, торгового фінансування, а також для цифрових валют центральних банків (CBDC). Консорціум R3 об'єднує понад 300 фінансових установ по всьому світу.

1.6.5. Quorum

Quorum, розроблений JPMorgan Chase і наразі підтримуваний ConsenSys, є корпоративною версією Ethereum з додатковими можливостями конфіденційності та продуктивності. Платформа зберігає сумісність з Ethereum, що дозволяє використовувати існуючі інструменти розробки та смарт-контракти [34].

Рис.1.14 «Логотип Quorum (ConsenSys)»

Ключові доповнення Quorum до базового Ethereum включають:

— Приватні транзакції - механізм, що дозволяє обмежити видимість даних транзакції визначеним колом учасників. Реалізується через інтеграцію з менеджерами приватності Tessera або Constellation.

— Альтернативні механізми консенсусу - замість ресурсоємного PoW, Quorum підтримує IBFT (Istanbul Byzantine Fault Tolerance), Raft та QBFT, що забезпечують швидку фіналізацію транзакцій.

— Покращена продуктивність - оптимізації дозволяють досягати сотень транзакцій на секунду, достатньо для більшості корпоративних застосувань.

— Quorum знайшов застосування в банківській сфері, страхуванні, управлінні активами. Сумісність з Ethereum спрощує міграцію проектів між публічною та приватною версіями мережі.

1.6.6. Інші платформи (Polkadot, Cardano, Cosmos)

Окрім згаданих вище, на ринку присутня низка інших впливових блокчейн-платформ, кожна з яких пропонує унікальні архітектурні рішення.

Polkadot, створений співзасновником Ethereum Гевіном Вудом, фокусується на інтероперабельності між різними блокчейнами. Архітектура включає центральний ланцюжок (Relay Chain) та паралельні ланцюжки (parachains), які можуть мати власні правила консенсусу, але обмінюватися даними та активами. Це робить Polkadot ідеальною платформою для проектів, що потребують взаємодії з кількома блокчейн-екосистемами [35].

Рис.1.15 «Логотипи злів направо Polkadot, Cardano та Cosmos»

Cardano вирізняється академічним підходом до розробки - всі протокольні рішення проходять формальну верифікацію та рецензування науковою спільнотою. Платформа використовує унікальний алгоритм консенсусу Ouroboros (різновид PoS з математично доведеною безпекою) і поступово впроваджує функціональність смарт-контрактів через мову Plutus.

Cosmos реалізує концепцію «інтернету блокчейнів» через протокол Inter-Blockchain Communication (IBC). Кожен блокчейн в екосистемі Cosmos (званий «зоною») є незалежним, але може безпечно обмінюватися даними з іншими через спільний хаб. Cosmos SDK дозволяє створювати власні блокчейни з мінімальними зусиллями.

1.6.7. Порівняльна таблиця блокчейн-платформ

Для систематизації інформації про розглянуті платформи доцільно представити їх ключові характеристики у вигляді порівняльної таблиці.

Таблиця 1.16

Порівняльна характеристика блокчейн-платформ

Характеристика	**Bitcoin**	**Ethereum**	**Hyperledger Fabric**	**R3 Corda**	**Quorum**	**Polkadot**
Тип мережі	Публічна	Публічна	Приватна/консорціумна	Приватна/консорціумна	Приватна/консорціумна	Публічна
Механізм консенсусу	PoW	PoS	Pluggable (Raft, BFT)	Нотаріальний	IBFT, Raft, QBFT	NPoS

Пропускна здатність	7-10 TPS	15-30 TPS	1000+ TPS	1000+ TPS	100-1000 TPS	1000+ TPS
Смарт-контракти	Обмежені (Script)	Повноцінні (Solidity)	Chaincode (Go, JS, Java)	Contracts (Kotlin, Java)	Solidity	Substrate, Ink!
Конфіденційність	Низька	Низька	Висока (канали)	Дуже висока	Висока	Середня
Мова контрактів	Bitcoin Script	Solidity, Vyper	Go, JavaScript, Java	Kotlin, Java	Solidity	Rust, Ink!
Рік запуску	2009	2015	2016	2016	2016	2020
Основне призначення	Цифрові платежі	Універсальна платформа	Корпоративні рішення	Фінансовий сектор	Корпоративний Ethereum	Інтероперабельність

Вибір конкретної платформи залежить від специфіки проекту: для максимальної децентралізації та безпеки підійдуть Bitcoin або Ethereum, для корпоративних застосувань з вимогами до конфіденційності - Hyperledger Fabric або R3 Corda, для сценаріїв міжмережевої взаємодії - Polkadot або Cosmos.

1.7. Застосування блокчейну для забезпечення безпеки даних

1.7.1. Timestamping та нотаріальні послуги

Одним із найбільш очевидних та поширених застосувань блокчейну для безпеки даних є створення незмінних міток часу (timestamping). Ця функція дозволяє криптографічно підтвердити, що певні дані існували на конкретний момент часу та не були змінені відтоді [36].

Технічно процес полягає в обчисленні хешу документа або набору даних та записі цього хешу до блокчейну. Оскільки кожен блок має мітку часу, а сам ланцюжок є незмінним, хеш у блокчейні стає криптографічним доказом існування даних на момент запису. Важливо, що самі дані не потрібно зберігати в блокчейні - достатньо хешу, що забезпечує конфіденційність та економію ресурсів.

Практичні застосування timestamping включають:

— Захист інтелектуальної власності - автори можуть зафіксувати момент створення творів для підтвердження пріоритету.

— Нотаріальні послуги - верифікація існування документів (заповітів, договорів) на визначену дату.

— Наукові дослідження - фіксація дати отримання результатів для встановлення пріоритету відкриттів.

— Регуляторна відповідність - підтвердження своєчасного подання звітності.

Серед реальних проектів у цій сфері варто відзначити Proof of Existence - один із піонерських сервісів timestamping на базі Bitcoin, Originstamp - академічний проект для наукової верифікації, та OpenTimestamps - відкритий стандарт, що підтримується спільнотою.

1.7.2. Системи управління доступом

Традиційні системи управління доступом (Access Control Management) покладаються на централізовані сервери автентифікації та авторизації, що створює вже згадані проблеми єдиної точки відмови та концентрації довіри. Блокчейн пропонує альтернативну модель децентралізованого управління ідентифікацією та правами доступу [37].

Концепція Self-Sovereign Identity (SSI) передбачає, що користувачі володіють та контролюють власні ідентифікаційні дані без залежності від централізованих провайдерів. Верифіковані атрибути (освіта, професійні сертифікати, членство в організаціях) записуються до блокчейну у вигляді криптографічних підтверджень і можуть бути пред'явлені для отримання доступу до ресурсів.

Attribute-Based Access Control (ABAC) на базі смарт-контрактів дозволяє кодифікувати політики доступу як програмний код, що виконується автоматично. Наприклад, смарт-контракт може надавати доступ до документа лише користувачам з певним атрибутом (роль у організації, рівень допуску) без участі централізованого адміністратора.

Реальні впровадження включають проект uPort (наразі Veramo) для децентралізованої ідентифікації, Microsoft ION - систему ідентифікації на базі Bitcoin, та різноманітні корпоративні рішення на Hyperledger Indy.

1.7.3. Захист логів та журналів аудиту

Журнали подій (логи) є критичним елементом інформаційної безпеки - вони дозволяють відстежувати дії користувачів, виявляти інциденти та проводити розслідування. Проте в традиційних системах самі логи є вразливими до маніпуляцій: зловмисник з достатніми привілеями може видалити або модифікувати записи про свої дії [38].

Блокчейн вирішує цю проблему, надаючи незмінне сховище для критичних журнальних записів. Замість (або на додаток до) локального зберігання, хеші логів або самі записи фіксуються у блокчейні, що унеможливлює їх непомітну модифікацію.

Архітектурні підходи до блокчейн-логування включають:

- Пряме записування - кожен логовий запис зберігається безпосередньо в блокчейні. Підходить для критичних подій низької частоти.
- Періодичне якоріння - хеші накопичених локально логів періодично записуються до блокчейну (наприклад, щогодини).
- Гібридний підхід - повні логи зберігаються у традиційному сховищі, а блокчейн містить Merkle Root для верифікації цілісності.

Серед проектів у цій сфері - Guardtime (використовує блокчейн-технологію KSI для захисту логів державних систем Естонії), Logsentinel та різноманітні рішення на базі Hyperledger.

1.7.4. Забезпечення цілісності файлів

Контроль цілісності файлів є фундаментальною задачею інформаційної безпеки, особливо для організацій, що працюють з чутливими даними. Блокчейн дозволяє створити незалежний та незмінний реєстр хешів критичних файлів для виявлення несанкціонованих модифікацій [39].

Типовий процес виглядає наступним чином:

- При створенні або легітимній модифікації файлу обчислюється його криптографічний хеш.
- Хеш разом із метаданими (ім'я файлу, шлях, час, автор) записується до блокчейну.
- При перевірці цілісності поточний хеш файлу порівнюється зі значенням у блокчейні.
- Розбіжність свідчить про модифікацію файлу після останньої фіксації.

Переваги порівняно з традиційними системами контролю цілісності (наприклад, OSSEC, Tripwire):

- Неможливість маніпуляції базою еталонних хешів.
- Незалежна верифікація без довіри до локальної системи.
- Криптографічне підтвердження часу останньої легітимної версії.

Обмеження включають необхідність повторного хешування при легітимних змінах та потенційні витрати на транзакції в публічних блокчейнах.

1.7.5. Ланцюги постачання та відстеження походження даних

Відстеження походження (provenance) даних та фізичних товарів є сферою, де блокчейн демонструє найбільш очевидні переваги. Традиційні системи трекінгу покладаються на централізовані бази даних окремих учасників ланцюга постачання, що створює проблеми довіри та розриви в інформації [40].

Блокчейн дозволяє створити єдиний незмінний журнал, де кожен учасник фіксує свої операції з товаром або даними. Кінцевий споживач може прослідкувати повну історію - від виробництва сировини до доставки готового продукту.

Таблиця 1.17

Приклади застосування блокчейну у ланцюгах постачання

Галузь	**Проект/Платформа**	**Опис застосування**
Продукти харчування	IBM Food Trust	Відстеження походження продуктів від ферми до магазину
Фармацевтика	MediLedger	Боротьба з контрафактними ліками
Алмази	Everledger	Підтвердження етичного походження дорогоцінного каміння
Логістика	TradeLens (Maersk + IBM)	Глобальний трекінг контейнерних перевезень
Мода	TextileGenesis	Відстеження походження тканин

Переваги блокчейну для ланцюгів постачання включають підвищену прозорість, зниження ризиків шахрайства, швидше виявлення проблем (наприклад, відкликання продукції) та покращення довіри споживачів.

1.8. Виклики та обмеження використання блокчейну

1.8.1. Технічні виклики

Незважаючи на потужний потенціал, впровадження блокчейн-технологій стикається з низкою технічних викликів, які необхідно враховувати при проектуванні систем. Ці виклики є об'єктом активних досліджень та розробок, однак універсальних рішень поки не знайдено [42].

Управління ключами залишається однією з найскладніших практичних проблем. Безпека блокчейн-систем безпосередньо залежить від збереження приватних ключів - їх втрата означає втрату доступу до активів без можливості відновлення, а компрометація - повний контроль зловмисника. Традиційні механізми відновлення паролів тут не працюють, що створює суттєві виклики для масового впровадження.

Оновлення протоколу в децентралізованих системах є значно складнішим процесом, ніж у централізованих. Зміни вимагають консенсусу спільноти, а несумісні оновлення можуть призводити до розгалуження мережі (форків). Історія знає приклади, коли суперечки щодо напрямку розвитку призводили до тривалих конфліктів та розколів (Bitcoin vs Bitcoin Cash, Ethereum vs Ethereum Classic).

Незрілість інструментарію порівняно з традиційними технологіями розробки. Хоча ситуація швидко покращується, все ще бракує стандартизованих фреймворків, засобів тестування та налагодження, кваліфікованих розробників.

1.8.2. Масштабованість

Масштабованість є, мабуть, найбільш обговорюваним обмеженням блокчейн-технологій, особливо для публічних мереж. Проблема відома як «трилема блокчейну» - твердження, що система не може одночасно максимізувати децентралізацію, безпеку та масштабованість [43].

Рис. 1.18 «Трилема блокчейну: трикутник з вершинами Децентралізація, Безпека, Масштабованість»

Публічні блокчейни на кшталт Bitcoin або Ethereum в базовій конфігурації обробляють лише десятки транзакцій на секунду - порівняйте з тисячами TPS у Visa чи мільйонами у сучасних базах даних. Ця обмеженість є прямим наслідком необхідності досягнення глобального консенсусу: кожна транзакція повинна бути верифікована та збережена всіма вузлами.

Рішення проблеми масштабованості розвиваються у кількох напрямках:

— Layer 2 рішення (Lightning Network, Optimistic Rollups, zkRollups) - винесення більшості транзакцій за межі основного ланцюжка з періодичною фіксацією результатів.

— Шардинг - розділення мережі на паралельні сегменти, що обробляють транзакції незалежно.

— Альтернативні консенсуси - механізми на кшталт DPoS або PoA, що жертвують децентралізацією заради продуктивності.

— Спеціалізовані блокчейни - створення окремих мереж під конкретні застосування з оптимізованими параметрами.

1.8.3. Конфіденційність даних

Парадоксально, але прозорість блокчейну, яка є перевагою для аудиту та довіри, створює проблеми для конфіденційності. У публічних мережах всі транзакції видимі кожному, що може бути неприйнятним для бізнес-застосувань з чутливими даними або для дотримання регуляторних вимог [44].

Проблема загострюється тим, що дані в блокчейні є не лише публічними, але й незмінними. Інформація, записана сьогодні, залишиться доступною назавжди, навіть якщо згодом виникне необхідність у її видаленні (наприклад, за вимогою «права на забуття» згідно з GDPR).

Технічні рішення для забезпечення конфіденційності включають:

- Приватні транзакції - технології на кшталт zk-SNARKs (Zcash) або Confidential Transactions дозволяють приховувати деталі операцій, зберігаючи можливість їх верифікації.
- Приватні канали - як у Hyperledger Fabric, де підмножини учасників мають власні ізольовані реєстри.
- Off-chain зберігання - в блокчейні фіксуються лише хеші даних, а самі дані зберігаються у зовнішніх системах з контролем доступу.
- Гомоморфне шифрування - теоретично дозволяє виконувати обчислення над зашифрованими даними, хоча практичні реалізації поки занадто повільні.

1.8.4. Регуляторні та юридичні аспекти

Правова невизначеність залишається серйозною перешкодою для впровадження блокчейн-рішень, особливо у регульованих галузях. Законодавство більшості країн не встигає за технологічним розвитком, створюючи зони невизначеності [45].

Юридичний статус смарт-контрактів залишається дискусійним. Чи є смарт-контракт юридично зобов'язуючим договором? Яке право застосовується до угоди, укладеної в децентралізованій мережі без географічної прив'язки? Хто несе відповідальність за помилки в коді? Ці питання здебільшого не мають чітких відповідей у чинному законодавстві.

Право на забуття (right to erasure) згідно з GDPR суперечить фундаментальній властивості незмінності блокчейну. Регулятори різних країн по-різному

інтерпретують цю колізію, створюючи ризики для проектів, що обробляють персональні дані.

Транскордонний характер публічних блокчейнів ускладнює визначення юрисдикції та застосовного права. Дані одночасно існують на тисячах вузлів у десятках країн із різними правовими режимами.

Регуляторні вимоги до фінансових операцій (KYC, AML) складно імплементувати у повністю децентралізованих системах, хоча приватні блокчейни дозволяють забезпечити необхідний рівень контролю.

1.8.5. Інтеграція з існуючими системами

Більшість організацій вже мають розвинену IT-інфраструктуру, і впровадження блокчейну рідко означає створення системи «з нуля». Необхідність інтеграції з існуючими базами даних, ERP-системами, застосунками створює значні технічні та організаційні виклики [46].

Проблема оракулів - блокчейн за своєю природою є замкненою системою, яка не може самостійно отримувати дані із зовнішнього світу. Для інтеграції з реальними бізнес-процесами необхідні «оракули» - посередники, що передають зовнішні дані до смарт-контрактів. Проте оракули є потенційною точкою централізації та вектором атаки.

Відмінності в моделях даних - реляційні бази даних та блокчейн мають принципово різні структури. Переведення існуючих схем даних у формат, придатний для блокчейну, може вимагати суттєвої перебудови архітектури.

Питання продуктивності - інтеграція може створювати вузькі місця, коли швидка внутрішня система очікує на повільне підтвердження транзакцій у блокчейні.

Організаційний опір - впровадження нової технології вимагає перенавчання персоналу, зміни бізнес-процесів, подолання скептицизму зацікавлених сторін.

1.8.6. Вартість впровадження та підтримки

Економічні аспекти є вирішальними для багатьох організацій при прийнятті рішення про впровадження блокчейну. Витрати включають як початкові інвестиції, так і постійні операційні витрати [47].

Початкові витрати охоплюють:

— Розробку або адаптацію блокчейн-рішення під специфічні потреби.

— Інтеграцію з існуючою інфраструктурою.

— Закупівлю або оренду апаратного забезпечення для вузлів.

— Навчання персоналу.

— Юридичну експертизу та сертифікацію.

Операційні витрати включають:

— Транзакційні комісії у публічних мережах (gas fees в Ethereum можуть бути значними).

— Підтримку та моніторинг інфраструктури.

— Оновлення та розвиток системи.

— Управління безпекою (зокрема, ключами).

Таблиця 1.19

Орієнтовна структура витрат на впровадження блокчейн-рішення

Категорія витрат	**Частка від бюджету**	**Примітки**
Розробка та інтеграція	40-50%	Залежить від складності рішення
Інфраструктура	15-25%	Сервери, мережа, безпека
Консалтинг та експертиза	10-20%	Юридичні, технічні консультації
Навчання персоналу	5-10%	Розробники, адміністратори, користувачі
Непередбачені витрати	10-15%	Резерв на ризики

При цьому важливо порівнювати витрати на блокчейн-рішення з альтернативами, враховуючи не лише прямі витрати, але й потенційні втрати від порушення цілісності даних, яким блокчейн може запобігти.

1.9. Висновки до розділу 1

По-перше, блокчейн являє собою потужну технологію розподіленого реєстру, що базується на криптографічних примітивах (хеш-функціях, асиметричній криптографії, цифрових підписах) та механізмах консенсусу для досягнення узгодженості в децентралізованому середовищі. Ключовими властивостями технології є децентралізація, незмінність даних, прозорість та криптографічна захищеність, що робить її привабливою для вирішення задач інформаційної безпеки.

По-друге, існує розмаїття типів блокчейн-мереж (публічні, приватні, консорціумні, гібридні) та механізмів консенсусу (PoW, PoS, PBFT, DPoS та інші), кожен з яких має свої переваги та обмеження. Вибір конкретного варіанту визначається специфікою задачі, вимогами до продуктивності, рівнем довіри між учасниками та регуляторним контекстом.

По-третє, проблема забезпечення цілісності даних є критичною в сучасних інформаційних системах. Традиційні централізовані підходи мають фундаментальні обмеження: єдину точку відмови, концентрацію довіри, вразливість до інсайдерських загроз та складність незалежного аудиту. Статистика кіберінцидентів 2023-2024 років підтверджує актуальність цих загроз.

По-четверте, блокчейн пропонує принципово нову модель забезпечення цілісності, засновану на математичних гарантіях замість довіри до окремих суб'єктів. Незмінність записів, прозорість операцій, децентралізація зберігання та можливість автоматизації політик через смарт-контракти створюють надійний фундамент для захисту критичних даних.

По-п'яте, аналіз існуючих платформ (Bitcoin, Ethereum, Hyperledger Fabric, R3 Corda, Quorum та інших) демонструє наявність зрілих рішень для різних сценаріїв застосування. Практичні впровадження у сферах timestamping, управління доступом, захисту логів, контролю цілісності файлів, ланцюгів постачання та медичних записів підтверджують життєздатність технології.

По-шосте, впровадження блокчейну стикається з низкою викликів: обмеженнями масштабованості, проблемами конфіденційності, регуляторною невизначеністю,

складністю інтеграції та значними витратами. Ці виклики не є непереборними, однак вимагають ретельного аналізу та планування при проектуванні конкретних рішень.

Таким чином, технологія блокчейн має значний потенціал для застосування у сфері забезпечення безпеки та цілісності даних, проте її впровадження потребує зваженого підходу з урахуванням специфіки конкретної організації, її технічних можливостей, регуляторного середовища та економічної доцільності.

РОЗДІЛ 2. ВИБІР ТА ОБҐРУНТУВАННЯ БЛОКЧЕЙН-РІШЕННЯ ДЛЯ МЕДИЧНОЇ УСТАНОВИ

2.1. Аналіз вимог до системи захисту медичних даних

Сучасна система охорони здоров'я України переживає період глибокої трансформації. Цифровізація медичних процесів, що розпочалася з впровадженням національної електронної системи eHealth, поставила перед приватними та державними медичними закладами нові виклики, пов'язані із забезпеченням належного рівня захисту персональних даних пацієнтів. Ці дані, відомі як електронні медичні картки (ЕМК), містять надзвичайно чутливу інформацію: історію захворювань, діагнози, результати лабораторних досліджень, призначене лікування, генетичні дані та іншу інформацію про фізичний і психічний стан здоров'я людини. Розголошення або несанкціоноване використання таких відомостей може призвести до серйозних наслідків - від дискримінації на робочому місці до шантажу, фінансових втрат та глибокої психологічної травми. Тому законодавчі та регуляторні вимоги до захисту медичних даних є серед найсуворіших у всьому спектрі інформаційної безпеки.

Нормативно-правова база України в цій сфері формується під впливом як національних реалій, так і процесу гармонізації з європейськими стандартами. Ключовим національним документом є Закон України "Про захист персональних даних", прийнятий у 2010 році [1]. Цей закон встановлює базові принципи роботи з будь-якою інформацією, що дозволяє ідентифікувати фізичну особу. Серед цих принципів - законність та справедливість обробки, відповідність мети обробки попередньо оголошеній меті, точність та актуальність даних, а також обмеження строків їх зберігання лише періодом, необхідним для досягнення мети. Закон чітко визначає, що медичні дані належать до особливої категорії персональних даних, обробка яких може здійснюватися лише за однієї з наступних умов: за явною письмовою згодою суб'єкта даних, якщо це необхідно для надання йому медичної допомоги, для виконання функцій у сфері охорони здоров'я, або коли це передбачено законом в інтересах національної безпеки чи громадського порядку.

Додаткові вимоги містяться в Законі України "Про інформацію", згідно з яким

відомості про стан здоров'я класифікуються як конфіденційна інформація з обмеженим доступом [3]. Це означає, що така інформація не може вільно поширюватися без згоди особи. Важливим є також Закон України "Про державні фінансові гарантії медичного обслуговування населення", який регулює організацію системи медичного обслуговування та містить норми щодо захисту прав пацієнтів, включаючи право на конфіденційність їхньої медичної інформації [4].

З появою національної електронної системи охорони здоров'я регуляторна база була доповнена специфічними нормативними актами. Зокрема, Постанова Кабінету Міністрів України № 411 від 25 квітня 2018 року "Деякі питання електронної системи охорони здоров'я" встановлює вимоги до медичних інформаційних систем (МІС), що підключаються до центральної бази даних [5]. Ці вимоги охоплюють як технічні аспекти (шифрування даних при передачі та зберіганні, використання кваліфікованого електронного підпису), так і організаційні (призначення відповідальних осіб, ведення журналів подій). Міністерство охорони здоров'я України підкреслює, що система eHealth будується на принципах роздільного зберігання персональних та медичних даних, що значно підвищує безпеку. Для ідентифікації та автентифікації користувачів застосовується двофакторна автентифікація та обов'язкове використання кваліфікованого електронного підпису (КЕП), що гарантує юридичну значущість кожної дії в системі [6].

Однак найбільш масштабним викликом для українських медичних закладів стає необхідність відповідності вимогам Загального регламенту про захист даних Європейського Союзу (General Data Protection Regulation, GDPR), який набув чинності 25 травня 2018 року [7]. Україна, як країна-асоціат ЄС, взяла на себе зобов'язання гармонізувати своє законодавство з нормами GDPR. Цей регламент встановлює найвищі на сьогодні стандарти захисту персональних даних у світі. GDPR розглядає дані про здоров'я як "особливу категорію персональних даних" (стаття 9), обробка яких, за загальним правилом, заборонена, за винятком чітко визначених випадків [8]. Регламент закріплює цілий спектр прав для суб'єктів

даних (пацієнтів), включаючи право на доступ до своїх даних, право на виправлення неточних даних, право на забуття (видалення даних) та право на портативність даних (отримання даних у структурованому, машиночитаному форматі для передачі іншому контролеру) [9].

Критично важливою вимогою GDPR є принцип "інформованої згоди". Пацієнт має надати явну, недвозначну та добровільну згоду на обробку своїх даних після того, як йому було детально роз'яснено: які саме дані збираються, з якою конкретною метою, як довго вони зберігатимуться, хто матиме до них доступ, які ризики існують і які права має пацієнт [10]. Форма згоди має бути зрозумілою, не може містити "прихованих" умов у дрібному шрифті. Більше того, пацієнт має право в будь-який момент відкликати свою згоду. Регламент також накладає жорсткі вимоги щодо повідомлення про витоки даних: контролер даних (медичний заклад) зобов'язаний повідомити наглядовий орган протягом 72 годин після виявлення інциденту, а в деяких випадках - і самих суб'єктів даних, якщо витік створює високий ризик для їхніх прав та свобод [11]. За порушення GDPR передбачені колосальні штрафи - до 20 мільйонів євро або до 4% від глобального річного обороту компанії, в залежності від того, що є більшим [12]. Ця норма робить дотримання GDPR не просто етичним обов'язком, а критичною бізнес-необхідністю для будь-якої приватної лікарні, що обслуговує резидентів ЄС або має наміри розширювати свою діяльність на європейський ринок.

Технічні вимоги до захисту медичних даних охоплюють декілька рівнів. По-перше, це криптографічний захист: всі дані, що зберігаються в базах даних та передаються мережами, мають бути зашифровані з використанням сучасних алгоритмів (наприклад, AES-256). По-друге, розмежування доступу: система повинна гарантувати, що користувач отримає доступ лише до тих даних, які необхідні для виконання його службових обов'язків (принцип найменших привілеїв, "least privilege"). По-третє, забезпечення цілісності: система має виявляти будь-які несанкціоновані зміни даних. По-четверте, аудит та моніторинг: всі дії користувачів, особливо ті, що стосуються доступу до конфіденційних даних, мають фіксуватися в незмінних журналах подій з можливістю їх подальшого

аналізу [13]. По-п'яте, резервне копіювання та відновлення: необхідно регулярно створювати резервні копії даних та забезпечувати можливість їх швидкого відновлення у випадку аварії або кібератаки.

Для приватної лікарні в Україні, що планує впровадження сучасної системи управління електронними медичними картками, дотримання всіх цих вимог є не лише юридичним обов'язком, але й питанням репутації та конкурентоспроможності. Пацієнти дедалі більше усвідомлюють свої права та обирають ті заклади, які можуть гарантувати безпеку їхньої приватної інформації. Водночас складність і багатошаровість вимог створює значні технічні та організаційні виклики, що вимагають застосування інноваційних технологічних підходів. Саме в цьому контексті технологія блокчейн, завдяки своїм фундаментальним властивостям, здатна стати одним з ключових інструментів для створення системи, що відповідає найвищим стандартам безпеки та довіри.

2.2. Критерії вибору блокчейн-платформи для медичної сфери

Вибір блокчейн-платформи для системи управління електронними медичними картками є стратегічним рішенням, що визначатиме архітектуру системи, її можливості, обмеження та вартість експлуатації на роки вперед. Цей вибір не може ґрунтуватися виключно на технічних параметрах продуктивності або популярності платформи на ринку. Для медичної сфери, з її унікальними вимогами до конфіденційності, юридичної відповідальності та життєво важливої надійності, необхідно сформулювати спеціалізований набір критеріїв оцінки, що враховує специфіку галузі. Ці критерії можна згрупувати в кілька категорій: технічні, безпекові, функціональні, організаційні, економічні та критерії відповідності регуляторним вимогам.

Технічні критерії визначають, чи може платформа взагалі справитися з обсягом та характером навантаження медичної установи. Продуктивність та пропускна здатність (throughput) вимірюються кількістю транзакцій, які система може обробити за секунду (TPS). Приватна лікарня середнього розміру може обслуговувати сотні пацієнтів щодня, кожен з яких генерує десятки записів (консультації, аналізи, призначення). Тому платформа повинна забезпечувати мінімум сотні, а краще - тисячі TPS з можливістю подальшого масштабування [14]. Затримка (latency), тобто час від відправлення транзакції до її завершення, критично важлива для користувацького досвіду. Лікарі не можуть чекати хвилинами підтвердження того, що запис збережено. Ідеальна затримка - частки секунди, прийнятна - кілька секунд [15]. Масштабованість визначає, чи може система підтримувати зростання навантаження. На відміну від публічних блокчейнів, які стикаються з проблемою "трилеми блокчейну" (неможливість одночасно максимізувати децентралізацію, безпеку та масштабованість), приватні корпоративні блокчейни можуть досягати значно вищих показників масштабованості, жертвуючи рівнем децентралізації, що є прийнятним компромісом для контрольованого середовища лікарні [16].

Безпекові та конфіденційні критерії є абсолютно центральними для медичних застосувань. Модель доступу до мережі - це фундаментальна характеристика, що

поділяє блокчейни на публічні (permissionless), де будь-хто може анонімно приєднатися до мережі, та приватні (permissioned), де всі учасники мають бути ідентифіковані та авторизовані [17]. Для медичних даних публічні блокчейни категорично неприйнятні через відсутність контролю над тим, хто може бачити транзакції. Механізми забезпечення конфіденційності повинні дозволяти приховувати чутливу інформацію навіть від інших учасників мережі. Це може досягатися через канали, приватні підледжери, шифрування на рівні додатку або інші криптографічні методи, такі як zero-knowledge proofs [18]. Криптографічний захист має бути заснований на перевірених, стійких алгоритмах (наприклад, ECDSA для підписів, SHA-256 або SHA-3 для хешування, AES для шифрування). Незмінність даних (immutability) - це ключова властивість блокчейну, що гарантує: після того, як запис додано до ланцюга, його неможливо змінити або видалити без виявлення [19]. Однак у контексті GDPR виникає парадокс: незмінність суперечить "праву на забуття". Цю проблему можна вирішити, зберігаючи в блокчейні не самі медичні дані, а лише їхні хеші та метадані, тоді як фактичні дані зберігаються окремо (off-chain) і можуть бути видалені за запитом [20].

Функціональні критерії визначають, наскільки гнучко платформа дозволяє реалізувати складну бізнес-логіку. Підтримка смарт-контрактів і їхня виразність - це здатність автоматизувати процеси управління доступом, валідації даних, автоматичних сповіщень. Обмежена скриптова мова (як у Bitcoin) не дозволить реалізувати необхідну складність, тоді як повноцінна мова програмування відкриває широкі можливості [21]. Інтероперабельність та підтримка стандартів - це можливість системи взаємодіяти з іншими медичними системами. Критично важлива підтримка міжнародних стандартів обміну медичною інформацією, таких як HL7 FHIR (Fast Healthcare Interoperability Resources), що дозволить безшовно інтегрувати блокчейн-рішення з існуючими МІС, лабораторними системами та державним реєстром eHealth [22]. Механізми консенсусу визначають, як учасники мережі досягають згоди щодо стану даних. Енергозатратний Proof-of-Work (PoW), що використовується в Bitcoin, абсолютно непридатний для корпоративних застосувань через повільність та екологічну неефективність. Для приватних мереж

більш доцільні BFT-подібні алгоритми (Practical Byzantine Fault Tolerance, Raft), що забезпечують швидкість та детермінованість.

Рис. 2.1 "Порівняльна діаграма механізмів консенсусу: Proof-of-Work, Proof-of-Stake та BFT у контексті швидкості, енергоефективності та рівня децентралізації"

Організаційні та експлуатаційні критерії стосуються практичних аспектів впровадження. Зрілість платформи та екосистеми - це наявність документації, активної спільноти розробників, готових компонентів, навчальних матеріалів та прикладів застосування [24]. Наявність професійної підтримки від вендора або партнерів критична для швидкого вирішення технічних проблем. Складність розгортання та підтримки визначає, чи потрібна висококваліфікована команда DevOps-інженерів постійно, чи система може бути відносно легко налаштована та підтримуватися існуючим IT-персоналом лікарні [25]. Вимоги до апаратного забезпечення - деякі блокчейни вимагають потужних серверів, інші можуть працювати на відносно скромному обладнанні, що впливає на загальну вартість інфраструктури.

Економічні критерії визначають фінансову доцільність рішення. Наявність власної криптовалюти та модель оплати транзакцій - це критично важливий фактор. Якщо платформа вимагає оплати за кожну транзакцію у власній криптовалюті

(наприклад, "газ" в Ethereum), це створює складнощі: лікарня має постійно купувати токени, піддаючись волатильності їхньої ціни, що робить бюджетування непередбачуваним. Для корпоративних застосувань краще платформи без нативної криптовалюти [26]. Вартість ліцензування - більшість корпоративних блокчейнів є open-source з ліцензією Apache 2.0, що дозволяє безкоштовне використання, але деякі комерційні версії або додаткові інструменти можуть потребувати ліцензій [27]. Загальна вартість володіння (Total Cost of Ownership, TCO) включає не лише початкові витрати на розробку, але й поточні витрати на підтримку серверів, оновлення ПЗ, оплату праці персоналу та потенційні штрафи за невідповідність регуляторним вимогам.

Критерії відповідності регуляторним вимогам та антикорупційний потенціал. Платформа повинна дозволяти реалізувати системи, що повністю відповідають українському законодавству та GDPR. Це включає можливість аудиту та простежуваності: кожна дія в системі (хто, коли, що змінив) має фіксуватися в незмінному журналі [28]. Така прозорість створює потужний антикорупційний ефект - підробка медичних довідок, незаконне видалення або зміна записів стають майже неможливими, оскільки залишають цифровий слід. Гранулярний контроль доступу дозволяє реалізувати складні політики, де пацієнт є "власником" своїх даних і може надавати та відкликати доступ іншим учасникам [29]. Сумісність з електронним підписом (КЕП), що використовується в Україні, забезпечує юридичну значущість електронних документів.

Таблиця 2.2.

Критерії оцінки блокчейн-платформ для медичних застосувань

Категорія критеріїв	**Критерій**	**Опис та важливість**
Технічні	Продуктивність (TPS)	Кількість транзакцій на секунду. Мінімум: 100-500 TPS, бажано: >1000 TPS
	Затримка транзакції	Час підтвердження транзакції. Прийнятно: <5 секунд, ідеально: <1 секунди

	Масштабованість	Можливість розширення системи при зростанні навантаження
Безпека та конфіденційність	Модель доступу	Приватна (permissioned) vs публічна (permissionless). Критично: приватна для медицини
	Механізми конфіденційності	Канали, приватні дані, шифрування, zero-knowledge proofs
	Криптографічний захист	Стійкі алгоритми підпису, хешування, шифрування
	Незмінність (Immutability)	Гарантія, що дані не можуть бути змінені заднім числом
Функціональні	Смарт-контракти	Наявність і виразність мови для програмування бізнес-логіки
	Інтероперабельність	Підтримка стандартів (HL7 FHIR), легкість інтеграції з МІС
	Механізм консенсусу	Швидкість і ефективність досягнення згоди (BFT > PoS > PoW для корпорацій)
Організаційні	Зрілість платформи	Наявність документації, спільноти, кейсів впровадження
	Професійна підтримка	Доступність вендора або партнерів для технічної допомоги
	Складність розгортання	Необхідний рівень кваліфікації персоналу
Економічні	Криптовалюта та оплата	Відсутність необхідності купувати токени - перевага для корпорацій
	Вартість ліцензування	Open-source (Apache 2.0) vs комерційна ліцензія
	Загальна вартість володіння (TCO)	Початкові та поточні витрати (інфраструктура, персонал, підтримка)
Регуляторні та антикорупційні	Відповідність GDPR/нац. законодавству	Можливість реалізації вимог до захисту персональних даних
	Аудит та простежуваність	Незмінний журнал всіх операцій для прозорості

	Контроль доступу	Гранулярне управління правами, контроль з боку пацієнта

2.3. Порівняльний аналіз блокчейн-платформ для медичних даних

Для об'єктивної оцінки придатності різних блокчейн-рішень для створення системи управління електронними медичними картками приватної лікарні необхідно провести детальний порівняльний аналіз провідних платформ. Обрано три платформи, що представляють різні покоління та філософії блокчейн-технології: Bitcoin (перше покоління, криптовалютний фокус), Ethereum (друге покоління, платформа смарт-контрактів) та Hyperledger Fabric (корпоративний блокчейн третього покоління). Цей вибір дозволяє проілюструвати еволюцію технології та виявити, яке рішення найкраще відповідає специфічним потребам медичної галузі.

2.3.1. Bitcoin: піонер блокчейн-технології з обмеженими можливостями для медицини

З технічної точки зору, Bitcoin має кілька фундаментальних характеристик, що роблять його абсолютно непридатним для використання як основи для системи ЕМК. По-перше, блокчейн Bitcoin є публічним та псевдоанонімним. Це означає, що всі транзакції записуються відкрито, і будь-хто в світі може завантажити повну копію блокчейну та переглянути всю історію всіх транзакцій. Хоча транзакції не пов'язані безпосередньо з іменами людей (замість них використовуються адреси-хеші), сучасні методи аналізу блокчейну та деанонімізації дозволяють з високою ймовірністю пов'язати транзакції з реальними особами, особливо якщо адреса коли-небудь була використана для взаємодії з регульованим сервісом (наприклад, біржа, що вимагає KYC-верифікацію) [32]. Для медичних даних така "прозорість" є неприйнятною, адже вона прямо суперечить законодавству про захист медичної таємниці та нормам GDPR, що вимагають суворого контролю над тим, хто може бачити конфіденційну інформацію про здоров'я [33].

По-друге, Bitcoin має вкрай обмежені можливості для програмування логіки. Його скриптова мова (Script) є навмисно обмеженою, не є Тьюрінг-повною і не підтримує складні умови та циклиці. Це зроблено з міркувань безпеки та спрощення перевірки транзакцій, але означає, що неможливо реалізувати смарт-

контракти, необхідні для управління правами доступу до медичних записів, автоматичного надання дозволів, валідації даних за складними правилами або інтеграції з іншими системами [34]. Найпростіші багатопідписні (multisig) схеми та тайм-локи - це максимум того, що дозволяє Bitcoin, чого категорично недостатньо для реалізації бізнес-процесів медичного закладу.

По-третє, продуктивність Bitcoin є надзвичайно низькою. Мережа була спроектована з пріоритетом безпеки та децентралізації над швидкістю. Новий блок створюється приблизно раз на 10 хвилин, а розмір блоку обмежений (близько 1 МБ), що дозволяє обробляти лише близько 3-7 транзакцій на секунду [35]. Для порівняння, платіжна система Visa обробляє тисячі транзакцій на секунду. Для лікарні, де сотні лікарів одночасно записують дані про пацієнтів, така пропускна здатність означала б годинні затримки в обробці запитів, що робить систему абсолютно непрацездатною. Крім того, під час пікових навантажень у мережі Bitcoin (наприклад, під час спекулятивних бумів) комісії за транзакції можуть зростати до десятків доларів за одну транзакцію [36], що робить використання системи економічно нераціональним для рутинних медичних записів.

По-четверте, механізм консенсусу Proof-of-Work є енергетично неефективним. Процес "майнінгу" вимагає від учасників мережі виконання величезної кількості обчислень для вирішення криптографічних головоломок, що споживає колосальну кількість електроенергії - за оцінками, річне споживання мережі Bitcoin порівнянне з енергоспоживанням цілих країн [37]. Це створює екологічні та етичні питання, які є неприйнятними для медичної установи, що має дотримуватися принципів сталого розвитку та корпоративної соціальної відповідальності.

Таблиця 2.3.

Оцінка платформи Bitcoin за ключовими критеріями для медичних застосувань

Критерій	**Оцінка Bitcoin**	**Коментар**
Модель доступу	Публічна (Permissionless)	Будь-хто може бачити транзакції - неприйнятно для медичних даних

Конфіденційність	Відсутня	Псевдоанонімність легко деанонімізується, немає вбудованих механізмів приховування даних
Продуктивність (TPS)	3-7 TPS	Критично недостатньо для медичного закладу
Затримка транзакції	~10-60 хвилин	Неприйнятно довго для робочих процесів лікарні
Смарт-контракти	Відсутні (обмежений Script)	Неможливо реалізувати складну логіку управління доступом
Інтероперабельність	Відсутня	Немає підтримки медичних стандартів (HL7 FHIR)
Механізм консенсусу	PoW (енергозатратний)	Повільний, дорогий, екологічно шкідливий
Вартість транзакцій	Висока і волатильна ($1-50+)	Непередбачувана вартість операцій
Зрілість платформи	Дуже висока	Найстаріша і найперевіреніша блокчейн-мережа, але це не компенсує інших недоліків
ПІДСУМОК	НЕПРИДАТНА	Bitcoin категорично не підходить для управління медичними даними

Bitcoin залишається важливою інновацією та домінуючою криптовалютою, але його архітектура оптимізована виключно для простого переміщення цифрових коштів у публічному середовищі. Спроби використання Bitcoin для інших застосувань, зокрема для зберігання та управління медичними даними, є фундаментально помилковими та приречені на провал через невідповідність базових принципів системи вимогам медичної галузі.

2.3.2. Ethereum: крок вперед з смарт-контрактами, але з проблемами для корпорацій

Ключовою інновацією Ethereum є Ethereum Virtual Machine (EVM) - віртуальна машина, що виконує код смарт-контрактів. Смарт-контракти пишуться на Тьюрінг-повній мові програмування Solidity (або на альтернативних мовах, таких як Vyper), що дозволяє розробникам створювати програми з будь-якою складністю логіки [40]. Це відкрило можливість автоматизації складних бізнес-процесів без довірених

посередників: від децентралізованих фінансових сервісів (DeFi) до систем управління ланцюгами постачання та цифрового мистецтва (NFT). Для медичних застосувань це означає, що можна запрограмувати складні правила контролю доступу до ЕМК, автоматичне виконання умов страхових контрактів або управління згодою пацієнтів [41].

Однак при ближчому розгляді виявляється, що публічна мережа Ethereum (Ethereum Mainnet) має ряд суттєвих недоліків для корпоративного, зокрема медичного, використання. По-перше, як і Bitcoin, публічний Ethereum є відкритою мережею, де всі транзакції та стан смарт-контрактів видимі для будь-кого [42]. Хоча можна зашифрувати дані перед записом у блокчейн, метадані транзакцій (хто, коли, з яким контрактом взаємодіяв, скільки "газу" витратив) залишаються видимими, що може дозволити витягти конфіденційну інформацію через аналіз шаблонів поведінки. Існують рішення для підвищення конфіденційності (наприклад, zk-SNARKs, що використовуються в проєкті Zcash, або Layer-2 рішення з додатковим шифруванням), але їх інтеграція складна і не є стандартною можливістю [43].

По-друге, продуктивність публічного Ethereum, хоча й вища за Bitcoin, все ще недостатня для великих корпоративних застосувань. До переходу на Proof-of-Stake (оновлення "The Merge" у вересні 2022 року) мережа обробляла приблизно 15 транзакцій на секунду [44]. Після переходу пропускна здатність базового шару залишилася подібною, хоча Layer-2 рішення (такі як rollups) обіцяють значно підвищити цей показник. Однак для приватної лікарні покладатися на складну інфраструктуру Layer-2 означає додаткові ризики та складність [45].

По-третє, модель оплати транзакцій через "газ" (gas) створює фінансові та операційні виклики. Кожна операція в Ethereum - від запису даних до виклику функції смарт-контракту - споживає обчислювальні ресурси мережі, які вимірюються в "газі". Користувач платить за газ у власній криптовалюті мережі (Ether, ETH). Вартість газу не є фіксованою, а визначається аукціоном: коли мережа перевантажена, користувачі конкурують, пропонуючи вищу ціну за газ, що призводить до різких стрибків вартості [46]. Під час криптовалютних бумів 2021

року вартість однієї транзакції в Ethereum могла досягати 50-200 доларів, що робило навіть прості операції економічно нераціональними [47]. Для лікарні, що щодня генерує тисячі записів, це означало б непередбачуваний і потенційно колосальний бюджет на "паливо" для блокчейну, що є абсолютно неприйнятним для планування витрат.

Однак Ethereum пропонує альтернативу публічній мережі: приватні (private) або консорціумні (consortium) блокчейни на базі Ethereum. Використовуючи спеціалізовані фреймворки, такі як Quorum (розроблений JP Morgan, заснований на Ethereum) або Hyperledger Besu (реалізація EVM від Hyperledger), можна створити закриту мережу з контрольованим доступом [48]. Такі мережі можуть значно підвищити продуктивність (тисячі TPS), забезпечити кращу конфіденційність через приватні транзакції та усунути потребу у криптовалюті та волатильних комісіях. Приватні Ethereum-мережі використовують ефективніші механізми консенсусу, такі як IBFT (Istanbul Byzantine Fault Tolerance) або Raft, замість Proof-of-Work.

Ця гнучкість робить Ethereum значно більш придатним для корпоративних застосувань, ніж Bitcoin. Для медичної установи приватна мережа на базі Ethereum є технічно реалізованим варіантом. Смарт-контракти на Solidity дозволять реалізувати складну логіку управління ЕМК та доступом. Однак є й недоліки: налаштування та підтримка приватної Ethereum-мережі вимагає високої кваліфікації команди розробників. Екосистема інструментів для Ethereum, хоча й величезна, орієнтована переважно на публічні мережі та DeFi-застосування, тому готових рішень саме для медичної галузі обмаль. Крім того, Ethereum не був спочатку спроектований як корпоративна платформа, тому деякі його рішення (наприклад, модель акаунтів, глобальний стан) можуть бути надлишковими або неоптимальними для завдань управління доступом та конфіденційністю в приватній мережі.

Таблиця 2.4.

Оцінка платформи Ethereum за ключовими критеріями для медичних застосувань

Критерій	**Публічний Ethereum**	**Приватний Ethereum (Quorum/Besu)**	**Коментар**
Модель доступу	Публічна	Приватна (Permissioned)	Приватні мережі дозволяють контролювати доступ
Конфіденційність	Обмежена	Поліпшена (приватні транзакції)	Quorum підтримує приватні транзакції між учасниками
Продуктивність (TPS)	~15-30 TPS (Mainnet)	100-1000+ TPS	Приватні мережі з IBFT/Raft значно швидші
Затримка транзакції	~15 секунд (блок)	Кілька секунд	Прийнятна затримка для медичних застосувань
Смарт-контракти	Повна підтримка (Solidity)	Повна підтримка (Solidity, EVM)	Можливість реалізувати складну логіку
Інтероперабельність	Обмежена	Можлива через адаптери	Потребує розробки шлюзів для інтеграції з HL7 FHIR
Механізм консенсусу	PoS (з 2022)	IBFT / Raft (ефективні)	Ефективні для корпоративних мереж
Вартість транзакцій	Висока і волатильна (газ)	Відсутня (немає газу в приватній мережі)	Приватні мережі усувають проблему вартості
Зрілість платформи	Висока (Mainnet)	Середня (корпоративні версії)	Велика спільнота, але корпоративні версії менш зрілі
Складність розгортання	Середня	Висока	Потребує досвідченої команди
ПІДСУМОК (публічний)	НЕПРИДАТНИЙ	МОЖЛИВИЙ, але з застереженнями	Публічний Ethereum не підходить. Приватний - можливий варіант, але не оптимальний

Підсумовуючи, Ethereum представляє значний крок вперед порівняно з Bitcoin

завдяки смарт-контрактам. Публічна мережа Ethereum неприйнятна для медичних даних через відкритість та вартість. Приватні реалізації на базі Ethereum (Quorum, Besu) є технічно прийнятним, але не оптимальним рішенням: вони можуть забезпечити необхідну функціональність, але вимагають значних зусиль для налаштування, не мають вбудованої підтримки специфічних для медицини стандартів і не були спочатку спроектовані з прицілом на корпоративну конфіденційність. Існує інше рішення, створене з нуля саме для таких завдань.

2.3.3. Hyperledger Fabric: корпоративний блокчейн, створений для конфіденційності

Hyperledger Fabric - це відкрита (open-source) модульна платформа для побудови приватних (permissioned) блокчейн-мереж, розроблена під егідою Hyperledger - проєкту Linux Foundation, започаткованого у 2015 році [52]. На відміну від Bitcoin та Ethereum, що створювалися як публічні, децентралізовані системи для роботи в довірливому середовищі, Fabric з самого початку проектувався для задоволення потреб підприємств, які працюють у контрольованих, але багатоорганізаційних середовищах [53]. Серед ранніх і найбільш активних учасників розробки були IBM, Intel, SAP, що визначило корпоративний фокус платформи. Перша продакшн-готова версія (v1.0) була випущена у липні 2017 року, і з тих пір платформа стабільно розвивається, отримуючи регулярні оновлення та розширення функціоналу [54].

Фундаментальною відмінністю Hyperledger Fabric є його приватна, permissioned архітектура. Це означає, що кожен учасник мережі - чи то індивідуальний користувач, чи організація, чи програмний компонент - має бути ідентифікований і авторизований для приєднання та виконання певних дій [55]. Ідентифікація відбувається через систему управління членством (Membership Service Provider, MSP), яка базується на інфраструктурі відкритих ключів (PKI) і використовує цифрові сертифікати стандарту X.509. Кожен учасник отримує сертифікат від довіреного Центру сертифікації (Certificate Authority, CA), який містить інформацію про його ідентичність, організаційну приналежність та набір атрибутів

(ролей) [56]. Це кардинально відрізняється від анонімності публічних блокчейнів і повністю відповідає вимогам медичного закладу, де кожна дія має бути однозначно пов'язана з конкретною особою для цілей аудиту та юридичної відповідальності.

Другою ключовою особливістю є механізм каналів (channels), який забезпечує безпрецедентний рівень конфіденційності на рівні архітектури [57]. Канал - це, по суті, окремий, ізольований леджер (блокчейн), доступ до якого мають лише ті організації, які були явно запрошені до цього каналу. Транзакції в одному каналі абсолютно невидимі для учасників інших каналів. Це дозволяє реалізувати складні сценарії приватності. Наприклад, у мережі лікарні можна створити:

— Загальний канал для внутрішньої адміністрації, де зберігається неперсоніфікована статистика, розклади, закупівлі.
— Окремі приватні канали для кожної пари "лікар-пацієнт", де зберігаються всі деталі консультацій та діагнозів. Жоден інший лікар, адміністратор чи працівник лікарні не матиме доступу до цього каналу без явного дозволу пацієнта [58].
— Спеціалізований канал для взаємодії з страховою компанією, де лікарня може передавати фінансову інформацію (рахунки, підтвердження послуг) без розкриття клінічних деталей.

Ця можливість створювати "блокчейн всередині блокчейну" є унікальною для Fabric і неможлива в публічних системах [59].

Додатково, Fabric пропонує механізм приватних даних (Private Data Collections, PDC), який дозволяє зберігати певні дані лише на вузлах обраних учасників каналу, тоді як інші учасники цього ж каналу отримують доступ лише до хешу цих даних [60]. Це надає ще один рівень гранулярності: навіть у спільному каналі можна приховати частину інформації від деяких учасників.

Третьою важливою особливістю є модульна архітектура Fabric, яка дозволяє замінювати та налаштовувати ключові компоненти системи відповідно до специфічних вимог [61]. Це включає:

— Механізм консенсусу: Fabric не "зашитий" на один алгоритм. Підтримуються різні варіанти, від простого Solo (для тестування) до відмовостійких Raft

(crash fault tolerance) та BFT-подібних алгоритмів (Byzantine fault tolerance) [62]. Для приватної мережі лікарні, де учасники довіряють один одному (або принаймні не очікують злонамірної поведінки), ефективного і швидкого Raft цілком достатньо.

— База даних світового стану: За замовчуванням використовується LevelDB, але можна налаштувати CouchDB, яка підтримує складні JSON-запити, що дуже зручно для пошуку та аналітики медичних записів [63].

— Політики підтвердження (Endorsement Policies): Можна гнучко налаштовувати, які організації або вузли мають підтвердити (endorses) транзакцію, щоб вона вважалася валідною. Наприклад, можна вимагати, щоб запис про постановку діагнозу був підтверджений підписами як лікуючого лікаря, так і завідувача відділення [64].

Четвертою особливістю є унікальна архітектура обробки транзакцій "Execute-Order-Validate", яка відрізняється від традиційної моделі "Order-Execute" в Ethereum [65]. У Fabric транзакція спочатку виконується на обраних вузлах (endorsing peers) як симуляція, без зміни стану леджера. Вузли підписують результат (endorsement). Потім ці підписані результати відправляються до служби упорядкування (ordering service), яка створює послідовність транзакцій і пакує їх у блоки. Нарешті, усі вузли (committing peers) отримують блок, перевіряють, чи відповідає транзакція політиці підтвердження, і лише тоді застосовують зміни до свого леджера [66]. Така архітектура дозволяє паралельно виконувати транзакції, що значно підвищує пропускну здатність до тисяч транзакцій на секунду, і гарантує детерміністичність та фінальність транзакцій за лічені секунди [67].

П'ята ключова перевага - відсутність власної криптовалюти та токенів. Hyperledger Fabric - це не криптовалютна платформа, а інструмент для управління даними та бізнес-процесами [68]. Це означає, що лікарні не потрібно купувати, зберігати і турбуватися про волатильність цін якихось токенів для оплати транзакцій. Немає концепції "газу". Вартість експлуатації системи визначається виключно вартістю серверів, мережевої інфраструктури та праці IT-персоналу, що робить бюджетування простим і передбачуваним.

Шостою особливістю є підтримка смарт-контрактів (які в термінології Fabric називаються "чейнкод", chaincode), написаних на універсальних мовах програмування, таких як Go, Java, JavaScript (Node.js) [69]. Це значно спрощує вхідний бар'єр для розробників порівняно зі специфічною Solidity в Ethereum. Більшість корпоративних команд вже мають досвід з цими мовами. Чейнкод виконується в ізольованому середовищі (Docker-контейнери), що забезпечує безпеку та можливість використання складних бібліотек для валідації даних, інтеграції з зовнішніми API або роботи зі стандартами, такими як HL7 FHIR [70].

Сьомий аспект - це зрілість платформи та активна екосистема. Hyperledger Fabric має велику і постійно зростаючу спільноту розробників, детальну документацію, численні туторіали та приклади коду [71]. Платформа використовується в продакшн-середовищах провідними корпораціями та урядами по всьому світу у найрізноманітніших галузях: від фінансів (Visa, Nasdaq) до ланцюгів постачання (Walmart, Maersk) і охорони здоров'я. Наприклад, американський проєкт Change Healthcare використовує Hyperledger Fabric для обробки мільйонів медичних заяв та транзакцій, що доводить масштабованість та надійність платформи для медичних застосувань [72].

Таблиця 2.5.

Оцінка платформи Hyperledger Fabric за ключовими критеріями для медичних застосувань

Критерій	**Оцінка Hyperledger Fabric**	**Коментар**
Модель доступу	Приватна (Permissioned)	Ідеально для медицини: всі учасники ідентифіковані через PKI/X.509
Конфіденційність	Дуже висока (канали + PDC)	Унікальний механізм каналів та приватних даних забезпечує гранулярний контроль
Продуктивність (TPS)	1000-10,000+ TPS	Архітектура "Execute-Order-Validate" забезпечує високу пропускну здатність
Затримка транзакції	<1-3 секунди	Детермінований і швидкий консенсус (Raft)
Смарт-контракти	Повна підтримка (Go, Java, Node.js)	Чейнкод на універсальних мовах, легкість розробки

Інтероперабельність	Висока	Легко інтегрується з існуючими системами, підтримка API, можливість роботи з FHIR
Механізм консенсусу	Модульний (Raft, BFT)	Ефективні і швидкі алгоритми для корпоративних мереж
Вартість транзакцій	✓ Відсутня (немає криптовалюти)	Передбачувана вартість володіння (TCO) без волатильності
Зрілість платформи	Висока (корпоративний фокус)	Активна спільнота, Linux Foundation, численні продакшн-кейси в медицині
Складність розгортання	Середня-Висока	Потребує кваліфікованої команди, але є багато інструментів і документації
Антикорупційний потенціал	Дуже високий	Незмінність, прозорий аудиторський слід, гранулярний контроль доступу
Відповідність GDPR/законодавству	Повна	Архітектура дозволяє реалізувати всі вимоги щодо захисту персональних даних
ПІДСУМОК	ОПТИМАЛЬНИЙ ВИБІР	Hyperledger Fabric ідеально підходить для створення системи ЕМК в лікарні

Hyperledger Fabric був створений саме для тих завдань, які стоять перед приватною лікарнею: безпечне управління чутливими даними в багатоорганізаційному середовищі з суворим контролем доступу, високою продуктивністю та відповідністю регуляторним вимогам. Всі його архітектурні рішення - від приватної моделі доступу та каналів до модульності та відсутності криптовалюти - спрямовані на забезпечення потреб підприємств, зокрема в медичній галузі [73].

Таблиця 2.6.

Зведена порівняльна таблиця блокчейн-платформ для медичних застосувань

Критерій / Платформа	**Bitcoin**	**Ethereum (публічний)**	**Ethereum (приватний)**	**Hyperledger Fabric**
Модель доступу	Публічна	Публічна	Приватна	Приватна
Конфіденційність	Відсутня	Обмежена	Поліпшена	Дуже висока (канали, PDC)

Продуктивність (TPS)	3-7	15-30	100-1000	1000-10,000+
Затримка	10-60 хв	~15 сек	Кілька сек	<1-3 сек
Смарт-контракти	Відсутні	Solidity (Turing-complete)	Solidity	Go/Java/Node.js
Інтероперабельність	Відсутня	Обмежена	Можлива	Висока
Консенсус	PoW (повільний)	PoS	IBFT/Raft	Raft/BFT (модульний)
Вартість транзакцій	Висока, волатильна	Висока, волатильна (газ)	Відсутня	Відсутня
Криптовалюта	Так (BTC)	Так (ETH)	Може бути відсутня	Немає
Зрілість (корпоративна)	Низька	Середня	Середня	Висока
Антикорупційний потенціал	Низький (для медицини)	Середній	Високий	Дуже високий
Відповідність GDPR	Неможлива	Складна	Можлива	Повна
ВИСНОВОК	НЕПРИДАТНИЙ	НЕПРИДАТНИЙ	МОЖЛИВИЙ	ОПТИМАЛЬНИЙ

2.4. Вибір оптимальної платформи

На основі детального порівняльного аналізу трьох провідних блокчейн-платформ за сукупністю технічних, функціональних, безпекових, економічних та регуляторних критеріїв, можна зробити однозначний висновок: Hyperledger Fabric є єдиним оптимальним вибором для створення системи управління електронними медичними картками в приватній лікарні в Україні.

Bitcoin, попри свою історичну значущість як піонера блокчейн-технології та найнадійнішої криптовалюти, абсолютно непридатний для управління медичними даними. Його публічна, псевдоанонімна природа прямо суперечить законодавчим вимогам конфіденційності. Відсутність підтримки смарт-контрактів унеможливлює реалізацію складної бізнес-логіки. Критично низька продуктивність (3-7 TPS) та довга затримка транзакцій (десятки хвилин) робили б систему абсолютно непрацездатною для щоденних операцій лікарні. Високі та непередбачувані комісії, енергозатратний Proof-of-Work - всі ці фактори виключають Bitcoin з розгляду.

Ethereum публічний представляє значний прогрес завдяки введенню смарт-контрактів на Solidity, що дозволяє програмувати складні сценарії. Однак він наслідує фундаментальний недолік Bitcoin - публічність мережі, що робить його неприйнятним для конфіденційних медичних даних. Продуктивність публічного Ethereum, хоч і вища за Bitcoin (~15-30 TPS), недостатня для великих навантажень. Модель оплати через "газ" з волатильними цінами створює бюджетні ризики. Перехід на Proof-of-Stake покращив енергоефективність, але не вирішив проблем конфіденційності та вартості.

Приватний Ethereum (на основі фреймворків Quorum або Hyperledger Besu) усуває багато недоліків публічної версії. Контрольована мережа дозволяє обмежити доступ, підвищити продуктивність до сотень і тисяч TPS, прибрати проблему волатильності вартості газу та використовувати ефективні консенсус-алгоритми (IBFT, Raft). З'являється підтримка приватних транзакцій, що підвищує конфіденційність. Для медичного закладу це технічно реалізований варіант. Однак є суттєві застереження. По-перше, екосистема Ethereum історично розвивалася

навколо публічних застосувань (DeFi, NFT), тому корпоративні версії менш зрілі, документовані та підтримувані. По-друге, Ethereum не був спроектований з урахуванням специфічних потреб корпорацій щодо гранулярної конфіденційності на рівні архітектури (немає аналогу каналів Fabric). По-третє, налаштування приватної Ethereum-мережі, особливо з інтеграцією механізмів приватності, вимагає високої кваліфікації команди.

Hyperledger Fabric, на противагу, був створений з нуля як корпоративна блокчейн-платформа для роботи з конфіденційними даними в багатоорганізаційних приватних мережах. Кожен аспект його дизайну відповідає вимогам, що постають перед медичним закладом:

1. Приватність на рівні архітектури: Система управління членством (MSP) з X.509-сертифікатами забезпечує ідентифікацію всіх учасників. Механізм каналів дозволяє створювати ізольовані леджери для різних груп учасників, що ідеально підходить для реалізації моделі "лікар-пацієнт". Приватні дані (PDC) надають додатковий рівень контролю. Це забезпечує повну відповідність вимогам GDPR та українського законодавства щодо захисту медичної таємниці [77].
2. Висока продуктивність: Архітектура "Execute-Order-Validate" з паралельним виконанням транзакцій та ефективними консенсус-алгоритмами (Raft) забезпечує пропускну здатність у тисячі TPS з затримкою менше 3 секунд. Це більш ніж достатньо для будь-якої лікарні з запасом на майбутнє масштабування [78].
3. Гнучкість розробки: Чейнкод на Go, Java або Node.js дозволяє легко знайти розробників і реалізувати складну логіку управління доступом, валідації даних, інтеграції зі стандартами HL7 FHIR. Модульна архітектура дозволяє налаштовувати політики підтвердження, бази даних, консенсус під конкретні потреби [79].
4. Відсутність криптовалюти: Немає токенів, немає волатильності, немає непередбачуваних витрат на "паливо". Вартість володіння системою

визначається виключно інфраструктурними та персональними витратами, що спрощує фінансове планування [80].

5. Антикорупційний ефект: Незмінність записів у блокчейні робить підробку медичних довідок або заднім числом зміну діагнозів практично неможливою. Кожна дія залишає незмінний цифровий слід з підписом автора і часовою міткою. Аудитори можуть отримати доступ до окремого каналу для перевірки справжності будь-якого документа. Це прямо протидіє корупційним практикам, що історично були проблемою української медицини [81].
6. Зрілість та підтримка: Hyperledger Fabric має потужну підтримку Linux Foundation, велику спільноту, детальну документацію та численні успішні кейси впровадження саме в медичній галузі (Change Healthcare, Hashed Health, MedRec та інші проєкти) [82].
7. Масштабованість: Система може починати з одної лікарні, а згодом розширюватися на мережу лікарень або інтегруватися з національною системою eHealth, зберігаючи модель безпеки та конфіденційності [83].

Жоден з недоліків Hyperledger Fabric не є критичним. Складність розгортання вища, ніж у централізованої системи, але вона компенсується наявністю інструментів (Hyperledger Cello, Kubernetes Operators), детальних туторіалів та можливістю залучення спеціалізованих консалтингових компаній на етапі впровадження. Початкові інвестиції в навчання команди окупляться через підвищену безпеку, довіру пацієнтів та зниження корупційних ризиків [84].

Таким чином, обґрунтований вибір для приватної лікарні в Україні - це Hyperledger Fabric. Це рішення не є компромісом, а є платформою, яка спеціально створена для таких завдань і забезпечує найвищий рівень відповідності як технічним, так і юридичним, етичним та бізнесовим вимогам.

Рис. 2.7 «Рішення для медичної установи: чому Hyperledger Fabric»

2.5. Архітектура запропонованого рішення

Після обґрунтованого вибору Hyperledger Fabric як технологічної основи, наступним критично важливим етапом є проектування детальної архітектури системи управління електронними медичними картками для приватної лікарні. Ця архітектура має бути не лише технічно коректною, але й максимально відповідати реальним робочим процесам медичного закладу, забезпечувати безшовну інтеграцію з існуючими інформаційними системами та створювати надійний фундамент для майбутнього розширення.

2.5.1. Учасники мережі (Organizations) та їхні ролі

Блокчейн-мережа на базі Hyperledger Fabric будується навколо концепції організацій-учасників. Кожна організація має власну інфраструктуру, вузли (peers), політики безпеки та ідентичності. Для системи ЕМК приватної лікарні пропонується наступна структура учасників [85]:

1. HospitalOrg (Організація лікарні) - це основний учасник мережі, що представляє саму лікарню як юридичну особу. Ця організація керуватиме декількома вузлами (peer nodes), на яких зберігатимуться копії леджерів та виконуватиметься чейнкод. Усередині HospitalOrg будуть визначені різні ролі користувачів з різними рівнями доступу:

— Лікарі: Мають право створювати та оновлювати медичні записи пацієнтів, яким вони надають допомогу.

— Медсестри та молодший медперсонал: Можуть мати обмежений доступ - наприклад, вносити показники життєдіяльності, результати вимірювань, але не мають права встановлювати діагнози.

— Адміністратори лікарні: Керують технічною інфраструктурою мережі, реєструють нових користувачів, але не мають прямого доступу до конфіденційних медичних даних пацієнтів без спеціального дозволу (принцип розділення обов'язків).

— Керівництво відділень: Може мати доступ до агрегованої, знеособленої статистики для управлінських рішень [86].

2. PatientOrg (Організація пацієнтів) - логічна група, що представляє пацієнтів. Хоча пацієнти як приватні особи не розгортають власну блокчейн-інфраструктуру, вони отримують унікальні цифрові ідентичності (X.509 сертифікати) від CA лікарні. Через зручний клієнтський додаток (мобільний або веб) пацієнти можуть:

— Переглядати власну повну медичну історію.
— Надавати доступ до своєї ЕМК іншим лікарям (наприклад, при зверненні до спеціаліста з іншої лікарні або для отримання "другої думки").
— Відкликати наданий доступ.
— Переглядати аудиторський журнал: хто, коли і які дані переглядав чи змінював.

3. InsuranceOrg (Організація страхових компаній) - один або кілька учасників, що представляють страхові компанії, з якими співпрацює лікарня. Вони приєднуються до мережі для автоматизованої обробки страхових випадків. InsuranceOrg матиме доступ лише до обмеженого набору каналів, де передаються фінансові та процедурні дані (коди послуг, рахунки, підтвердження факту надання медичної допомоги), але без доступу до клінічних деталей (діагнозів, результатів аналізів, анамнезу) [88].

4. AuditorOrg (Організація регуляторів/аудиторів) - представники державних органів (наприклад, Міністерства охорони здоров'я України, регіональних управлінь охорони здоров'я) або незалежні аудиторські компанії. Вони можуть бути запрошені до спеціального read-only (лише для читання) каналу, що дозволяє їм перевіряти відповідність процесів нормативним вимогам, але зі строгим обмеженням доступу до персональних даних (наприклад, лише до анонімізованих або агрегованих даних, або до конкретних записів за судовим рішенням).

2.5.2. Топологія вузлів та інфраструктура

Фізична топологія мережі складається з кількох типів вузлів, кожен з яких виконує специфічні функції [90]:

Peer nodes (Вузли-учасники): Це основні робочі одиниці мережі. Кожна організація розгортає один або кілька peer-вузлів. Для HospitalOrg рекомендується

розгорнути мінімум 3-5 peer-вузлів для забезпечення високої доступності та розподілення навантаження. Peer-вузли виконують дві функції:

- Endorsing peers (Підтверджуючі): Виконують чейнкод (симулюють транзакцію) і підписують результат своїм сертифікатом. Політика підтвердження (endorsement policy) визначає, скільки і яких peers мають підтвердити транзакцію (наприклад, "мінімум 2 з 5 peers HospitalOrg").
- Committing peers (Зберігаючі): Отримують упорядковані блоки від ordering service, валідують транзакції всередині блоків і додають їх до свого леджера [91].

Ordering Service (Служба упорядкування): Відповідає за консенсус - отримання транзакцій від peers, домовленість про їхній порядок та створення блоків. Для забезпечення відмовостійкості рекомендується використовувати Raft-based ordering service з мінімум 3-5 orderer-вузлів (краще непарна кількість для алгоритму Raft). Ці вузли можуть розташовуватися на окремих серверах в дата-центрі лікарні або в хмарній інфраструктурі [92].

Certificate Authority (CA, Центр сертифікації): Кожна організація має власний CA-сервер (Fabric CA), який відповідає за видачу, оновлення та відкликання сертифікатів для всіх користувачів та вузлів організації. CA є довіреною основою системи ідентифікації. Рекомендується розгортати CA в захищеному середовищі з резервуванням [93].

2.5.3. Канали та модель конфіденційності

Канали є ключовим механізмом для забезпечення конфіденційності. Пропонується створити кілька типів каналів:

1. Main Hospital Channel (Головний канал лікарні): Об'єднує всі peer-вузли HospitalOrg. У цьому каналі зберігаються загальні, неперсоніфіковані дані: довідники медичних процедур, реєстр обладнання, розклади, журнали адміністративних подій. Доступ мають всі співробітники лікарні відповідно до їхніх ролей.

2. Patient-Doctor Private Channels (Приватні канали "Пацієнт-Лікар"): Для

кожного унікального зв'язку пацієнта з його лікуючим лікарем (або групою лікарів, що ведуть пацієнта) створюється динамічний приватний канал. У цьому каналі зберігаються всі конфіденційні деталі: анамнез, діагнози, призначення, результати аналізів. Жоден інший учасник мережі, крім цього пацієнта та уповноважених лікарів, не має доступу до леджера цього каналу. Якщо пацієнт надає доступ іншому лікарю (наприклад, для консультації), цей лікар додається до каналу, або створюється новий спільний канал [95].

3. Insurance Channel (Канал для страхування): Окремий канал між HospitalOrg та InsuranceOrg. У цьому каналі лікарня передає лише ту інформацію, що необхідна для обробки страхової заяви: коди процедур (наприклад, за класифікатором ICD-10), дати надання послуг, вартість. Медичні деталі (чому було призначено процедуру, результати) залишаються в приватному каналі пацієнта [96].

4. Audit Channel (Аудиторський канал): Read-only канал для AuditorOrg. Аудитори можуть переглядати метадані транзакцій (хто, коли, який тип операції виконав) для перевірки відповідності, але самі медичні дані можуть бути зашифровані або видані лише за окремим запитом і дозволом пацієнта.

2.5.4. Леджер та модель даних

Леджер у Hyperledger Fabric складається з двох компонентів [98]:

World State (Світовий стан) - це база даних ключ-значення, що містить поточний стан всіх активів. Рекомендується використовувати CouchDB як базу даних світового стану, оскільки вона підтримує складні JSON-запити, що дозволить ефективно шукати пацієнтів за різними критеріями (ім'я, дата народження, номер страхового полісу) [99].

Blockchain (Транзакційний лог) - незмінний ланцюг блоків, що зберігає повну історію всіх транзакцій. Це забезпечує повний аудиторський слід. Кожен блок містить хеш попереднього блоку, що робить зміну історії практично неможливою.

Модель даних ЕМК: Дані пацієнта будуть структуровані відповідно до стандарту HL7 FHIR (Fast Healthcare Interoperability Resources). FHIR визначає "ресурси" - стандартизовані об'єкти для представлення медичної інформації [100].

Приклади ресурсів:

- Patient: Демографічні дані пацієнта (ім'я, дата народження, контакти).
- Observation: Результати спостережень (наприклад, вимірювання тиску, рівень глюкози в крові).
- Condition: Стан здоров'я або діагноз (наприклад, "Гіпертонія").
- MedicationRequest: Призначення ліків.
- DiagnosticReport: Звіт про діагностичну процедуру (наприклад, результати аналізу крові, висновок МРТ) [101].

Для оптимізації зберігання великих файлів (медичні зображення, геномні дані) використовується гібридний підхід (on-chain + off-chain):

- On-chain (у блокчейні): Зберігається FHIR-ресурс з метаданими (дата створення, автор, тип файлу) та криптографічний хеш файлу (наприклад, SHA-256). Також зберігаються права доступу до цього файлу.
- Off-chain (поза блокчейном): Сам файл зберігається в захищеному зовнішньому сховищі (може бути власний сервер лікарні з шифруванням диска або хмарне HIPAA-compliant сховище, таке як AWS S3 з відповідними налаштуваннями).

Коли користувач запитує файл, система спочатку перевіряє його права доступу через блокчейн. Якщо доступ дозволено, система отримує файл з off-chain сховища, обчислює його хеш та порівнює з хешем, збереженим у блокчейні. Якщо хеші збігаються, файл автентичний. Якщо ні - файл був підмінений, і система відхиляє його.

2.5.5. Чейнкод (Смарт-контракти) та бізнес-логіка

Чейнкод буде реалізовувати всю бізнес-логіку системи. Пропонується розробити декілька чейнкодів для різних функцій [103]:

PatientRecordChaincode: Управління ЕМК пацієнтів.

Функції:

- createPatientRecord(patientID, fhirPatientResource): Створення нового запису пацієнта при першому зверненні до лікарні. Записує FHIR Patient resource у леджер.
- addMedicalEntry(patientID, doctorID, fhirResource): Додавання нового медичного запису (Observation, Condition, MedicationRequest, тощо). Перевіряє, чи має doctorID право доступу до ЕМК цього пацієнта.
- getPatientRecord(patientID, requesterID): Отримання медичних даних пацієнта. Перевіряє права requesterID перед поверненням даних.
- getPatientHistory(patientID, requesterID): Отримання повної історії змін ЕМК з блокчейну (аудиторський слід) [104].

AccessControlChaincode: Управління правами доступу. Функції:

- grantAccess(patientID, granteeID, accessLevel, duration): Пацієнт надає доступ до своєї ЕМК іншому лікарю або організації. Створює Access Control Entry (ACE) у леджері з визначенням рівня доступу (read-only, read-write) та терміну дії.
- revokeAccess(patientID, granteeID): Пацієнт відкликає доступ. Видаляє або деактивує відповідний ACE.
- checkAccess(patientID, requesterID): Перевірка, чи має requesterID доступ до даних patientID. Використовується іншими чейнкодами перед виконанням операцій [105].

InsuranceChaincode: Обробка страхових заяв. Функції:

- createClaim(patientID, hospitalID, procedureCodes, totalCost): Лікарня створює страхову заяву на основі наданих послуг. Записується у Insurance Channel.
- approveClaim(claimID, insuranceID): Страхова компанія підтверджує заяву.
- rejectClaim(claimID, insuranceID, reason): Страхова компанія відхиляє заяву з поясненням [106].

AuditChaincode: Журналювання та аудит. Функції:

- logAccess(patientID, accessorID, action, timestamp): Автоматичне логування кожної операції доступу до ЕМК.

— queryAuditLog(patientID, startDate, endDate): Запит на отримання журналу подій для конкретного пацієнта за період [107].

Чейнкод буде написано мовою Go через її високу продуктивність, строгу типізацію та відмінну підтримку в екосистемі Hyperledger Fabric. Всі функції чейнкоду включатимуть валідацію вхідних даних, перевірку прав доступу через аналіз X.509 сертифіката ініціатора та детальне логування дій для аудиту.

Таблиця 2.8.

Основні функції чейнкоду та їх призначення

Чейнкод	**Функція**	**Призначення**	**Хто може викликати**
PatientRecord	createPatientRecord	Створення нової ЕМК	Адміністратор реєстратури
	addMedicalEntry	Додавання медичного запису	Лікар (з правами доступу)
	getPatientRecord	Отримання ЕМК	Пацієнт, уповноважений лікар
	getPatientHistory	Отримання аудиторського сліду	Пацієнт, аудитор
AccessControl	grantAccess	Надання доступу до ЕМК	Пацієнт
	revokeAccess	Відкликання доступу	Пацієнт
	checkAccess	Перевірка прав доступу	Внутрішній виклик іншими чейнкодами
Insurance	createClaim	Створення страхової заяви	Фінансовий відділ лікарні
	approveClaim	Підтвердження заяви	Страхова компанія
	rejectClaim	Відхилення заяви	Страхова компанія
Audit	logAccess	Логування операцій	Автоматично при кожній операції
	queryAuditLog	Запит журналу подій	Пацієнт, аудитор, адміністратор (з обмеженнями)

Така архітектура створює надійну, гнучку та масштабовану систему, що повністю відповідає потребам сучасної приватної лікарні в Україні та закладає фундамент для майбутньої інтеграції з іншими медичними установами та державними реєстрами.

2.6. Механізми забезпечення конфіденційності медичних даних

Конфіденційність медичних даних є не просто бажаною характеристикою, а абсолютною, юридично обов'язковою вимогою для будь-якої системи, що працює з інформацією про стан здоров'я громадян. Архітектура Hyperledger Fabric надає потужний інструментарій для створення багатошарової системи захисту конфіденційності, що поєднує ізоляцію на рівні мережі, криптографічний захист та гранулярний контроль доступу [109].

1. Ізоляція через канали (Channels): Як вже зазначалося, механізм каналів є фундаментальним інструментом конфіденційності в Fabric. Кожен канал має власний леджер, повністю незалежний від інших каналів. Учасники одного каналу не можуть бачити, які транзакції відбуваються в інших каналах, і навіть не знають про їхнє існування, якщо не є членами цих каналів [110]. У контексті медичної системи це означає, що приватний канал між лікарем А та пацієнтом Б містить інформацію, абсолютно недоступну для лікаря В, адміністратора системи або будь-якого іншого учасника мережі. Лише пацієнт Б може, за власним бажанням, надати доступ лікарю В, додавши його до каналу або створивши новий спільний канал. Цей підхід реалізує принцип "need-to-know" (доступ лише за потребою) на архітектурному рівні [111].

2. Приватні колекції даних (Private Data Collections, PDC): Іноді потрібен ще більш гранулярний рівень контролю навіть всередині каналу. Наприклад, у каналі можуть бути кілька організацій (лікарня, страхова компанія, регулятор), але лише деякі з них повинні бачити конкретну частину даних. Private Data Collections дозволяють визначити, що певні дані будуть зберігатися лише на peer-вузлах обраних організацій, тоді як інші учасники каналу отримають доступ лише до хешу цих даних [112]. Наприклад, результат тесту на ВІЛ або генетичний аналіз можна зберігати в PDC, доступній лише лікарю-інфекціоністу та пацієнту, тоді як інші лікарі в тому ж каналі побачать лише хеш та факт існування запису, але не його вміст. Це забезпечує конфіденційність на рівні, недосяжному для публічних блокчейнів [113].

3. Шифрування даних (Encryption): Хоча канали та PDC забезпечують ізоляцію, додатковий рівень захисту надає шифрування самих даних перед записом у леджер. Hyperledger Fabric підтримує використання криптографічних бібліотек на рівні чейнкоду [114]. Пропонується застосувати end-to-end шифрування для особливо чутливих полів даних (наприклад, анамнез психічних захворювань, інформація про ВІЛ-статус, генетичні дані). Це можна реалізувати наступним чином:

— Симетричне шифрування (AES-256): Кожен запис або поле шифрується за допомогою унікального симетричного ключа.

— Асиметричне шифрування для управління ключами: Симетричний ключ, у свою чергу, шифрується відкритим ключем пацієнта та відкритими ключами всіх уповноважених лікарів (з їхніх X.509 сертифікатів). Зашифровані копії симетричного ключа зберігаються в леджері.

Доступ до даних: Лише ті учасники, чиї приватні ключі можуть розшифрувати симетричний ключ, зможуть потім розшифрувати самі дані [115].

Такий підхід забезпечує, що навіть якщо зловмисник отримає фізичний доступ до серверів з леджером, він побачить лише зашифровані дані, які неможливо прочитати без приватних ключів уповноважених осіб.

4. Контроль доступу на основі атрибутів (Attribute-Based Access Control, ABAC): Система управління ідентифікацією Fabric (MSP) дозволяє включати в X.509 сертифікати користувачів атрибути, що описують їхні ролі, посади, відділення, спеціалізацію [117]. Чейнкод може приймати рішення про надання доступу на основі цих атрибутів.

Наприклад:

— Лише користувач з атрибутом role=doctor може викликати функцію addMedicalEntry.

— Лише користувач з атрибутом role=patient може викликати grantAccess для своєї власної ЕМК.

Користувач з атрибутом department=cardiology може мати доступ до

агрегованої кардіологічної статистики, але не до конкретних ЕМК пацієнтів інших відділень.

Це дозволяє реалізувати складні, гнучкі політики доступу, що автоматично адаптуються до організаційної структури лікарні без необхідності вручну управляти доступом для кожного окремого користувача.

5. Анонімізація та псевдонімізація даних: Для випадків, коли дані потрібні для дослідницьких або статистичних цілей, але без ідентифікації конкретних пацієнтів (що відповідає вимогам GDPR щодо мінімізації обробки персональних даних), можна створити окремий канал або функції чейнкоду, що повертають анонімізовані або псевдонімізовані дані [120].

Наприклад:

— Анонімізація: Видалення всіх прямих ідентифікаторів (ім'я, дата народження, адреса) та узагальнення інших полів (наприклад, точний вік замінюється віковою групою "50-60 років").

— Псевдонімізація: Заміна реальних ідентифікаторів на псевдоніми (унікальні, але не зв'язані з реальною особою коди). Зв'язок псевдоніма з реальною особою зберігається окремо під подвійним захистом і може бути відновлений лише за надзвичайних обставин (наприклад, за судовим рішенням) [121].

6. Zero-Knowledge Proofs (Доведення з нульовим розголошенням): Це передовий криптографічний метод, що дозволяє довести факт володіння певною інформацією або її відповідність певним критеріям без розкриття самої інформації [122]. Наприклад, лікарня може довести страховій компанії, що пацієнт дійсно отримав конкретну процедуру (для обробки страхової заяви), не розкриваючи при цьому діагноз, який став причиною цієї процедури. Хоча впровадження ZKP є технічно складним і ресурсозатратним, воно може бути доцільним для найбільш чутливих сценаріїв у майбутніх ітераціях системи [123].

Ця комплексна, багатошарова стратегія забезпечення конфіденційності гарантує, що система не лише відповідає, а й перевершує вимоги GDPR та українського законодавства, створюючи довірче середовище, де пацієнти можуть бути впевнені в абсолютній недоторканності своїх найінтимніших даних.

2.7. Управління доступом на основі блокчейну

Система управління доступом є серцевиною будь-якого рішення для захисту конфіденційних даних. Запропонована архітектура на базі Hyperledger Fabric реалізує багаторівневу, гранулярну та керовану пацієнтом модель контролю доступу, що поєднує криптографічну ідентифікацію, рольовий доступ (RBAC), доступ на основі атрибутів (ABAC) та динамічне управління дозволами [125].

Рівень 1: Ідентифікація та автентифікація (Identity Layer): Вся система доступу будується на фундаменті довірених цифрових ідентичностей. Кожен користувач і кожен вузол у мережі має унікальний X.509 сертифікат, виданий та підписаний довіреним Центром сертифікації (CA) відповідної організації [126]. Коли користувач намагається виконати будь-яку операцію (наприклад, лікар хоче додати запис до ЕМК), він підписує запит своїм приватним ключем. Система перевіряє цей підпис за допомогою відкритого ключа з сертифіката, забезпечуючи автентифікацію (підтвердження, що запит дійсно надійшов від цієї особи, а не від зловмисника) [127]. Сертифікат також містить атрибути, що описують роль та повноваження користувача, які використовуються для авторизації (визначення, чи має ця особа право виконати запитувану дію).

Рівень 2: Рольовий контроль доступу (RBAC - Role-Based Access Control): Користувачі групуються за ролями, кожна з яких має попередньо визначений набір дозволів [128]. Основні ролі в системі:

— Patient (Пацієнт):
    — Дозволено: Переглядати власну ЕМК, переглядати журнал доступу до своєї ЕМК, надавати доступ іншим лікарям/організаціям (grantAccess), відкликати доступ (revokeAccess), завантажувати копії своїх медичних документів.
    — Заборонено: Змінювати медичні записи, створені лікарями (принцип цілісності даних), переглядати ЕМК інших пацієнтів.
— Doctor (Лікар):
    — Дозволено: Переглядати ЕМК пацієнтів, за якими він закріплений або яким пацієнт надав доступ, додавати нові медичні записи

(addMedicalEntry), оновлювати власні попередні записи (з фіксацією історії змін), призначати ліки, направлення на аналізи.

— Заборонено: Переглядати ЕМК пацієнтів без дозволу, змінювати записи інших лікарів, видаляти записи з леджера (лише позначення як "неактуальний" з поясненням причини) [129].

— Nurse (Медсестра):

— Дозволено: Переглядати обмежену частину ЕМК (призначення, які потрібно виконати), вносити показники життєдіяльності (тиск, температура, пульс), результати вимірювань.

— Заборонено: Встановлювати діагнози, призначати ліки, переглядати повну медичну історію.

— Administrator (Адміністратор системи):

— Дозволено: Керувати інфраструктурою блокчейн-мережі, реєструвати нових користувачів, видавати сертифікати, моніторити продуктивність системи, доступ до технічних логів.

— Заборонено: Прямий доступ до конфіденційних медичних даних пацієнтів (принцип розділення обов'язків) [130].

— Auditor (Аудитор):

— Дозволено: Переглядати метадані транзакцій (хто, коли, яку операцію виконав), аналізувати анонімізовані або агреговані дані, доступ до повних ЕМК лише за спеціальним дозволом (наприклад, при розслідуванні інциденту).

— Заборонено: Змінювати будь-які дані, доступ до конфіденційної інформації без належних підстав.

Рівень 3: Доступ на основі атрибутів (ABAC - Attribute-Based Access Control): RBAC визначає загальні дозволи для ролі, але ABAC додає гнучкість, дозволяючи приймати рішення про доступ на основі додаткових атрибутів користувача, ресурсу та контексту [131]. Приклади:

— Атрибут department=cardiology у сертифікаті лікаря може надавати йому автоматичний доступ до кардіологічної статистики або ЕМК пацієнтів, госпіталізованих у кардіологічному відділенні.
— Атрибут specialization=oncologist може вимагатися для доступу до особливо чутливих онкологічних записів.
— Контекстні атрибути (час доступу, місцезнаходження) можуть використовуватися для додаткової перевірки. Наприклад, доступ до системи з IP-адреси поза мережею лікарні може вимагати додаткової автентифікації [132].

Рівень 4: Динамічне управління доступом, кероване пацієнтом (Patient-Controlled Access): Це найінноваційніший аспект системи. Пацієнт не є пасивним об'єктом, дані якого контролюються лікарнею, а активним власником своїх даних. Через зручний мобільний або веб-додаток пацієнт може:

— Переглядати поточні дозволи: Хто має доступ до його ЕМК, який рівень доступу (read-only чи read-write), коли доступ було надано, чи є термін дії.
— Надавати тимчасовий доступ: Наприклад, пацієнт, який консультується у спеціаліста з іншої лікарні, може надати цьому лікарю доступ на 30 днів. Після закінчення терміну доступ автоматично відкликається.
— Надавати обмежений доступ: Пацієнт може дозволити лікарю бачити лише певні розділи ЕМК (наприклад, лише результати кардіологічних обстежень, але не психіатричний анамнез).
— Відкликати доступ миттєво: У будь-який момент пацієнт може відкликати доступ, і система негайно заборонить подальші запити від цього лікаря.
— Отримувати сповіщення: Пацієнт отримує push-сповіщення на мобільний телефон кожного разу, коли хтось отримує доступ до його ЕМК, що дозволяє негайно виявити несанкціоновані спроби [134].

Ця модель повністю відповідає вимогам GDPR щодо права на доступ, права на портативність даних та права контролювати обробку своїх персональних даних.

Таблиця 2.9.

Матриця прав доступу за ролями

Роль \ Операція	**Переглядати власну ЕМК**	**Переглядати чужу ЕМК**	**Додавати медичний запис**	**Змінювати власний запис**	**Змінювати чужий запис**	**Надавати доступ**	**Відкликати доступ**	**Переглядати журнал доступу**	**Керувати інфраструктурою**
Patient	✓	×	×	×	×	✓ (до власної ЕМК)	✓ (до власної ЕМК)	✓ (власної ЕМК)	×
Doctor	✓	✓ (з дозволом)	✓ (з дозволом)	✓ (з фіксацією історії)	×	×	×	✓ (обмежений)	×
Nurse	✓	✓	✓	✓	×	×	×	×	×
Administrator	✓	× (без спец. дозволу)	×	×	×	×	×	✓ (технічний лог)	✓
Auditor	×	✓ (анонімізовані/за дозволом)	×	×	×	×	×	✓ (повний лог метаданих)	×
Insurance	×	✓ (лише фінансові дані, без діагнозів)	×	×	×	×	×	×	×

Рівень 5: Аудиторський слід та недозволеність відмови (Non-Repudiation): Кожна транзакція в блокчейні підписується приватним ключем ініціатора і фіксується в незмінному леджері з позначкою часу [136]. Це створює абсолютно надійний, криптографічно захищений аудиторський слід, який доводить:

— Хто виконав дію (ідентичність з сертифіката).

— Що саме було зроблено (тип операції, які дані були змінені).

— Коли (точна часова мітка, що не може бути змінена).

Чому (опціонально, коментар до операції).

Ініціатор дії не може пізніше заперечувати свою причетність (non-repudiation), оскільки його цифровий підпис є незаперечним доказом. Це критично важливо для юридичної відповідальності та боротьби з внутрішніми загрозами [137].

Така комплексна система управління доступом робить систему практично непроникною для несанкціонованого доступу і водночас зручною та гнучкою для законних користувачів.

2.8. Інтеграція з існуючими медичними інформаційними системами

Успішне впровадження блокчейн-рішення в лікарні залежить не лише від його технічної досконалості, але й від здатності безшовно інтегруватися з існуючою IT-екосистемою. Сучасна лікарня використовує безліч спеціалізованих систем: Медичну інформаційну систему (МІС) для ведення пацієнтів, Лабораторну інформаційну систему (ЛІС), Радіологічну інформаційну систему (РІС), систему управління фармацією, фінансову систему та іншими [138]. Блокчейн не покликаний замінити ці системи, а має стати надійним шаром забезпечення довіри, цілісності та контрольованого обміну даними між ними [139].

Роль стандарту HL7 FHIR: Ключем до інтероперабельності в медичній галузі є міжнародний стандарт HL7 FHIR (Fast Healthcare Interoperability Resources) [140]. FHIR визначає:

— Стандартизовану структуру даних: Медична інформація представляється у вигляді "ресурсів" - простих, модульних об'єктів (Patient, Observation, Condition, MedicationRequest, тощо), описаних у форматі JSON або XML.
— RESTful API: FHIR базується на стандартних HTTP-методах (GET, POST, PUT, DELETE), що робить інтеграцію інтуїтивною для розробників.
— Семантичну сумісність: Використання стандартизованих словників (наприклад, SNOMED CT для діагнозів, LOINC для лабораторних аналізів) забезпечує, що системи різних вендорів "розуміють" одне одного [141].

Архітектура інтеграції: Пропонується гібридна архітектура, де блокчейн співіснує з традиційними базами даних через шар API Gateway (шлюз) [142]:

1. Існуюча МІС (наприклад, BIT Master від компанії "БІТ", "Медзошит", або зарубіжні системи як Epic, Cerner) продовжує виконувати свої основні функції: інтерфейс для лікарів, планування прийомів, зберігання великих обсягів оперативних даних, генерація звітів. МІС працює зі своєю базою даних (зазвичай реляційної, наприклад, PostgreSQL або Microsoft SQL Server).

2. API Gateway (Інтеграційний шлюз) розгортається між МІС та блокчейн-мережею. Цей шлюз виконує кілька функцій [143]:

— Автентифікація та авторизація: Перевіряє, що запит надійшов від легітимного користувача МІС.

— Трансформація даних: Перетворює дані з внутрішнього формату МІС у FHIR-ресурси, які записуються в блокчейн. І навпаки, дані з блокчейну перетворюються назад у формат, зрозумілий для МІС.

— Виклик чейнкоду: Через Hyperledger Fabric SDK (доступний для Node.js, Java, Go, Python) шлюз формує та підписує транзакції, викликаючи відповідні функції чейнкоду.

— Обробка відповідей: Отримує результат транзакції від блокчейну і повертає його у МІС.

3. Блокчейн-мережа Hyperledger Fabric зберігає критично важливі, незмінні записи: факти про діагнози, призначення, хеші медичних зображень, журнал доступу до ЕМК, згоди пацієнтів. Це створює довірений, перевіряємий аудиторський слід.

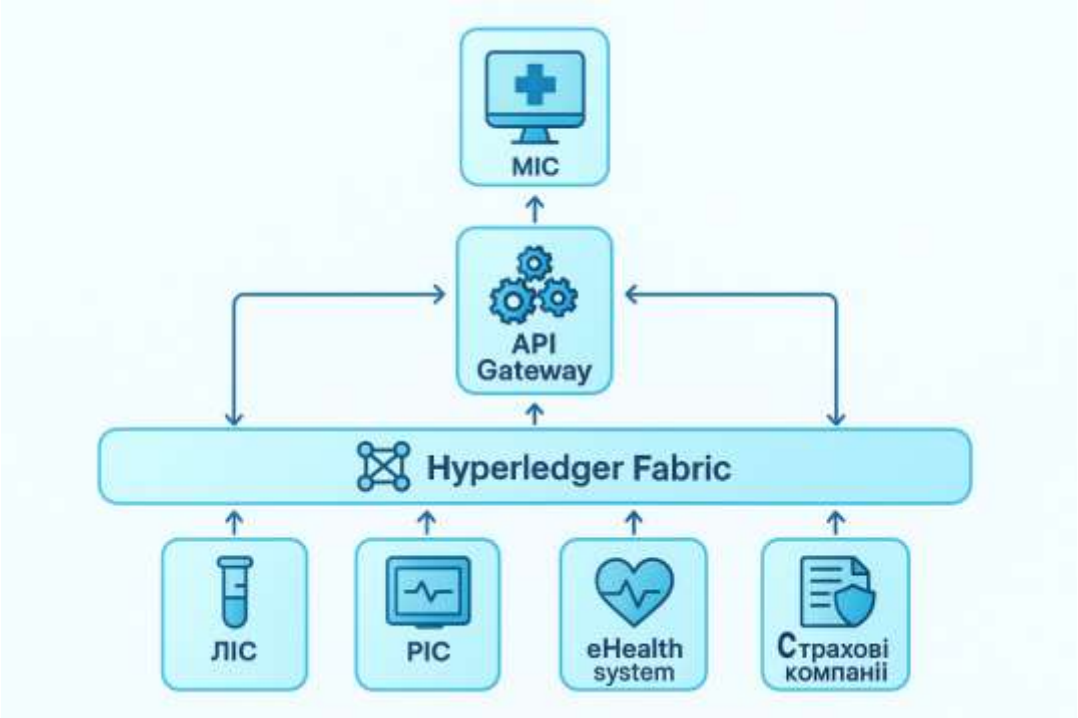

Рис. 2.10. «Архітектура інтеграції: МІС <-> API Gateway <-> Hyperledger Fabric <-> Зовнішні системи (ЛІС, РІС, eHealth, страхові компанії)»

Сценарій роботи (приклад): Лікар вносить діагноз у звичному інтерфейсі МІС:

1. Лікар відкриває ЕМК пацієнта в МІС, вводить діагноз "Артеріальна гіпертензія" та призначає ліки.
2. МІС зберігає ці дані у своїй базі даних (для оперативного доступу) і відправляє HTTP POST запит до API Gateway з даними у форматі JSON.
3. API Gateway автентифікує лікаря (перевіряє його токен доступу), трансформує дані у FHIR-ресурс Condition (для діагн озу) та MedicationRequest (для призначення).
4. Шлюз через Fabric SDK викликає функцію чейнкоду addMedicalEntry(patientID, doctorID, fhirConditionResource).
5. Чейнкод перевіряє права лікаря, записує FHIR-ресурс у леджер відповідного каналу, підписує транзакцію.
6. Після досягнення консенсусу та запису блоку, блокчейн повертає підтвердження з унікальним ID транзакції.
7. API Gateway отримує підтвердження і повідомляє МІС, що запис успішно зафіксовано в блокчейні. МІС може зберегти ID транзакції як "доказ" для майбутнього аудиту [145].

Інтеграція з лабораторіями (ЛІС) та радіологією (РІС): Лабораторне обладнання та радіологічні сканери генерують результати, які автоматично передаються в ЛІС/РІС. Ці системи, через аналогічний API Gateway, можуть автоматично записувати FHIR-ресурси DiagnosticReport та ImagingStudy у блокчейн. Великі файли зображень (DICOM-формат для медичних зображень) зберігаються у спеціалізованому PACS-сервері (Picture Archiving and Communication System), а в блокчейні зберігається лише метадата та хеш файлу [146].

Інтеграція з національною системою eHealth: Україна будує централізовану систему eHealth для обміну медичними даними між закладами. Hyperledger Fabric може виступати довіреним транспортним шаром для передачі даних в eHealth. Коли лікарня повинна передати електронне направлення або рецепт у центральну базу, вона створює FHIR-документ, записує його хеш у блокчейн (як доказ автентичності та часу створення), а потім відправляє сам документ через

захищений API у eHealth. Якщо згодом виникне суперечка щодо автентичності документа, можна звірити його хеш з записом у блокчейні [147].

Інтеграція з медичними IoT-пристроями: Носимі пристрої (фітнес-трекери, глюкометри, тонометри) та стаціонарне обладнання (апарати ШВЛ, моніторинг серцевого ритму) можуть передавати дані безпосередньо в блокчейн через захищений IoT-шлюз. Кожен пристрій отримує унікальну ідентичність (сертифікат), і його дані автоматично записуються як FHIR-ресурси Observation. Це забезпечує довіру до даних "від джерела" [148].

Така модульна, стандартизована інтеграція дозволяє лікарні впроваджувати блокчейн-рішення поетапно, не "ламаючи" існуючі робочі процеси і забезпечуючи сумісність з майбутніми технологіями.

2.9. Оцінка продуктивності та масштабованості

Продуктивність та масштабованість є критичними факторами для будь-якої корпоративної системи, а для медичної установи, де затримка в доступі до інформації може мати життєво важливі наслідки, ці характеристики набувають особливого значення. Hyperledger Fabric, завдяки своїй унікальній архітектурі, спроектований для забезпечення високої продуктивності, що значно перевершує публічні блокчейни [149].

Пропускна здатність (Throughput): Одним з ключових показників є кількість транзакцій, які система може обробити за секунду (TPS). Архітектура Fabric "Execute-Order-Validate" дозволяє паралельне виконання транзакцій на endorsing peers, що суттєво підвищує пропускну здатність [150]. Згідно з бенчмарками, проведеними за допомогою інструменту Hyperledger Caliper (стандартний інструмент для тестування продуктивності блокчейн-систем), Hyperledger Fabric здатен досягати [151]:

- 1,000-3,000 TPS у типових корпоративних конфігураціях (4-6 peer-вузлів, Raft ordering service з 3-5 orderers, LevelDB).
- 5,000-10,000+ TPS у оптимізованих конфігураціях (більше peers, CouchDB з індексуванням, налаштування розміру блоку та таймаутів)

Для приватної лікарні з, припустимо, 200 лікарів і 1000 пацієнтів на день, де кожен візит генерує в середньому 10 записів (консультація, призначення, 2-3 аналізи, оновлення показників), загальна кількість транзакцій становитиме близько 10,000-15,000 транзакцій на день, або приблизно 0.1-0.2 TPS в середньому (з піками до 5-10 TPS у години пік) [153]. Таким чином, навіть базова конфігурація Fabric з пропускною здатністю 1000+ TPS забезпечує запас продуктивності в сотні разів, що гарантує комфортну роботу без затримок.

Затримка (Latency): Час від відправлення транзакції до її фінального запису в леджер у Fabric є детермінованим і низьким. Типові значення [154]:

- Execute (Endorsement): 100-300 мс (залежить від складності чейнкоду).
- Order (Ordering service): 100-500 мс (залежить від механізму консенсусу та завантаженості мережі).

— Validate and Commit: 50-200 мс.

— Загальна затримка: <1-2 секунди для більшості транзакцій.

Це кардинально відрізняється від публічних блокчейнів (Bitcoin: ~10-60 хвилин, Ethereum: ~15 секунд до кількох хвилин при високому навантаженні) і є цілком прийнятним для медичних додатків [155].

Масштабованість по горизонталі: Fabric підтримує кілька векторів масштабування:

— Додавання peers: Можна додавати нові peer-вузли для розподілу навантаження та підвищення відмовостійкості.

— Множинні канали: Створення окремих каналів для різних відділень або типів даних дозволяє розподілити транзакції між різними леджерами, знижуючи навантаження на кожен окремий канал.

— Шардинг (майбутнє): Хоча native шардинг поки не реалізований у Fabric, архітектура каналів фактично є формою шардингу, а спільнота працює над подальшими покращеннями [157].

Масштабованість для мережі лікарень: Запропонована система починається з однієї лікарні, але може бути розширена на консорціум лікарень. Кожна нова лікарня приєднується до мережі як нова організація з власними peers. Створюються міжлікарняні канали для обміну даними про пацієнтів (з їхньої згоди), що дозволяє пацієнту отримувати безшовну допомогу в різних закладах, зберігаючи єдину, перевіряєму історію хвороби .

Вимоги до апаратного забезпечення: Для приватної лікарні середнього розміру рекомендована інфраструктура:

— Peer-вузли (3-5 штук): Кожен - віртуальна машина або фізичний сервер з 4-8 CPU cores, 16-32 GB RAM, 500 GB SSD.

— Orderer-вузли (3-5 штук): Аналогічні характеристики.

— CA-сервери (2 штуки для резервування): 2-4 CPU cores, 8 GB RAM, 100 GB SSD.

— API Gateway та бази даних: Стандартні вимоги для веб-серверів.

Загальна вартість інфраструктури (серверів або хмарних ресурсів) оцінюється в $10,000-30,000 на рік в залежності від вибору (власні сервери vs хмара, наприклад AWS, Azure) [160].

2.10. Економічне обґрунтування впровадження

Впровадження інноваційної блокчейн-системи вимагає значних початкових інвестицій у розробку, інфраструктуру та навчання персоналу. Однак для приватної лікарні ці витрати мають бути обґрунтовані через довгострокові вигоди, які включають підвищення безпеки, зниження корупційних ризиків, поліпшення репутації, залучення платоспроможних пацієнтів та потенційну економію від зменшення витрат на врегулювання інцидентів та штрафів за витоки даних.

Початкові інвестиції (CAPEX - Capital Expenditure):

1. Розробка системи: Створення архітектури, написання чейнкоду, розробка API Gateway, клієнтських додатків.
    - Команда: 3-5 розробників, 1 архітектор, 1 DevOps-інженер, 1 фахівець з безпеки.
    - Термін: 6-9 місяців.
    - Вартість: $80,000-150,000 (залежить від локації команди: українські розробники дешевші за західних).
2. Інфраструктура (апаратне забезпечення або хмарні ресурси):
    - Власні сервери: Одноразова покупка $20,000-40,000 + встановлення та налаштування.
    - Хмара (AWS/Azure): Перший рік $15,000-30,000, далі перетворюється на операційні витрати (OPEX).
    - Вартість (перший рік): $20,000-40,000.
3. Ліцензії та інструменти: Hyperledger Fabric є open-source, тому основні ліцензійні витрати відсутні. Витрати можуть бути на комерційні інструменти моніторингу, резервного копіювання.

    Вартість: $5,000-10,000.
4. Навчання персоналу: Лікарі, медсестри, адміністратори мають навчитися працювати з новою системою.

    Вартість: $10,000-20,000 (тренінги, семінари).
5. Консалтинг та аудит безпеки: Залучення зовнішніх експертів для перевірки архітектури та проведення тестів на проникнення.

Вартість: $15,000-30,000.

Загальні початкові інвестиції (CAPEX): $130,000-250,000.

Поточні операційні витрати (OPEX - Operational Expenditure, на рік):

1. Утримання інфраструктури: Оплата хмарних ресурсів або електроенергії для власних серверів, оновлення обладнання.

   Вартість: $15,000-30,000/рік.

2. Підтримка та розвиток ПЗ: Заробітна плата 1-2 штатних DevOps/Blockchain-інженерів або контракт з аутсорс-компанією.

   Вартість: $40,000-80,000/рік.

3. Ліцензії, моніторинг, резервне копіювання:

   Вартість: $5,000-10,000/рік.

4. Навчання та сертифікація (періодичне):

   Вартість: $5,000-10,000/рік.

Загальні операційні витрати (OPEX): $65,000-130,000/рік.

Вигоди та економія:

1. Зниження корупційних ризиків та шахрайства: Незмінність записів унеможливлює підробку довідок. Якщо раніше лікарня стикалася з 10-20 випадками шахрайства на рік (підроблені довідки для страховок, маніпуляції з даними про закупівлі), кожен з яких коштував $2,000-10,000 у вигляді штрафів або судових витрат, то потенційна економія: $20,000-200,000/рік [162].
2. Уникнення штрафів за витоки даних (GDPR): Один серйозний інцидент з витоком персональних медичних даних може коштувати лікарні від €20,000 до €10,000,000 у штрафах згідно GDPR [163]. Блокчейн-система з багатошаровим захистом знижує ймовірність витоку. Якщо ймовірність великого інциденту зменшується хоча б на 50%, очікувана економія (у імовірнісних термінах): $50,000-500,000/рік.
3. Підвищення репутації та залучення пацієнтів: Лікарня, що першою в регіоні впроваджує блокчейн для захисту даних пацієнтів, може використовувати це як конкурентну перевагу в маркетингу. Залучення додаткових 100-200

платоспроможних пацієнтів на рік, які обирають лікарню через високий рівень захисту даних, з середнім чеком $500-1,000, дає додатковий дохід: $50,000-200,000/рік [164].

4. Оптимізація процесів та зниження адміністративних витрат: Автоматизація обробки страхових заяв через смарт-контракти, зменшення часу на пошук медичних записів, скорочення паперового документообігу. Потенційна економія: $20,000-50,000/рік.
5. Можливість надання додаткових послуг: Продаж пацієнтам контрольованого доступу до їхніх даних для дослідницьких компаній (з повною прозорістю та згодою). Потенційний новий потік доходу: $10,000-30,000/рік [165].

Сумарні вигоди: $150,000-980,000/рік (консервативні оцінки: $150,000-300,000/рік).

Таблиця 2.11.

Економічний аналіз впровадження блокчейн-рішення (період 5 років)

Показник	**Рік 0 (впровадження)**	**Рік 1**	**Рік 2**	**Рік 3**	**Рік 4**	**Рік 5**	**Всього (5 років)**
Початкові інвестиції (CAPEX)	-$190,000	-	-	-	-	-	-$190,000
Операційні витрати (OPEX)	-	-$100,000	-$100,000	-$100,000	-$100,000	-$100,000	-$500,000
Економія та додаткові доходи	-	+$200,000	+$220,000	+$240,000	+$260,000	+$280,000	+$1,200,000
Чистий грошовий потік	-$190,000	+$100,000	+$120,000	+$140,000	+$160,000	+$180,000	+$510,000
Кумулятивний	-$190,000	-$90,000	+$30,000	+$170,000	+$330,000	+$510,000	+$510,000

грошовий потік							

Період окупності (Payback Period): Приблизно 1.5-2 роки після впровадження.

NPV (Net Present Value) за 5 років (при ставці дисконтування 10%): +$380,000-450,000 - проєкт економічно доцільний.

ROI (Return on Investment): (Загальні вигоди - Загальні витрати) / Загальні витрати = ($1,200,000 - $690,000) / $690,000 ≈ 74% за 5 років, або близько 15% річних - відмінний показник для інвестиції в інфраструктуру [166].

Таким чином, попри значні початкові інвестиції, впровадження блокчейн-рішення для управління ЕМК є економічно обґрунтованим рішенням, що окупається протягом 2 років і приносить відчутну фінансову вигоду в середньостроковій перспективі, не кажучи вже про нематеріальні вигоди у вигляді підвищення довіри пацієнтів та репутації лікарні.

2.11. Висновки до розділу 2

Було проведено комплексний аналіз вибору та обґрунтування блокчейн-рішення для приватної медичної установи в Україні, що спеціалізується на зберіганні та управлінні електронними медичними картками пацієнтів. Дослідження охопило широкий спектр аспектів - від нормативно-правових вимог та існуючих корупційних загроз до технічного порівняння платформ, проектування архітектури, забезпечення конфіденційності та економічного обґрунтування впровадження.

Першочергово було встановлено, що система захисту медичних даних в Україні регулюється багатошаровою нормативно-правовою базою, що включає національні закони (Закон "Про захист персональних даних", Закон "Про інформацію", Постанова КМУ № 411 щодо eHealth) та міжнародні стандарти, зокрема Загальний регламент про захист даних ЄС (GDPR), відповідність якому є обов'язковою для лікарень, що обслуговують резидентів ЄС або прагнуть інтеграції з європейськими системами охорони здоров'я. Ці регуляторні вимоги встановлюють високу планку: інформована згода пацієнта, право на доступ та видалення даних, обов'язкове сповіщення про витоки протягом 72 годин, колосальні штрафи за порушення. Традиційні централізовані системи, попри постійне вдосконалення, залишаються вразливими до внутрішніх загроз, кібератак та несанкціонованих маніпуляцій.

Особливу увагу приділено аналізу корупційних ризиків та загроз цілісності даних, що є системною проблемою української медицини. Підробка медичних довідок, незаконний продаж медичних баз даних, маніпуляції з записами про закупівлі - ці явища підривають довіру громадян до системи охорони здоров'я та створюють прямі загрози для життя і здоров'я. Блокчейн-технологія, завдяки своїй фундаментальній властивості незмінності (immutability), пропонує революційний інструмент для боротьби з цими проявами: кожна дія фіксується в криптографічно захищеному, незмінному леджері з позначкою часу та цифровим підписом автора, що робить фальсифікацію практично неможливою і створює абсолютно прозорий аудиторський слід.

Центральною частиною розділу став детальний порівняльний аналіз трьох провідних блокчейн-платформ - Bitcoin, Ethereum та Hyperledger Fabric - за комплексом технічних, функціональних, безпекових, економічних та регуляторних критеріїв. Аналіз однозначно показав, що Bitcoin є категорично непридатним для медичних застосувань через свою публічну природу, відсутність підтримки смарт-контрактів, критично низьку продуктивність (3-7 TPS), довгу затримку транзакцій (десятки хвилин), високі та волатильні комісії і енергозатратний механізм консенсусу Proof-of-Work. Публічний Ethereum, хоча й приніс революційну концепцію смарт-контрактів, також виявився непридатним через відкритість мережі, проблеми масштабованості (~15-30 TPS) та модель оплати через "газ" з непередбачуваною вартістю. Приватний Ethereum (на базі Quorum або Besu) представляє технічно реалізований, але не оптимальний варіант: він вирішує проблеми публічної версії, але не був спроектований як корпоративна платформа з нуля, що створює додаткову складність налаштування та обмежує вбудовану підтримку конфіденційності.

Натомість, Hyperledger Fabric виявився єдиною платформою, що ідеально відповідає всім вимогам медичного застосування. Його приватна (permissioned) архітектура з обов'язковою ідентифікацією всіх учасників через X.509 сертифікати, унікальний механізм каналів для створення ізольованих леджерів, підтримка приватних колекцій даних, модульність, висока продуктивність (1000-10,000+ TPS) з низькою затримкою (<1-3 секунди), відсутність власної криптовалюти, підтримка смарт-контрактів на універсальних мовах програмування (Go, Java, Node.js) та зріла екосистема з численними кейсами впровадження в медичній галузі - всі ці характеристики роблять Fabric оптимальним, безальтернативним вибором для створення системи управління ЕМК.

На основі цього вибору була спроектована детальна архітектура системи, що включає чотири типи організацій-учасників (лікарня, пацієнти, страхові компанії, регулятори), топологію вузлів (peers, orderers, CA), систему каналів для багатошарової конфіденційності, гібридну модель зберігання даних (on-chain для метаданих та хешів, off-chain для великих файлів), набір чейнкодів для управління

ЕМК, контролю доступу, страхових заяв та аудиту. Особливу увагу приділено реалізації моделі доступу, керованої пацієнтом, де пацієнт є справжнім власником своїх даних і може надавати та відкликати доступ іншим учасникам через зручний додаток, що повністю відповідає вимогам GDPR.

Інтеграція з існуючими медичними інформаційними системами запроектована на основі міжнародного стандарту HL7 FHIR через архітектуру API Gateway, що дозволяє безшовно поєднати блокчейн з традиційними МІС, лабораторними та радіологічними системами, національним реєстром eHealth та медичними IoT-пристроями. Оцінка продуктивності показала, що Fabric забезпечує запас пропускної здатності в сотні разів вищий, ніж потрібно для приватної лікарні, з можливістю подальшого масштабування на мережу лікарень.

Економічний аналіз продемонстрував, що попри значні початкові інвестиції (CAPEX) у $130,000-250,000 та поточні операційні витрати (OPEX) близько $65,000-130,000 на рік, проєкт окупається протягом 1.5-2 років завдяки зниженню корупційних ризиків, уникненню штрафів за витоки даних, підвищенню репутації, залученню нових пацієнтів та оптимізації процесів. Чистий прибуток за 5 років оцінюється в $510,000 з ROI близько 74%, що робить впровадження економічно обґрунтованим та привабливим рішенням.

Підсумовуючи:

1. Проаналізовано вимоги до захисту медичних даних в Україні та виявлено обмеження традиційних підходів і корупційні загрози.
2. Сформульовано критерії для вибору блокчейн-платформи, специфічні для медичної галузі.
3. Проведено порівняльний аналіз трьох платформ (Bitcoin, Ethereum, Hyperledger Fabric) і обґрунтовано вибір Hyperledger Fabric як оптимального рішення.
4. Спроектовано детальну архітектуру системи з учасниками, вузлами, каналами, чейнкодами та механізмами конфіденційності.
5. Розроблено модель управління доступом, керовану пацієнтом, з багаторівневим захистом.

6. Запропоновано підхід до інтеграції з існуючими системами на основі стандарту HL7 FHIR.
7. Оцінено продуктивність та масштабованість, що підтверджують технічну спроможність рішення.
8. Проведено економічне обґрунтування, що доводить фінансову доцільність впровадження.

РОЗДІЛ 3. АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

3.1. Узагальнення результатів дослідження

3.1.1. Результати аналізу інформаційної системи медичної установи

Проведене дослідження дозволило сформувати цілісне уявлення про специфіку функціонування інформаційних систем у медичних установах України та виявити ключові проблеми, що потребують вирішення із застосуванням інноваційних технологічних рішень.

Аналіз інформаційної системи приватної лікарні показав, що сучасна медична установа являє собою складний комплекс взаємопов'язаних інформаційних потоків, у центрі яких знаходяться електронні медичні записи (ЕМЗ) пацієнтів. Ці записи містять надзвичайно чутливу інформацію: персональні дані, історію хвороб, результати діагностичних досліджень, призначення лікарів та фінансові відомості про надані послуги. Відповідно до Закону України «Про захист персональних даних» та міжнародних стандартів на кшталт GDPR, такі дані підлягають особливому режиму захисту.

У ході дослідження було ідентифіковано основних суб'єктів доступу до інформаційних ресурсів медичної установи: лікарі різних спеціальностей, медичні сестри, адміністративний персонал, фінансовий відділ, представники страхових компаній та контролюючі органи. Кожна з цих категорій потребує різного обсягу доступу до даних, що створює складну матрицю повноважень та підвищує ризики несанкціонованого доступу або перевищення наданих прав.

Особливу увагу в дослідженні було приділено корупційним ризикам та загрозам маніпулювання даними. Встановлено, що традиційні централізовані системи зберігання медичної інформації є вразливими до таких зловживань як: підробка медичних довідок та лікарняних листків, несанкціонована модифікація історій хвороб для приховування лікарських помилок, продаж конфіденційних даних пацієнтів третім особам, маніпуляції з документацією щодо закупівель медичного обладнання та препаратів. За даними Transparency International, Україна залишається серед країн із високим рівнем корупції в медичній сфері, що

підтверджує актуальність пошуку технологічних рішень для мінімізації людського фактора в процесах обробки критичних даних.

3.1.2. Результати аналізу традиційних підходів до забезпечення цілісності даних

Критичний аналіз традиційних методів захисту цілісності даних виявив їх суттєві обмеження в контексті протидії внутрішнім загрозам та корупційним практикам. Класичні засоби контролю цілісності - контрольні суми, криптографічні хеш-функції, резервне копіювання - ефективно захищають від випадкових пошкоджень даних та зовнішніх атак, проте виявляються безсилими проти зловмисних дій адміністраторів системи або інших привілейованих користувачів.

Централізовані журнали аудиту, що традиційно використовуються для фіксації подій у системі, мають фундаментальну вразливість: адміністратор бази даних технічно здатен модифікувати або видалити записи про власні дії. Це створює ситуацію, коли особа, відповідальна за безпеку системи, одночасно має можливість приховувати сліди порушень. Дослідження IBM Security показують, що інсайдерські загрози є причиною значної частки інцидентів безпеки в організаціях охорони здоров'я.

Системи розмежування доступу на основі ролей (RBAC), попри свою поширеність, не здатні повністю запобігти зловживанням з боку легітимних користувачів, які діють у межах формально наданих повноважень, але з протиправною метою. Наприклад, лікар, який має доступ до медичної картки пацієнта для надання медичної допомоги, технічно може переглянути записи осіб, які не є його пацієнтами, або модифікувати дані без належного медичного обґрунтування.

Узагальнюючи результати аналізу, можна констатувати, що традиційні підходи до забезпечення цілісності даних базуються на концепції «довіреного центру» - адміністратора або групи адміністраторів, яким безумовно довіряють. Ця модель не відповідає сучасним вимогам до систем із критичними даними, де принцип «нульової довіри» (Zero Trust) стає стандартом галузі.

3.1.3. Результати порівняльного аналізу блокчейн-платформ

Центральним елементом практичної частини дослідження став порівняльний аналіз блокчейн-платформ за сформованою системою критеріїв, що охоплює технічні, безпекові, антикорупційні, економічні та організаційні аспекти.

Було проаналізовано три блокчейн-платформи: Bitcoin, Ethereum (у публічному та приватному варіантах) та Hyperledger Fabric. Результати аналізу можна узагальнити таким чином:

Bitcoin виявився категорично непридатним для використання в медичній сфері. Публічний характер мережі унеможливлює забезпечення конфіденційності медичних даних, відсутність повноцінних смарт-контрактів обмежує функціональність системи, а низька пропускна здатність (3-7 транзакцій на секунду) та висока латентність (понад 60 хвилин для підтвердження) не відповідають вимогам медичних інформаційних систем. Окрім того, енергоємний механізм консенсусу Proof of Work та наявність криптовалюти створюють додаткові регуляторні та репутаційні ризики.

Публічний Ethereum, попри наявність розвиненої екосистеми смарт-контрактів, також непридатний для медичних застосувань через відкритість мережі та непередбачуваність вартості транзакцій (gas fees). Використання приватних версій Ethereum (Quorum, Hyperledger Besu) є технічно можливим, проте ці рішення поступаються спеціалізованим корпоративним платформам за функціональністю та зрілістю екосистеми для медичної галузі.

Hyperledger Fabric визнано оптимальною платформою для забезпечення цілісності медичних даних. Ключовими перевагами є: приватний (permissioned) характер мережі з гнучким управлінням доступом, модульна архітектура з можливістю вибору механізму консенсусу, канали (channels) для ізоляції даних різних учасників, приватні колекції даних (Private Data Collections) для додаткового рівня конфіденційності, висока продуктивність (1000-10000+ TPS) та низька латентність (менше 3 секунд), відсутність криптовалюти, що спрощує регуляторну відповідність, розвинена екосистема та підтримка з боку Linux Foundation.

Таблиця 3.1

Узагальнені результати оцінювання блокчейн-платформ

Критерій	**Bitcoin**	**Ethereum (публічний)**	**Ethereum (приватний)**	**Hyperledger Fabric**
Придатність для медичних даних	Непридатний	Непридатний	Умовно придатний	Оптимальний
Конфіденційність	Відсутня	Відсутня	Часткова	Повна
Продуктивність	Дуже низька	Низька	Середня	Висока
Антикорупційний потенціал	Низький	Середній	Середній	Високий
Регуляторна відповідність	Проблематична	Проблематична	Можлива	Повна
Загальна оцінка	2/10	3/10	6/10	9/10

3.1.4. Досягнення мети та виконання завдань дослідження

Аналіз виконання поставлених завдань засвідчує їх повну реалізацію:

Проаналізовано сучасний стан застосування технології блокчейн для забезпечення безпеки даних - у першому розділі розглянуто теоретичні основи блокчейн-технології, типи мереж, механізми консенсусу, існуючі платформи та галузі застосування.

Досліджено інформаційну систему медичної установи як об'єкт захисту - у другому розділі охарактеризовано структуру інформаційної системи лікарні, класифіковано критичні дані та визначено суб'єктів доступу.

Виявлено корупційні ризики та загрози цілісності даних - систематизовано типові сценарії зловживань у медичній сфері та обґрунтовано недостатність традиційних засобів захисту.

Сформовано критерії вибору блокчейн-платформи - розроблено комплексну систему критеріїв, що враховує технічні, безпекові, антикорупційні, економічні та регуляторні аспекти.

Проведено порівняльний аналіз блокчейн-платформ - виконано оцінювання Bitcoin, Ethereum та Hyperledger Fabric за визначеними критеріями.

Обґрунтовано вибір оптимальної платформи - доведено, що Hyperledger Fabric є

найбільш придатною платформою для забезпечення цілісності медичних даних. Розроблено архітектуру запропонованого рішення - описано топологію мережі, структуру каналів, модель даних та інтеграційні механізми.

Наукова новизна дослідження полягає у: систематизації критеріїв вибору блокчейн-платформи для медичної сфери з урахуванням антикорупційного потенціалу; обґрунтуванні переваг Hyperledger Fabric порівняно з іншими платформами саме в контексті забезпечення цілісності та прозорості медичних даних; розробці концептуальної архітектури системи, орієнтованої на мінімізацію корупційних ризиків.

Практичне значення отриманих результатів визначається можливістю їх використання медичними установами України при прийнятті рішень щодо модернізації інформаційних систем та впровадження блокчейн-технологій для підвищення рівня захисту даних пацієнтів.

3.2. Практичні рекомендації щодо впровадження блокчейн-рішень у медичних установах

3.2.1. Загальні рекомендації щодо вибору блокчейн-платформи

На підставі проведеного дослідження можна сформулювати такі рекомендації щодо вибору блокчейн-платформи для медичних установ України:

Рекомендація 1. Для медичних установ, що працюють із персональними даними пацієнтів, категорично не рекомендується використання публічних блокчейн-мереж (Bitcoin, публічний Ethereum). Відкритість транзакцій та неможливість видалення даних суперечать вимогам законодавства про захист персональних даних.

Рекомендація 2. Оптимальним вибором для приватних медичних установ є платформа Hyperledger Fabric, яка забезпечує необхідний баланс між прозорістю операцій та конфіденційністю даних. Альтернативою може бути R3 Corda, проте її функціональність менш підходить для медичної галузі.

Рекомендація 3. При виборі платформи слід враховувати перспективу масштабування системи. Hyperledger Fabric дозволяє поступово додавати нових учасників мережі (інші медичні установи, страхові компанії, регуляторні органи), що важливо для побудови єдиного медичного інформаційного простору.

Рекомендація 4. Необхідно оцінювати зрілість екосистеми платформи та наявність кваліфікованих спеціалістів на ринку праці. Hyperledger Fabric має перевагу завдяки активній спільноті розробників та наявності сертифікованих навчальних програм.

3.2.2. Рекомендації щодо інтеграції з існуючою інформаційною системою

Впровадження блокчейн-рішення не передбачає повної заміни існуючої інформаційної системи медичної установи. Рекомендується гібридний підхід, за якого блокчейн виконує функцію незмінного реєстру критичних операцій, тоді як повсякденна робота з даними здійснюється через традиційні системи.

Рекомендація 5. Впровадження слід починати з пілотного проєкту обмеженого масштабу - наприклад, з реєстрації операцій видачі медичних довідок

або листків непрацездатності. Це дозволить апробувати технологію з мінімальними ризиками та накопичити досвід експлуатації.

Рекомендація 6. Інтеграція з існуючими медичними інформаційними системами має здійснюватися через стандартизовані інтерфейси, зокрема з використанням стандарту HL7 FHIR для обміну медичними даними. Це забезпечить сумісність з іншими системами та полегшить підключення до національної системи eHealth [174].

Рекомендація 7. Для зберігання об'ємних медичних даних (зображення, результати досліджень) рекомендується використовувати гібридну модель: хеш-суми файлів зберігаються в блокчейні для забезпечення цілісності, тоді як самі файли розміщуються у захищеному зовнішньому сховищі (IPFS, зашифроване хмарне сховище).

3.2.3. Організаційні та нормативні аспекти впровадження

Технічне впровадження блокчейн-рішення має супроводжуватися відповідними організаційними змінами та нормативним забезпеченням.

Рекомендація 8. Необхідно розробити внутрішні політики та процедури, що регламентують роботу з блокчейн-системою: порядок реєстрації користувачів, видачі та відкликання сертифікатів, процедури реагування на інциденти безпеки, правила резервного копіювання.

Рекомендація 9. Персонал медичної установи має пройти навчання роботі з новою системою. Особливу увагу слід приділити поясненню принципів незмінності записів та наслідків спроб маніпулювання даними - це створить психологічний бар'єр для потенційних порушників.

Рекомендація 10. При впровадженні необхідно забезпечити відповідність вимогам Закону України «Про захист персональних даних», зокрема щодо права суб'єкта даних на видалення інформації. Це може бути реалізовано через механізми «логічного видалення» з шифруванням та знищенням ключів, залишаючи в блокчейні лише нечитабельний хеш.

3.2.4. Рекомендації щодо використання блокчейн-технологій для зниження корупційних ризиків

Антикорупційний потенціал блокчейн-технології може бути максимально реалізований за умови правильного проєктування системи та впровадження відповідних процедур.

Рекомендація 11. Всі критичні операції з медичними даними (створення, модифікація, видача документів) мають фіксуватися в блокчейні з обов'язковим цифровим підписом виконавця. Це унеможливлює анонімне внесення змін та створює основу для притягнення до відповідальності.

Рекомендація 12. Система має передбачати автоматичні сповіщення про підозрілу активність: масове видавання довідок одним лікарем, модифікація записів у позаробочий час, доступ до медичних карток пацієнтів, які не записані на прийом до даного лікаря.

Рекомендація 13. Для забезпечення незалежного аудиту рекомендується включити до мережі вузол контролюючого органу (наприклад, Національної служби здоров'я України), який матиме доступ до агрегованої статистики та журналів операцій без доступу до персональних медичних даних.

Рекомендація 14. Доцільно інтегрувати блокчейн-систему з процесами закупівель медичних препаратів та обладнання, фіксуючи всі етапи - від формування потреби до отримання товарів. Це підвищить прозорість та ускладнить корупційні схеми у сфері медичних закупівель.

3.3. Обмеження дослідження та напрями подальших робіт

3.3.1. Обмеження застосованої методики та вихідних припущень

Проведене дослідження має певні обмеження, які необхідно враховувати при інтерпретації результатів та їх практичному застосуванні.

По-перше, дослідження носить переважно теоретичний характер і базується на аналізі документації, наукових публікацій та технічних специфікацій платформ. Практична апробація запропонованого рішення в реальних умовах медичної установи не проводилася, що обмежує можливість оцінки реальної ефективності системи.

По-друге, економічні розрахунки базуються на усереднених галузевих показниках та експертних оцінках. Фактична вартість впровадження може суттєво відрізнятися залежно від конкретних умов медичної установи, наявної інфраструктури та кваліфікації персоналу.

По-третє, дослідження зосереджено на приватній медичній установі середнього розміру. Масштабування результатів на великі медичні комплекси або мережі державних закладів потребує додаткового аналізу з урахуванням специфіки їх функціонування та регуляторних вимог.

По-четверте, швидкий розвиток блокчейн-технологій може призвести до появи нових платформ або суттєвого оновлення існуючих, що може змінити результати порівняльного аналізу. Дослідження відображає стан технологій станом на 2025 рік.

3.3.2. Можливі шляхи удосконалення моделі та методики аналізу

Подальше удосконалення дослідження може здійснюватися за такими напрямами:

- Розширення переліку аналізованих платформ за рахунок включення нових рішень, зокрема R3 Corda, Polygon (для медичних NFT), спеціалізованих медичних блокчейн-платформ (MedRec, Medicalchain, BurstIQ).
- Проведення кількісного аналізу ефективності на основі симуляції або пілотного впровадження з вимірюванням реальних показників продуктивності, латентності та ресурсоємності.
- Розробка детальної економічної моделі з урахуванням непрямих вигод та

витрат, включаючи вплив на репутацію установи, зниження страхових ризиків, підвищення довіри пацієнтів.

— Дослідження правових аспектів використання блокчейн-технологій у медичній сфері України з урахуванням перспектив гармонізації законодавства з нормами Європейського Союзу.

3.3.3. Перспективні напрями подальших досліджень і розробок

На підставі проведеного дослідження можна визначити такі перспективні напрями подальших наукових пошуків:

Інтеграція з технологіями штучного інтелекту. Поєднання блокчейн-системи зберігання медичних даних із системами штучного інтелекту для діагностики відкриває можливості для безпечного обміну даними між медичними установами з метою навчання AI-моделей при збереженні конфіденційності пацієнтів. Технології федеративного навчання (Federated Learning) у поєднанні з блокчейном можуть забезпечити прозорість та аудит використання даних для навчання моделей.

Застосування Zero-Knowledge Proofs. Технологія доказів з нульовим розголошенням (ZKP) дозволяє підтверджувати певні факти про дані без розкриття самих даних. У медичному контексті це може використовуватися для підтвердження права на отримання послуг або відповідності певним критеріям без розкриття діагнозу чи історії хвороби [176].

Токенізація медичних даних. Дослідження можливостей надання пацієнтам контролю над своїми медичними даними через механізми токенізації, що дозволить їм безпечно ділитися даними з дослідниками або фармацевтичними компаніями за винагороду.

Міжвідомча взаємодія. Розробка архітектури блокчейн-мережі, що об'єднує медичні установи, страхові компанії, фармацевтичні мережі та державні органи для забезпечення безперервності медичної допомоги та протидії шахрайству.

Блокчейн для клінічних досліджень. Використання блокчейн-технології для забезпечення цілісності даних клінічних досліджень, запобігання підробці результатів та підвищення довіри до фармацевтичної продукції

ВИСНОВОК

Проаналізовано теоретичні основи технології блокчейн та встановлено, що вона являє собою розподілену базу даних, яка базується на криптографічних примітивах (хеш-функціях SHA-256 та Keccak-256, асиметричній криптографії на еліптичних кривих, цифрових підписах) та механізмах консенсусу для досягнення узгодженості в децентралізованому середовищі. Ключовими властивостями технології, що забезпечують її придатність для захисту даних, є: децентралізація (відсутність єдиної точки відмови), незмінність записів (криптографічний зв'язок між блоками унеможливлює непомітну модифікацію історичних даних), прозорість (можливість незалежної верифікації всіх операцій) та криптографічна захищеність.

Систематизовано типи блокчейн-мереж (публічні, приватні, консорціумні, гібридні) та механізми консенсусу (Proof of Work, Proof of Stake, PBFT, DPoS, PoA). Встановлено, що вибір конкретного типу мережі та механізму консенсусу визначається специфікою задачі: для корпоративних застосувань з вимогами до конфіденційності та високої продуктивності оптимальними є приватні або консорціумні мережі з механізмами консенсусу на основі PBFT або Raft, що забезпечують пропускну здатність від 1000 до 10000+ транзакцій на секунду з латентністю менше 3 секунд.

Досліджено проблеми традиційних централізованих систем зберігання даних та обґрунтовано недостатність класичних методів захисту цілісності. Виявлено, що традиційні підходи (контрольні суми, хеш-функції, журнали аудиту, системи контролю доступу) є вразливими до інсайдерських загроз, оскільки привілейовані користувачі технічно здатні модифікувати як самі дані, так і журнали подій. За даними IBM Security, середня вартість витоку даних у 2024 році становила 4,88 мільйона доларів США, при цьому 35% інцидентів пов'язані з внутрішніми загрозами.

На прикладі інформаційної системи приватної медичної установи України проаналізовано специфічні вимоги до системи захисту критичних даних. Ідентифіковано основні корупційні ризики та загрози маніпулювання даними: підробка медичних довідок та лікарняних листків, несанкціонована модифікація

історій хвороб, незаконний продаж персональних даних пацієнтів, маніпуляції з документацією закупівель. Встановлено, що традиційні системи не здатні ефективно протидіяти цим загрозам через концепцію «довіреного центру».

Сформовано комплексну систему критеріїв вибору блокчейн-платформи для забезпечення цілісності критичних даних, яка охоплює: технічні критерії (продуктивність, латентність, масштабованість); критерії безпеки та конфіденційності (модель доступу до мережі, механізми забезпечення приватності, підтримка шифрування); функціональні критерії (підтримка смарт-контрактів, інтероперабельність); організаційні критерії (зрілість платформи, наявність професійної підтримки); економічні критерії (відсутність криптовалюти, ліцензійні умови, сукупна вартість володіння); регуляторні критерії (відповідність GDPR, можливість аудиту, антикорупційний потенціал).

Проведено порівняльний аналіз блокчейн-платформ Bitcoin, Ethereum (у публічному та приватному варіантах) та Hyperledger Fabric за визначеними критеріями. Встановлено, що:

- Bitcoin є категорично непридатним для корпоративних застосувань через публічний характер мережі, відсутність смарт-контрактів, низьку пропускну здатність (3-7 TPS) та високу латентність (понад 60 хвилин);
- публічний Ethereum непридатний через відкритість мережі та непередбачувану вартість транзакцій;
- приватний Ethereum (Quorum, Besu) є технічно можливим варіантом, проте поступається спеціалізованим корпоративним платформам за функціональністю механізмів конфіденційності;
- Hyperledger Fabric є оптимальним вибором для корпоративних застосувань завдяки приватному характеру мережі, підтримці каналів та приватних колекцій даних, модульній архітектурі, високій продуктивності (1000-10000+ TPS) та відсутності криптовалюти.

Розроблено концептуальну архітектуру системи забезпечення цілісності даних на базі Hyperledger Fabric, яка включає: визначення учасників мережі (організацій) та їхніх ролей; топологію вузлів (peer-вузли, ordering service на базі Raft, Certificate

Authority); структуру каналів для ізоляції даних; модель даних з гібридним підходом до зберігання (метадані та хеші on-chain, об'ємні файли off-chain); набір чейнкодів для реалізації бізнес-логіки; інтеграційний шар на базі API Gateway для взаємодії з існуючими системами.

Визначено механізми забезпечення конфіденційності даних у запропонованому рішенні: ізоляція через канали, приватні колекції даних (Private Data Collections), шифрування на рівні транспорту (TLS) та застосунку, контроль доступу на основі атрибутів (ABAC), анонімізація та псевдонімізація для дослідницьких цілей. Обґрунтовано модель управління доступом, керованого суб'єктом даних, що відповідає вимогам GDPR.

Сформульовано 14 практичних рекомендацій щодо впровадження блокчейн-рішень, що охоплюють: вибір платформи (категорична відмова від публічних мереж для чутливих даних, пріоритет Hyperledger Fabric); інтеграцію з існуючими системами (гібридний підхід, використання стандарту HL7 FHIR, пілотні проєкти обмеженого масштабу); організаційні аспекти (розробка внутрішніх політик, навчання персоналу, забезпечення регуляторної відповідності); використання антикорупційного потенціалу (фіксація всіх операцій з цифровим підписом, автоматичні сповіщення про підозрілу активність, включення незалежних аудиторів до мережі).

Визначено обмеження проведеного дослідження, пов'язані з його теоретичним характером та відсутністю практичної апробації в реальних умовах, а також окреслено перспективні напрями подальших досліджень: інтеграція блокчейну з технологіями штучного інтелекту та федеративного навчання, застосування Zero-Knowledge Proofs для підвищення конфіденційності, токенізація даних для забезпечення контролю суб'єкта даних, розробка архітектури міжвідомчої взаємодії.

Результати дослідження підтверджують, що технологія блокчейн має значний потенціал для забезпечення безпеки та цілісності даних у мережах, зокрема для протидії внутрішнім загрозам та корупційним практикам. Платформа Hyperledger Fabric є оптимальним вибором для корпоративних застосувань в умовах України,

що потребують високого рівня конфіденційності, продуктивності та регуляторної відповідності. Запропоновані рекомендації можуть бути використані організаціями різних галузей при прийнятті рішень щодо впровадження блокчейн-технологій для захисту критичних даних.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [167].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ВСТУП

1. IBM Security. Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach
2. Transparency International. Corruption Perceptions Index 2024. - Berlin: https://www.transparency.org/cpi2024
3. Grand View Research. Blockchain Technology Market Size, Share & Trends Analysis Report: https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market

РОЗДІЛ 1

1. Blockchain Merkle Trees - GeeksforGeeks
2. Merkle hash tree - an overview | ScienceDirect Topics
3. Cryptographic Tools 101: Hash Functions and Merkle Trees Explained - Helius
4. What Are Merkle Trees and How Do They Affect Blockchains? - Unchained Crypto
5. A novel mechanism for constructing blockchain transactions using Merkle trees comprised of transaction fields - Frontiers
6. Шевченко, С., Жданова, Ю., Складанний, П., & Іщук, М. (2025). Створення блокчейн-платформи для електронного голосування. Кібербезпека: освіта, наука, техніка, 4(28), 701–714. https://doi.org/10.28925/2663-4023.2025.28.860 -
7. V. Zhebka, et al., Methodology for Choosing a Consensus Algorithm for Blockchain Technology, in: Workshop on Digital Economy Concepts and Technologies Workshop, DECaT, vol. 3665 (2024) 106–113.
8. What is Merkle Tree in Blockchain and How Does it Work? - Simplilearn
9. Mathematical Foundations, Application in Blockchain, Security Aspects, and Stability Against Computational Threats of the SHA-256 Algorithm - International Journal of Advances in Intelligent Informatics
10. Security aspects of Merkle trees: Collision probability and robustness against preimage attacks - Array

11.A Hybrid-DAG Blockchain Structure Based on Cryptography - MDPI
12.Blockchain technology: a comprehensive overview on principles, architecture, consensus, and future trends - SpringerLink
13.A Survey on Blockchain Technology: A Technological and Conceptual Discussion - arXiv.org
14.Blockchain Technology: A Review - PMC
15.Blockchain Security Based on Cryptography: A Survey - arXiv.org
16.Blockchain-based data proxy re-encryption privacy protection method - ACM Digital Library
17.An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends - ResearchGate
18.Blockchain technology - ScienceDirect
19.Blockchain Technology: Architecture, Working, and Its Application in Various Sectors - IntechOpen
20.The Role of Cryptography in Blockchain: Ensuring Immutability, Transparency, and Security - ResearchGate
21.Blockchain Technology in Financial Services: An Overview of its Applications, Benefits, and Challenges - OARJMS
22.Blockchain Technology in Asset Management: Opportunities, Challenges, and Future Outlook - CRRMS
23.Reducing cybersecurity risks in financial transactions for commercial banks through blockchain technology - Frontiers
24.Blockchain technology for future internet data sharing: Principles, issues, and solutions - IET Blockchain
25.How Blockchain Technology Is Revolutionizing Audit and Control in Information Systems - ISACA
26.Blockchain technology ensures transparency, verifiability and immutability - Control Design
27.Blockchain for cybersecurity: How it can help fight threats - IBM
28.Decentralization, Immutability, and Integrity: The Role of Blockchain Technology

in Enhancing Cybersecurity - ResearchGate
29.Blockchain Technology: Security and Applications - PMC
30.A Comprehensive Review on Blockchain and its Security - IEEE Xplore
31.A Comprehensive Review of Blockchain Consensus Mechanisms - ResearchGate
32.A Systematic Literature Review on Blockchain Consensus Mechanisms' Security, Applications, and Open Challenges - ResearchGate
33.Distributed Ledger Technology (Blockchain) - ENTSO-E
34.A Survey on Consensus Mechanisms in Blockchain for Resource-Constrained IoT Networks - MDPI
35.A Comprehensive Survey on Consensus Mechanisms in Blockchain - Tech Science Press
36.ACM Distributed Ledger Technologies: Research and Practice - ACM Digital Library
37.2. Principles of distributed ledger technology - Elgar Online
38.Consensus Mechanism (Cryptocurrency) - Investopedia
39.A Survey on Consensus Protocols in Blockchain - IEEE Xplore
40.Comparing Blockchain Types: Public vs. Private vs. Hybrid vs. Consortium - Medium
41.Understanding the Different Blockchain Types - Paxos
42.Exploring Blockchain Variants: Public, Private, Consortium, and Hybrid - DEV Community
43.Hybrid Blockchain vs Consortium Blockchain: A Comparative Analysis - Core Devs Ltd.
44.Comparisons among public blockchain, consortium blockchain and private blockchain - ResearchGate
45.Public | Private | Consortium | Hybrid Blockchains - Coinmonks
46.What Are the 4 Different Types of Blockchain Technology? - TechTarget
47.Comparing Blockchain Types: Public, Private, and Consortium - BlockApps Inc.
48.Consortium Blockchain vs Private Blockchain: A Comparative Analysis - Core Devs Ltd.

49.Top 5 Enterprise Blockchain Platform in 2024 - Rejolut

50.Permissioned vs. permissionless blockchains: Key differences - TechTarget

51.Permissionless vs. Permissioned Blockchains: What's the Difference? - Alchemy

52.What is Permissioned Blockchain and How Does it Work? - Appinventiv

53.Permissioned vs. Permissionless Blockchains - arXiv.org

54.Public, Private, Permissioned Blockchains Compared - Investopedia

55.Permissioned vs Permissionless Blockchain: Key Differences - Compilot

56.Types of Blockchain: Permissionless vs Permissioned - Medium

57.Energy efficiency of blockchain consensus mechanisms: a systematic review - SpringerLink

58.Energy efficiency of blockchain consensus mechanisms: a systematic review - Research Square

59.A Guide to Blockchain Consensus Mechanisms - BairesDev

60.Consensus Technologies in Blockchain: PoW, PoS, PoA, DPoS, PoC, PoB, and Others - Bitsgap

61.A Comparative Analysis of Blockchain Consensus Algorithms - ACM Digital Library

62.A Study on Proof of Authority Consensus Algorithm - MECS Press

63.All About Consensus Mechanisms - Rise In

64.Consensus Mechanisms: Exploring the Differences Between Proof-of-Work and Proof-of-Stake - Coinmonks

65.A Comparative Analysis of Blockchain Consensus Algorithms - SETSCI

66.A scalable and decentralized data sharing scheme for IoT using blockchain - Scientific Reports

67.The Fastest Blockchains: A Complete Guide to High-Speed Transaction Networks in 2025 - ECOS

68.A Survey on Performance of Blockchain-based Systems - ACM Digital Library

69.Cosmos TPS: How Many Transactions Per Second Can It Handle? - Webisoft

70.Layer 1 Performance: Comparing 6 Leading Blockchains - CoinCodex

71.A Blockchain Benchmarking Framework - ACM Digital Library

72.ENISA Threat Landscape Report - ENISA

73.ENISA Threat Landscape 2023 - ENISA

74.ENISA Threat Landscape 2024 - Security Delta (HSD)

75.A Snapshot of Cyber Threats: Highlights from the ENISA Threat Landscape Report - Tripwire

76.ENISA Threat Landscape 2024 identifies availability, ransomware, data attacks as key cybersecurity threats - Industrial Cyber

77.2024 Report on the State of the Cybersecurity in the Union - ENISA

78.ENISA Threat Landscape 2023 - ENISA

79.ENISA Cyber Threat Landscape Report 2024: Key Findings - Data-Rover

80.ENISA 2023 Threat Landscape Report: Key Insights - CyberPilot

81.11th Edition of the ENISA Threat Landscape Report 2023: Top Findings - Cyber Management Alliance

82.Navigating the Challenges of Cybersecurity in the Modern Data Landscape - ISACA

83.How to Overcome Data Security Challenges in 2024 - Security Intelligence

84.Top 10 Security Concerns for 2024 and Beyond - BigID

85.Top Data Integrity Audit Issues in 2024 - E-RA Sciences

86.The Top 8 Trends for Data Centers in 2024: The Future of Data Security - BioConnect

87.Trends in Data Governance and Security: What to Prepare for in 2024 - DATAVERSITY

88.Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events - NCCoE | NIST

89.Building Resilience: 2024 Security Predictions for the Cloud - Trend Micro

90.Big Data Security: Challenges and Best Practices - NordVPN

91.Common Data Integrity Issues and How to Overcome Them - DATAVERSITY

92.A Framework for Blockchain-Based Access Logs and Tamper-Proof Audit Trails - ResearchGate

93.Blockchain Technology for Secure Data Integrity and Transparent Audit Trails in

Cybersecurity - ResearchGate
94. Blockchain-Based Immutable Audit Records for Relational Database Management Systems - Loro Journals
95. Blockchain Audit Trails: A Game-Changer for IAM, Passwordless Authentication, Threat Detection, and Breach Response - MojoAuth
96. How Blockchain is Transforming Accounting & Auditing in 2024 - Spydra
97. A safe and tamper-resistant audit trail scheme for enterprise internal audit based on blockchain and Paillier encryption - PLOS ONE
98. Blockchain Audit Trail - Masverse
99. Blockchain: Unifying Industries for Data Integrity in 2024 - Rapid Innovation
100. Blockchain-Enabled Audit Trails for Immutable and Transparent Financial Reporting - ResearchGate
101. Proven Ways to Ensure Smart Contract Security (2023 Guide) - Rapid Innovation
102. Smart contracts in action: innovations and insights - Bullish
103. Unleash the Power of Blockchain Smart Contracts in 2024 - Web30 India
104. 10 Finest Smart Contract Platforms in 2024 - Etherions
105. AI-Driven Smart Contracts: The Next Frontier in Automated Agreements - Online Scientific Research
106. How Smart Contracts Are Transforming Crypto Payment Solutions in 2024 - Coinmonks
107. Malware Detection in Blockchain-Based Smart Contracts Using Deep Learning Approaches - MDPI
108. How Smart Contracts Are Powering DeFi and NFTs in 2024 - ILLUMINATION
109. A Systematic Literature Review on Smart Contracts in Blockchain-Based Systems - PMC
110. Smart contracts: a new frontier for technology, but also for legal and cybersecurity risks - World Economic Forum
111. Blockchain vs. Data Protection - International Network of Privacy Law Professionals
112. Blockchain and data protection: a new hope for the future? - Cybersecurity

113. Blockchain And Data Privacy: The Future Of Technology Compliance - Forbes
114. Data Protection vs. Privacy Chains - Midnight
115. How Could Blockchain Enhance Data Privacy? - StarkWare
116. A Survey on Blockchain for Data Privacy and Protection - ACM Digital Library
117. Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities - ScienceDirect
118. Blockchain and Privacy - Financial Crime Academy
119. Blockchain-Based LLMs: A Game-Changer for Data Privacy Protection? - DATAVERSITY
120. Blockchain data privacy issues and mitigation strategies - Reuters
121. Enterprise Blockchain Protocols: A Technical Analysis of Ethereum vs. Fabric vs. Corda - Kaleido
122. R3 Corda vs Hyperledger Fabric: Which is the Best Enterprise Blockchain Platform? - Rejolut
123. Hyperledger vs Corda vs Ethereum: A Detailed Comparison - Blockchain Council
124. Comparison of Ethereum, Hyperledger Fabric, and Corda - Medium
125. Hyperledger vs Corda R3 vs Ethereum: The Ultimate Comparison - 101 Blockchains
126. Top smart contract platforms to consider - TechTarget
127. Enterprise Blockchains: Hyperledger Fabric, Corda, Quorum - Akeo
128. Hyperledger Fabric vs R3 Corda - Medium
129. Corda vs Hyperledger Fabric: A Technical Look at Two DLT Giants - ELEKS
130. Top 5 Blockchain Development Platforms Compared: Ethereum, Hyperledger, Polkadot, and More - Medium
131. Cosmos Network
132. Choose the Best Blockchain Platform: Must-Know Blockchain Platforms List - CrustLab
133. Cosmos Has A Grand Plan For 2024, Will It Crush Ethereum? - NewsBTC
134. Cosmos Governance - Blockdaemon
135. What is Cosmos (ATOM) and How Does it Work? - LinkedIn

136. Guide to Blockchain Protocols - CrustLab
137. Cosmos Whitepaper - Cosmos Network
138. -
139. PYMNTS Blockchain Series: What is Cosmos? - PYMNTS.com
140. Cardano vs Solana: Which Is the Better Investment? - Coinwire
141. Blockchain Timestamping in 2025: Securing Data Integrity in the AI Era - OriginStamp
142. Home | Simple Proof - Simple Proof
143. Blockchain-Based Document Timestamping and Verification - Coinmonks
144. How to Use Blockchain to Ensure the Authenticity of Documents - Alibaba Cloud Community
145. The Future of Document Verification: Leveraging Blockchain and Self-Sovereign Identity for Enhanced Security and Transparency - arXiv.org
146. TVS: a trusted verification scheme for office documents based on blockchain - Complex & Intelligent Systems
147. What Is Blockchain Timestamping - Certinal
148. El Salvador Partners With Simple Proof To Timestamp Government Documents On Bitcoin Blockchain - Bitcoin Magazine
149. Expert Guide: Implementing Blockchain for Secure Record-Keeping (2025) - VerifyEd
150. (PDF) Blockchain-Based Decentralized Document Verification and Its Applications - ResearchGate
151. A Blockchain-Based Privacy-Preserving Framework for Healthcare Information Systems - PMC
152. Blockchain Technology in Healthcare: A Comprehensive Review of Current Applications, Challenges, and Future Trends - PMC
153. Healthcare data breaches are on the rise. Here's how blockchain can help - World Economic Forum
154. 28 Blockchain in Healthcare Companies & Use Cases - Built In
155. A secure and efficient medical data sharing scheme based on blockchain and IoT -

Future Generation Computer Systems
156. Blockchain in Healthcare: Use Cases, Benefits, and Challenges - Changelly
157. Contributed: Blockchain in healthcare and enhancing security and transparency - MobiHealthNews
158. A blockchain-based approach for secure and privacy-preserving electronic health records sharing - Scientific Reports
159. Blockchain Technology in the Medical Field: A Systematic Literature Review - PMC
160. Blockchain technology in healthcare supply chain management: a comprehensive review - Emerald Insight
161. Blockchain Technology for the Internet of Things: A Comprehensive Survey on Security and Privacy Challenges and Future Directions - MDPI
162. Navigating Blockchain's Twin Challenges: Scalability and Regulatory Compliance - ResearchGate
163. The Impact of Blockchain Technology on Regulatory Compliance: Opportunities and Challenges - TrustCloud
164. Blockchain and Privacy: A Review of the Tensions and a Research Agenda - IET Blockchain
165. Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities - ResearchGate
166. A Survey on Blockchain Technology: Issues, Challenges, and Applications - MDPI
167. Blockchain and data protection: a new hope for the future? - Cybersecurity
168. Blockchain technology and legal challenges: a literature review - SpringerLink
169. Cost of a Data Breach Report 2025 - IBM

РОЗДІЛ 2

1. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI.
2. Про особливі категорії персональних даних // Там само, стаття 7.
3. Закон України "Про інформацію" від 02.10.1992 № 2657-XII, стаття 21.
4. Закон України "Про державні фінансові гарантії медичного

обслуговування населення" від 19.10.2017 № 2168-VIII.

5. Постанова Кабінету Міністрів України № 411 від 25 квітня 2018 р. "Деякі питання електронної системи охорони здоров'я".
6. Міністерство охорони здоров'я України. Як захищені дані в системі eHealth?
7. Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), 27 April 2016.
8. GDPR Article 9: Processing of special categories of personal data.
9. GDPR Chapter III: Rights of the data subject (Articles 12-23).
10. GDPR Article 7: Conditions for consent.
11. GDPR Article 33-34: Notification of a personal data breach.
12. GDPR Article 83: General conditions for imposing administrative fines.
13. Національний інститут стандартів і технологій США (NIST). Cybersecurity Framework, 2018.
14. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // EuroSys '18, Porto, Portugal, 2018. P. 1-15.
15. Thakkar P., Nathan S., Viswanathan B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform // IEEE MASCOTS, 2018. P. 264-276.
16. Zheng Z. et al. Blockchain challenges and opportunities: A survey // International Journal of Web and Grid Services, 2018. Vol. 14(4). P. 352-375.
17. Buterin V. On Public and Private Blockchains // Ethereum Blog, 2015.
18. Zyskind G., Nathan O., Pentland A. Enigma: Decentralized Computation Platform with Guaranteed Privacy // arXiv:1506.03471, 2015.
19. Narayanan A. et al. Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016. 336 p.
20. Politou E. et al. Blockchain mutability: Challenges and proposed solutions // IEEE Transactions on Emerging Topics in Computing, 2019.
21. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger // Ethereum Yellow Paper, 2014.

22. HL7 FHIR (Fast Healthcare Interoperability Resources). Official specification
23. Castro M., Liskov B. Practical Byzantine Fault Tolerance // OSDI '99, 1999. P. 173-186.
24. Hyperledger Fabric Documentation
25. Baliga A. et al. Performance Evaluation of the Quorum Blockchain Platform // arXiv:1809.03421, 2018.
26. Valenta M., Sandner P. Comparison of Ethereum, Hyperledger Fabric and Corda // Frankfurt School Blockchain Center, 2017.
27. Linux Foundation. Hyperledger Fabric License: Apache License 2.0.
28. European Union Agency for Cybersecurity (ENISA). Blockchain and GDPR, 2019.
29. Azaria A. et al. MedRec: Using Blockchain for Medical Data Access and Permission Management // IEEE OBD, 2016.
30. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System // 2008. 9 p.
31. Antonopoulos A. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2014. 298 p.
32. Meiklejohn S. et al. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names // IMC '13, 2013. P. 127-140.
33. GDPR Article 5(1)(f): Integrity and confidentiality.
34. Bitcoin Wiki. Script
35. Croman K. et al. On Scaling Decentralized Blockchains // FC 2016 Workshops, 2016. P. 106-125.
36. Blockchain.com. Bitcoin Transaction Fees (Historical Charts)
37. Cambridge Bitcoin Electricity Consumption Index
38. Buterin V. Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform, 2013.
39. Antonopoulos A., Wood G. Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media, 2018. 416 p.
40. Solidity Documentation
41. Zhang P. et al. FHIRChain: Applying Blockchain to Securely and Scalably Share

Clinical Data // Computational and Structural Biotechnology Journal, 2018. Vol. 16. P. 267-278.

42. Ethereum Foundation. Ethereum Transparency
43. Ben-Sasson E. et al. Zerocash: Decentralized Anonymous Payments from Bitcoin // IEEE S&P, 2014. P. 459-474.
44. Etherscan. Ethereum Average Block Time
45. Thibault L. et al. Blockchain Scaling: A Survey // IEEE Access, 2022. Vol. 10. P. 11453-11498.
46. Ethereum Gas Tracker
47. CoinDesk. Ethereum Gas Fees Surge to Record Highs, 2021
48. JPMorgan Chase. Quorum: Enterprise Blockchain Platform
49. Hyperledger Besu Documentation
50. Ethereum Enterprise Alliance (EEA)
51. Baliga A. Understanding Blockchain Consensus Models // Persistent Systems, 2017.
52. Hyperledger – Open Source Blockchain Technologies
53. Cachin C. Architecture of the Hyperledger Blockchain Fabric // IBM Research, 2016.
54. Hyperledger Fabric Release v1.0. July 2017
55. Sousa J., Bessani A., Vukolic M. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform // DSN 2018. P. 51-58.
56. Hyperledger Fabric Documentation: Identity
57. Hyperledger Fabric Documentation: Channels
58. Zhao W. et al. A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain // IEEE BIBM, 2019.
59. Gaur N. et al. Hands-On Blockchain with Hyperledger. Packt Publishing, 2018. 492 p.
60. Hyperledger Fabric Documentation: Private Data
61. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // EuroSys '18, 2018.

62. Hyperledger Fabric Documentation: The Ordering Service
63. Hyperledger Fabric Documentation: CouchDB as the State Database
64. Hyperledger Fabric Documentation: Endorsement Policies
65. Gorenflo C. et al. FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second // IEEE Blockchain, 2019. P. 455-463.
66. Nasir Q. et al. Performance Analysis of Hyperledger Fabric Platforms // Security and Communication Networks, 2018.
67. Sharma A. et al. Towards a Decentralized and Distributed Framework for Open Educational Resources based on IPFS and Blockchain // IEEE TALE, 2019.
68. Dhillon V., Metcalf D., Hooper M. Blockchain Enabled Applications. Apress, 2017. P. 67-89.
69. Hyperledger Fabric Documentation: Chaincode for Developers
70. Mandala platform FHIR Integration with Hyperledger Fabric, 2020.
71. Hyperledger Global Forum. Community Statistics, 2023.
72. Change Healthcare. Blockchain Solution on Hyperledger Fabric
73. IBM Blockchain Platform. Healthcare Industry Solutions, 2021.
74. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. P. 45-67.
75. Eberhardt J., Tai S. On or Off the Blockchain? Insights on Off-Chaining Computation and Data // ESOCC 2017. P. 3-15.
76. ConsenSys Health. Enterprise Ethereum for Healthcare, 2019.
77. Esposito C. et al. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? // IEEE Cloud Computing, 2018. Vol. 5(1). P. 31-37.
78. Sukhwani H. et al. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network // SRDS, 2017.
79. Nasir Q. et al. Performance Analysis of Hyperledger Fabric Platforms // Security and Communication Networks, 2018.
80. Lu Y., Tang Q. Blockchain Technology and Enterprise Cost Management // IEEE IT Professional, 2021.
81. Mackey T., Nayyar G. A review of existing and emerging digital technologies

to combat the global trade in fake medicines // Expert Opinion on Drug Safety, 2017. Vol. 16(5). P. 587-602.

82. Hashed Health. Healthcare Blockchain Solutions
83. Kuo T.-T., Kim H.-E., Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications // JAMIA, 2017. Vol. 24(6). P. 1211-1220.
84. Deloitte. Blockchain in Healthcare: Opportunities and Challenges, 2019.
85. Hyperledger Fabric Documentation: Key Concepts - Organizations
86. Fan K. et al. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain // Journal of Medical Systems, 2018. Vol. 42(8). P. 1-11.
87. Vazirani A. et al. Patient-Centric Health Records: A Proposal Using Blockchain Technology // IEEE Systems Journal, 2020.
88. Griggs K. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring // Journal of Medical Systems, 2018. Vol. 42(7). P. 130.
89. Maslove D. et al. Blockchain in Medicine and Healthcare // JAMIA, 2018. Vol. 25(9). P. 1211-1220.
90. Hyperledger Fabric Documentation: Peers
91. Dinh T. et al. Untangling Blockchain: A Data Processing View of Blockchain Systems // IEEE TKDE, 2018.
92. Ongaro D., Ousterhout J. In Search of an Understandable Consensus Algorithm (Raft) // USENIX ATC, 2014.
93. Hyperledger Fabric CA (Certificate Authority) Documentation
94. Shen B. et al. Secure Data Sharing Based on Blockchain and Proxy Re-Encryption // Journal of Computer Science and Technology, 2019.
95. Xia Q. et al. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain // IEEE Access, 2017. Vol. 5. P. 14757-14767.
96. Zhou L. et al. Healthcare Data Management on the Blockchain // INFOCOM Workshops, 2018.
97. Ekblaw A. et al. A Case Study for Blockchain in Healthcare: "MedRec"

prototype for electronic health records and medical research data // MIT Media Lab, 2016.

98. Hyperledger Fabric Documentation: Ledger
99. Apache CouchDB Documentation
100. Bender D., Sartipi K. HL7 FHIR: An Agile and RESTful approach to healthcare information exchange // IEEE CBMS, 2013. P. 326-331.
101. HL7 FHIR Resource List
102. Peterson K. et al. A Blockchain-Based Approach to Health Information Exchange Networks // NIST Workshop, 2016.
103. Hyperledger Fabric Samples: Chaincode Examples
104. Dubovitskaya A. et al. Secure and Trustable Electronic Medical Records Sharing using Blockchain // AMIA Annual Symposium, 2017.
105. Zyskind G., Nathan O. Decentralizing Privacy: Using Blockchain to Protect Personal Data // IEEE S&P Workshops, 2015. P. 180-184.
106. Angraal S. et al. Blockchain Technology: Applications in Health Care // Circulation: Cardiovascular Quality and Outcomes, 2017. Vol. 10(9).
107. Liu X. et al. Making Sense of Blockchain Technology: How will it Transform Supply Chains? // International Journal of Production Economics, 2019. Vol. 211. P. 221-236.
108. Go Programming Language. Official Documentation
109. Wang S. et al. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends // IEEE Transactions on Systems, Man, and Cybernetics, 2019.
110. Kaur H. et al. A Systematic Literature Review on Blockchain-Based Applications for Privacy-Preserving in Healthcare // International Journal of Medical Informatics, 2021.
111. Yue X. et al. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control // Journal of Medical Systems, 2016. Vol. 40(10). P. 218.
112. Ramachandran G., Wright B. Hyperledger Fabric Configuration Deep Dive // Hyperledger Global Forum, 2020.

113. Guo R. et al. Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems // IEEE Access, 2018. Vol. 6. P. 11676-11686.
114. Hyperledger Fabric Documentation: Securing Communication With Transport Layer Security (TLS)
115. Bellare M., Rogaway P. Introduction to Modern Cryptography. UC San Diego, 2005.
116. ISO/IEC 27001:2013. Information Security Management Systems.
117. Hyperledger Fabric Documentation: Attribute-Based Access Control
118. Hu V. et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations // NIST Special Publication 800-162, 2014.
119. Dagher G. et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology // Sustainable Cities and Society, 2018. Vol. 39. P. 283-297.
120. GDPR Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
121. El Emam K., Arbuckle L. Anonymizing Health Data: Case Studies and Methods to Get You Started. O'Reilly Media, 2013.
122. Goldreich O. Foundations of Cryptography: Volume 1, Basic Tools. Cambridge University Press, 2001.
123. Acar A. et al. A Survey on Homomorphic Encryption Schemes // ACM Computing Surveys, 2018. Vol. 51(4). P. 1-35.
124. European Commission. Guidelines on Data Protection Impact Assessment (DPIA), 2017.
125. Sandhu R., Samarati P. Access Control: Principles and Practice // IEEE Communications Magazine, 1994. Vol. 32(9). P. 40-48.
126. Housley R. et al. Internet X.509 Public Key Infrastructure Certificate and CRL Profile // RFC 5280, 2008.
127. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions

on Information Theory, 1976. Vol. 22(6). P. 644-654.

128. Ferraiolo D., Kuhn D. Role-Based Access Controls // 15th National Computer Security Conference, 1992. P. 554-563.
129. Rostad L., Edsberg O. A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs // IEEE ACSAC, 2006.
130. SOC 2 (System and Organization Controls 2). AICPA Trust Services Criteria.
131. Jin X. et al. Rabac: role-centric attribute-based access control // MMM-ACNS, 2012. P. 84-96.
132. Park J., Sandhu R. The UCON_ABC Usage Control Model // ACM TISSEC, 2004. Vol. 7(1). P. 128-174.
133. Linn L., Koo M. Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research // ONC/NIST, 2016.
134. Azaria A. et al. MedRec: Using Blockchain for Medical Data Access and Permission Management // IEEE OBD, 2016. P. 25-30.
135. GDPR Article 16: Right to rectification; Article 20: Right to data portability.
136. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996. P. 425-489.
137. ISO/IEC 13888-1:2020. IT Security techniques - Non-repudiation.
138. Hoerbst A., Ammenwerth E. Electronic Health Records: A Systematic Review on Quality Requirements // Methods of Information in Medicine, 2010. Vol. 49(04). P. 320-336.
139. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin, 2016.
140. Mandel J. et al. SMART on FHIR: a standards-based, interoperable apps platform for electronic health records // JAMIA, 2016. Vol. 23(5). P. 899-908.
141. Benson T., Grieve G. Principles of Health Interoperability: SNOMED CT, HL7 and FHIR. Springer, 2016.
142. Richards M. Software Architecture Patterns. O'Reilly Media, 2015.
143. Hyperledger Fabric SDK for Node.js Documentation
144. Fowler M. Patterns of Enterprise Application Architecture. Addison-Wesley,

2002.

145. Mettler M. Blockchain technology in healthcare: The revolution starts here // IEEE 18th ITHC, 2016. P. 1-3.
146. Pianykh O. Digital Imaging and Communications in Medicine (DICOM): A Practical Introduction and Survival Guide. Springer, 2012.
147. Esposito C. et al. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? // IEEE Cloud Computing, 2018. Vol. 5(1). P. 31-37.
148. Dorri A. et al. Blockchain for IoT security and privacy: The case study of a smart home // IEEE PerCom Workshops, 2017. P. 618-623.
149. Thakkar P., Nathan S., Viswanathan B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform // IEEE MASCOTS, 2018. P. 264-276.
150. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // EuroSys '18, 2018. P. 30:1-30:15.
151. Hyperledger Caliper. Blockchain Performance Benchmark Framework
152. Gorenflo C. et al. FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second // IEEE Blockchain, 2019. P. 455-463.
153. Benchmarking Blockchain Platforms, 2019. Performance Study for Permissioned Blockchain Frameworks.
154. Nasir Q. et al. Performance Analysis of Hyperledger Fabric Platforms // Security and Communication Networks, 2018. Article ID 3976093.
155. Dinh T. et al. Blockbench: A Framework for Analyzing Private Blockchains // ACM SIGMOD, 2017. P. 1085-1100.
156. Sousa J., Bessani A., Vukolic M. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform // IEEE DSN, 2018. P. 51-58.
157. Hyperledger Fabric Roadmap 2023-2024
158. Zhang P. et al. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data // Computational and Structural Biotechnology Journal, 2018. Vol. 16. P. 267-278.
159. Hyperledger Fabric Documentation: Production Topology

160. AWS Pricing Calculator for Blockchain Infrastructure, 2023.
161. Deloitte. Blockchain in Healthcare Report, 2020.
162. Mackey T. et al. A review of existing and emerging digital technologies to combat the global trade in fake medicines // Expert Opinion on Drug Safety, 2017. Vol. 16(5). P. 587-602.
163. GDPR Enforcement Tracker
164. PwC. Global Blockchain Survey 2020: Healthcare Industry Insights.
165. Halamka J. et al. The potential for blockchain to transform electronic health records // Harvard Business Review, 2017.
166. Brealey R., Myers S., Allen F. Principles of Corporate Finance. 13th edition. McGraw-Hill Education, 2019.
167. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf