УДК 004.9 **doi: 10.26906/SUNZ.2024.3.175**

О. В. Шматко[1], Д. В. Кулініч[1], Т. В. Горбач[2]

[1] Харківський національний технічний університет радіоелектроніки, Харків, Україна
[2] Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

РОЗРОБКА ТА ДОСЛІДЖЕННЯ АРХІТЕКТУРНОЇ МОДЕЛІ СИСТЕМИ ОБМІНУ ПЕРСОНАЛЬНИМИ ДАНИМИ НА ОСНОВІ БЛОКЧЕЙН

Анотація. Актуальність. Сучасне суспільство стикається з зростаючою потребою у безпечному, на-дійному та прозорому обміні персональними даними пацієнтів у сфері охорони здоров'я. Захист конфіденційності та цілісності медичної інформації є пріоритетом для забезпечення якісного та ефективного медичного догляду. Блокчейн-технології надають обіцяючий інструмент для вирішення цієї проблеми, дозволяючи створити децентралізовану та безпечну систему обміну персональними да-ними пацієнтів. **Метою даної роботи** є забезпечення високого рівня безпеки та конфіденційності медичних даних, а також підвищення ефективності процесів у сфері охорони здоров'я за рахунок розробки програмних компонентів системи обміну персональними даними пацієнтів на основі блокчейн-технологій**. Об'єктом дослідження** є система обміну персональними даними пацієнтів у сфері охорони здоров'я. **Предметом дослідження** є програмні компоненти, що базуються на блокчейн-технологіях, призначені для забезпечення безпеки, прозорості та ефективності обміну медичною інформацією. **Результати.** У даній роботі запропоновано архітектурну модель безпечної та ефективної системи обміну медичними даними, яка може бути широко впроваджена у сфері охорони здоров'я. **Висновок.** Впровадження системи безпечного обміну персональними даними на основі технології блокчейн у сфері охорони здоров'я допоможе покращити якість медичного обслуговування та забезпечити швидший доступ до важливих даних для медичного персоналу. Теоретична значимість полягає у розширенні знань щодо застосування блокчейн-технологій у галузі охорони здоров'я та питань безпеки та конфіденційності медичної інформації. Це дослідження може бути основою для подальших досліджень у цій галузі та сприяти розвитку нових методів та підходів до обміну медичними даними.

Ключові слова: блокчейн, персональні дані пацієнтів, IoTM, смарт-контракти, Ethereum, модель системи обміну медичними даними.

Вступ

Медичні дані містять багато записів даних про пацієнтів, які важливі для подальшого лікування та майбутніх досліджень. Однак для захисту конфіденційності даних їх необхідно надійно зберігати і надавати спільний доступ до них. Блокчейн широко використовується в управлінні медичними даними завдяки своїм децентралізованим функціям і захисту від несанкціонованого доступу.

Медичні дані актуальні для всіх. У них записується фізична інформація про наш організм. Це важливо для діагностики та лікування захворювань [1]. З швидким розвитком штучного інтелекту медичні дані стали великим надбанням. Це може допомогти нам створити діагностичні моделі зі штучним інтелектом та допомогти лікарям у діагностиці. Хоча запис медичної інформації еволюціонував від початкових паперових записів до електронних медичних записів (EMR), які є більш зручними для доступу та зберігання даних, необхідно приділяти більше уваги захисту конфіденційності даних [2]. Багато лікарень та установ зменшили передачу та обмін даними, щоб уникнути витоку конфіденційних даних, що призвело до утворення розрізнених даних, оскільки медичні дані розкидані по різних закладах охорони здоров'я [3].

Конфіденційність та безпека медичних даних також призводять до інших проблем. Наприклад, для безпеки пацієнтів необхідно повторно обстежувати кожного разу, коли вони потрапляють до нової лікарні. Така поведінка призводить до марної трати енергії і грошей. З метою захисту конфіденційності пацієнтів медичні дані не можуть передаватися науковим установам, що перешкоджає розвитку медицини. Це спонукало до пошуку безпечних методів зберігання і передачі даних, і блокчейн широко використовується, завдяки своїй децентралізованої природі, захищеної від несанкціонованого доступу, для обміну медичними даними [4]. Сучасне суспільство стикається з зростаючою потребою у безпечному, надійному та прозорому обміні персональними даними пацієнтів у сфері охорони здоров'я. Захист конфіденційності та цілісності медичної інформації є пріоритетом для забезпечення якісного та ефективного медичного догляду. Блокчейн-технології надають обіцяючий інструмент для вирішення цієї проблеми, дозволяючи створити децентралізовану та безпечну систему обміну персональними даними пацієнтів.

Об'єктом дослідження є система обміну персональними даними пацієнтів у сфері охорони здоров'я. Предметом дослідження є програмні компоненти, що базуються на блокчейн-технологіях, призначені для забезпечення безпеки, прозорості та ефективності обміну медичною інформацією.

Метою цієї роботи є забезпечення високого рівня безпеки та конфіденційності медичних даних, а також підвищення ефективності процесів у сфері охорони здоров'я за рахунок розробки програмних компонентів системи обміну персональними даними пацієнтів на основі блокчейн-технологій.

Основна частина

У зростаючому світі технологій речі навколо нас стають розумніші, ніж ми думаємо. Такі галузі, як охорона здоров'я, також є революціонерами завдяки новітнім технологіям. У міру розвитку технологій якість та ефективність галузі охорони здоров'я також швидко ростуть. І лікарі, і пацієнти отримують переваги від

технологічного прогресу в галузі охорони здоров'я. Тепер ми отримуємо лабораторні звіти, МРТ і комп'ютерну томографію за менший час і є більш ефективними і точними, ніж раніше. Цифрові рентгенівські знімки-революційний спосіб поглянути на переломи та пухлини в кістках, а також Цифрове зберігання медичних записів відкривають новий спосіб догляду за пацієнтами з використанням технологій глибокого навчання і штучного інтелекту. Крім того, завдяки технологічним досягненням можливий постійний віддалений моніторинг пацієнтів та збір даних від пацієнтів у режимі реального часу за допомогою датчиків IOT, а також виконання аналізу без затримок [1].

Тепер ми можемо точніше прогнозувати важкі захворювання (наприклад, рак) і призначати ліки на дуже ранній стадії. Хоча зберігання медичних даних в цифровому вигляді дає багато переваг, воно також відкриває двері для забезпечення безпеки загрози та втрата даних. Як ми знаємо, медичні дані є критично важливими даними, вони складаються з конфіденційної і чутливої інформації, що відноситься до пацієнтів.

Отже, нам потрібен надійний механізм для підтвердження цілісності, конфіденційності безпеки медичних даних. Інтеграція технології блокчейн з галуззю охорони здоров'я може вирішити проблеми, пов'язані з цілісністю та безпекою даних. Тепер ми можемо більш ефективно і безпечно обмінюватися даними про пацієнтів, пов'язаними зі здоров'ям, з лікарями і постачальниками медичних послуг.

Спочатку (у 70-х роках) система охорони здоров'я називалася healthcare 1.0. В охороні здоров'я відчувалася гостра нестача ресурсів і обмежувалася можливість взаємодії з цифровими системами. Витрати і час були збільшені через відсутність вбудованих біомедичних датчиків, коли медичні компанії протягом цього періоду перейшли на паперові рецепти та звітність. Концепція систем охорони здоров'я виникла в 1991 році до 2005 року з healthcare 2.0. На цьому етапі використовувалося цифрове відстеження, що дозволяє лікарям використовувати обладнання для візуалізації для вивчення стану здоров'я пацієнта. З впровадженням інтернет-платформи постачальники медичних послуг почали створювати онлайн-спільноти і використовувати хмарні сервери для зберігання інформації про пацієнтів, що забезпечило повсюдний доступ як для пацієнта, так і для практикуючого лікаря. Healthcare 3.0, породила концепцію користувальницької настройки медичних карт пацієнтів. Нові користувальницькі інтерфейси забезпечують індивідуальний і оптимізований досвід роботи. На додаток до цих досягнень були впроваджені системи медичної документації, які дозволяють відстежувати медичні дані пацієнтів в режимі реального часу і на універсальному рівні. Аналогічним чином, поряд із системами EHR, такими як HL7, які були інтегровані для зберігання інформації про пацієнтів, почали з'являтися автономні немережеві системи, такі як канали соціальних мереж. Це скоротило обмін медичними даними, будь то в мережі або між клініцистами, які використовують HL7. Цей методи також покращили здатність взаємодіяти та комунікувати з пацієнт. Ера охорони здоров'я 4.0 почалася в 2016 році і триває по сьогодні [3]. За цей час було застосовано ряд різних технологій, включаючи туманні обчислення, прикордонні обчислення, Хмарні обчислення, Інтернет речей, просунуту аналітику, штучний інтелект і машинне навчання, а також блокчейн, щоб перетворити його в інтелектуальну систему охорони здоров'я або Індустрія охорони здоров'я 4.0. Основна увага була приділена носимим датчикам стану здоров'я.

Innoplexus поєднує в собі штучний інтелект і блокчейн для забезпечення безперервного сканування глобальних даних науки про життя [5]. Система надає дані науково-дослідним інститутам і фармацевтичним компаніям. BlockRx - це платформа, яка успішно використовується в реальних додатках [6]. Платформа поєднує в собі технологію блокчейн і передову технологію цифрової бухгалтерської книги iSolve. Платформа об'єднує медичні дані з біомедичних та науково-дослідних інститутів. BlockRx був застосований на практиці і домігся значного розвитку.

Було опубліковано кілька статей, в яких узагальнюються моделі, засновані на блокчейне. Джин та ін. аналізують конфіденційність обміну медичними даними за допомогою типу блокчейна, використовуваного в моделі [7]. Огляд ділить блокчейни на дві категорії: без дозволів і з дозволеним доступом. Потім аналізуються переваги та недоліки залежно від типів блокчейнів. Лейлі та ін. проаналізували ряд робіт, опублікованих у період з 2016 по 2020 рік [8]. Ця стаття присвячена ситуаціям застосування в охороні здоров'я і не фокусується в першу чергу на порівнянні та узагальненні моделей. Саха та ін. узагальнили деякі підходи до охорони здоров'я, засновані на блокчейне, але вони не порівнюють ці підходи [9]. Ісраа та ін. провели аналіз моделі з унікальної точки зору, розглядаючи як переваги, так і загрози, які технологія представляє пацієнтам [10]. Хассельгрен та ін. провели статистичний аналіз опублікованих робіт. Однак у цьому огляді не було узагальнено методів [11]. Сюй та ін. в основному аналізують застосування блокчейна в медичних даних про онкологію, таких як відстежуваність ліків і обмін даними про онкологію [12].

Блокчейн-це децентралізована розподілена технологія (DDT) [16]. У блокчейні колекція записів, які закривають обмін або передачу цінностей та цифрових активів, таких як транзакції, товари та послуги, розробляється та управляється розподіленою системою обчислювальних вузлів у одноранговій мережі. Блокчейн походить від біткоіни, технології, що представляє собою розподілену базу даних з постійно зростаючими записами, що розглядаються як блок, і ці записи не можуть бути змінені [19]. Основна ідея блокчейна полягає в стабілізації цілісності, відстежуваності і підзвітності спільно використовуваних даних. Розподілена книга обмежує методи, включаючи збереження та автентифікацію, які виконуються в мережі взаємодіючих вузлів. Ці вузли впроваджують програмне забезпечення для аудиту, яке узгоджує зображення спільної книги між одноранговою мережею акціонерів, представляючи всі підзвітні дії за допомогою цифрових відбитків пальців або хеш-кодів. Книга класифікується як розповсюджена та визначається під час запису даних. У блокчейні у кожного учасника вузла є своя загальна бухгалтерська книга. Він генерує

прозорий, незмінний запис [20]. Журнали блокчейна забезпечують точність для прийняття повідомлень в IT-середовищі health, а журнали аудиту - для подальших запитів про такі дозволи і продуктивності моделей доступу. Виходячи з цієї функціональності, фреймворк працює як послідовний опис авторизації доступу до електронної медичної інформації (EHI). За останнє десятиліття дослідники впровадили кілька систем управління охороною здоров'я, заснованих на блокчейні, для забезпечення різних цілей безпеки [21, 22]. Блокчейн гарантує, що дані не були підроблені в результаті шкідливих атак, і перевіряє безліч аспектів Походження даних [23]. Ця технологія використовує криптографічні методи, а розподілене середовище мережі блокчейн забезпечує поширення всієї інформації, що забезпечує видимий, заслуговує довіри цифровий відбиток пальця і перевіряються шляху [24].

Існує два основних види блокчейна: безстроковий і дозволений блокчейн. Публічний блокчейн також називають блокчейном без прав доступу. Першим винаходом блокчейна без прав доступу є біткоіни. Блокчейн без дозволів легкодоступний і відкритий для дій з читання і запису всіма учасниками системи [25]. Це означає, що кожен може брати участь у системі з псевдонімною ідентифікацією. Користувач також може читати інформацію або транслювати її в ефір і ідентифікується як частина механізму консенсусу [26, 27]. Ethereum також застосовує блокчейн без дозволів, і будь-який бажаючий може розробляти і комбінувати смарт-контракти по мережі без будь-яких обмежень з боку розробників. Дозволений блокчейн також називають приватним блокчейном. Окрема організація використовує дозволений блокчейн [28]. На відміну від блокчейна без дозволів, блокчейн з дозволами розроблений таким чином, що учасники мережі заздалегідь визначені для дій читання/запису і назавжди ідентифікуються всередині системи. Отже, основна відмінність між блокчейном без прав доступу та блокчейном з дозволами полягає в тому, як користувач може отримати доступ до мережі. У дозволеній блокчейн-мережі впровадьте візантійську відмовостійкість (BFT) [29]. Структура Hyperledger розроблена таким чином, щоб забезпечити безпеку технології Загального реєстру і розширити можливості дозволених користувачів.

Hyperledger Fabric-це тип дозволеної блокчейн-технології, яка працює на основі блокчейн-підприємства з відкритим вихідним кодом, підтримуваного Linux Foundation [30]. Hyperledger-це постійно поширений колективний або приватний блокчейн, який намагається вдосконалити технологію блокчейн за допомогою галузевих додатків. Як правило, Hyperledger Fabric - це розподілена мережа, що формулює однорангову систему, де кожен одноранговий вузол має репліковану, узгоджену копію структури даних блокчейна, зокрема, ланцюговий Індекс транзакції, що описує виклик і виконання ланцюгових кодів. Hyperledger Fabric дає можливість розширити спектр застосування технології блокчейн за межі кріптовалютних угод, які розрізняють різні області застосування реляційних баз даних, включаючи управління медичною інформацією [31].

Linux Foundation підтримувала проекти Hyperledger Fabric, одним з таких прикладів є Hyperledger Composer. Архів бізнес-мережі (BNA) - це функціональна розробка Hyperledger Composer, яка успадкована від блокчейна Hyperledger Fabric [15].

Бізнес-мережа включає в себе учасників, і вони об'єднуються за допомогою їх ідентифікації, а також активів, які генеруються в системі; транзакції визначають обмін активами. Ці правила передбачають виконання транзакцій, званих смарт-контрактами, і в кінцевому підсумку всі транзакції зберігаються в бухгалтерській книзі. Малюнок 1 ілюструє загальну архітектуру Hyperledger Composer. Файл моделі містить три основні компоненти: учасники, активи та транзакції. Учасники є кінцевими користувачами системи і можуть мати справу з активами та взаємодіяти з іншими за допомогою транзакцій. Активи, як правило, є змінними, збереженими в мережі. Транзакції є цілями системи і викликаються для оновлення налаштувань. Файл сценарію в бізнес-мережі визначає багато функцій транзакцій у системі. Він складається з Java Script (JS) і має справу з бізнес-логікою, яка визначає, які стандарти діють для користувачів і які типи ресурсів є загальними. Список контролю доступу (ACL) описує різні діапазони доступу, якими володіють учасники в мережі. У файлі ACL фіксується мета учасників, що визначає їх ефективність при створенні, читанні, оновленні або видаленні ресурсів. Файл запиту пояснює склад та використання запитів із системи. Вони залишаються фіксованими для екстраполяції транзакцій журналу, який містить записи всіх попередніх транзакцій у мережі. Архівний запис-це список реєстру, наданий архівним записом, який включає історію транзакцій та подій, виконаних у системі. Поки транзакція обробляється, запис журналу оновлюється, зберігаючи історію всіх транзакцій всередині бізнес-мережі. Учасники з їх ідентифікаційними даними беруть участь у відправці транзакцій, а ресурси записів журналу можуть бути вилучені за допомогою запитів composer для запиту певних записів.

Блокчейн можна розділити на публічний ланцюжок, приватний ланцюжок і консорціумний ланцюжок в залежності від способу участі [15]. Публічна мережа, як випливає з назви, є повністю загальнодоступною та доступною для всіх. Оскільки дані в ланцюжку не можуть бути змінені, публічні ланцюги вважаються повністю децентралізованими. Ланцюжок консорціуму обмежений лише авторизованими учасниками для участі, а дозволи на читання та запис та дозволи на облік участі в блокчейні формулюються відповідно до правил Альянсу. Приватний ланцюжок використовується тільки в приватних організаціях, а дозволи на читання і запис в блокчейн і дозволу на участь в бухгалтерському обліку формулюються відповідно до правил приватної організації. Беруть участь вузлів небагато, і вони строго обмежені [16]. У табл. 1 порівнюються різні типи блокчейнів.

Як децентралізована однорангова система, вузли отримують транзакції в іншому порядку [17]. Отже, необхідні послідовні алгоритми для забезпечення того, щоб вузли узгоджували транзакції. Proof of work (POW) - це перший успішний децентралізований блокчейн-алгоритм консенсусу. Для вирішення візантійської проблеми було запропоновано практичний алгоритм Візантійська відмовостійкість

(PBFT) [18]. Це гарантує, що блокчейн все ще може нормально функціонувати з деякими несправними або шкідливими вузлами.

Таблиця 1 – **Порівняння різних типів блокчейнів**

Тип блокчейну	Децентралізація	Пропускна здатність	Витрати	Масштабованість
Державна мережа	Висока	Низька	Високі	Погана
Мережа консорціумів	Середня	Середня	Середні	Відмінна
Приватна мережа	Низька	Висока	Низькі	Відмінна
Гібридна мережа	-	-	Низькі	Велика

Смарт-контракти - це комп'ютерні протоколи, які поширюють, перевіряють або приводять у виконання контракти інформаційним способом [19]. Смарт-контракти не вимагають аутентифікації третьою стороною, а успішні транзакції відстежуються і незворотні. Для складання юридично дійсного контракту використовується комп'ютерна програма, і цей контракт може бути виконаний автоматично. Смарт-контракт-це код, розгорнутий на блокчейні, який гарантує безпеку транзакцій без нагляду Третіх Сторін [20]. Процес укладення смарт-контракту показаний на рис. 1.

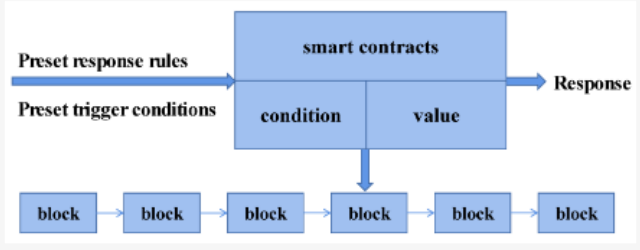

Рис. 1. Системна модель. Джерело: [20]

1. Децентралізація: виконання смарт-контрактів не повинно залежати від участі або втручання сторонніх організацій, а нагляд і арбітраж контрактів здійснюються комп'ютерами;

2. Незмінність: як тільки смарт-контракт розгорнуть, весь вміст не може бути змінено. Це чимось схоже на контракт в традиційному світі, який не може бути змінений після його підписання;

3. Низька вартість: оскільки смарт-контракти не вимагають контролю з боку стороннього посередника, як тільки відбувається порушення контракту, код вводиться в дію і має набагато меншу вартість у порівнянні з традиційними контрактами;

4. Відкритість і прозорість: після успішного розгортання смарт-контракт буде працювати відповідно до дизайн-кодом і може бути переглянутий будь-яким Користувачем з високим ступенем прозорості [21].

Існує багато ситуацій, в яких блокчейн використовується для обміну медичними даними, і зараз існує три типи в залежності від сценаріїв застосування. Перший-це безпечне зберігання даних і доступ до них на основі блокчейна. Другий-використання блокчейна в поєднанні з IOMT. Третє-використання блокчейна для заміни центрального федерального навчального закладу.

Поява EMR принесла зручність, а також проблеми конфіденційності. Через проблеми безпеки медичні дані не можуть передаватися вільно. Було запропоновано кілька моделей, заснованих на блокчейні [22].

Заснована на блокчейні модель 'medichain' була запропонована Rahul et al. [23]. Ця модель використовує блокчейн як базу даних для зберігання повної інформації про випадок пацієнта в блоці. Записи транзакцій хешуються для зберігання отриманих хеш-значень у дереві Merkle, щоб забезпечити безпеку даних та запобігти підробці, тим самим зменшуючи помилки при прийнятті клінічних рішень. Щоб вирішити проблему широкого спектру джерел та різноманітних структур медичних даних, дані з усіх полів об'єднуються в єдиний гіперпростір, що зберігається у запропонованій структурі. У цьому методі використовується ланцюгове зберігання. Однак блокчейн менш масштабований. Зберігання даних у мережі також коштує дорого. Wu впроваджує орієнтовану на пацієнта модель контролю доступу із збереженням конфіденційності в процес контролю доступу до приватної інформації в системах охорони здоров'я [24]. Потім технологія блокчейн використовується для створення приватної платформи зберігання інформації, а для реалізації передачі інформації використовуються стандартні криптографічні алгоритми. У цьому процесі конфіденційна інформація також захищається договором авторизації файлів для подальшого запобігання крадіжці медичної конфіденційної інформації. Модель пропонує детальний метод контролю доступу із збереженням конфіденційності, який надає користувачам різні привілеї на основі оцінки їх типів. Інформація про EMR зберігається в хмарній базі даних і розміщується сторонньою організацією, що надає хмарні сервіси. Коли дані зберігаються в хмарі, генерується хеш цих даних. Потім хеш зберігається в блокчейні. Коли дані в хмарі підробляються, їх можна порівняти за хеш-значенням у ланцюжку. У цій моделі консенсусним алгоритмом є POW, який вимагає великої кількості неприпустимих обчислень вузлами. Liu et al. запропонували полегшену модель на основі блокчейна для обміну та захисту медичних даних [25]. Модель використовує технологію повторного шифрування через проксі для забезпечення обміну даними між лікарями в різних лікарнях. Використовувану хеш-функцію важко зіставити. Таким чином, збережену медичну інформацію практично неможливо підробити. Традиційне делеговане підтвердження зацікавленості вдосконалено для отримання нового алгоритму консенсусу, який є більш безпечним і надійним. Розроблено механізм зіставлення захворювань, що дозволяє пацієнтам, які страждають одним і тим же захворюванням, спілкуватися один з одним. Після взаємної аутентифікації сеансові ключі можуть бути встановлені між пацієнтами. Цей механізм може допомогти пацієнтам обмінюватися інформацією про захворювання. Приватна мережа швидка в транзакціях, але менш децентралізована. Вона більше підходить для додатків всере-

дині компаній або установ. Це не застосовується, коли багато пацієнтів і лікарень.

Схема спільного використання EHR на основі гібридного ланцюга запропонована Yu et al. зберігає приватну частину електронного обігу у федеративному ланцюжку, а не приватну частину - у публічному ланцюжку [26]. Тільки ліцензовані користувачі можуть отримати доступ до закритої частини, А до закритої частини можна надати доступ науковим установам для розвитку медицини. Модель також використовує автономне сховище, і в ланцюжку зберігаються тільки хеші даних, щоб запобігти підробці даних, а смарт-контракти можуть автоматично управляти запитом EMR, процесом затвердження і використання. Гібридний ланцюговий підхід, що застосовується в моделі, є дуже новим. Однак вузлам не надаються атрибути, і використовується грубий контроль доступу.

Zou та ін. розробили нову структуру ланцюжка, щоб уникнути проблеми розгалуження, і запропонували заснований на довірі механізм консенсусу для протидії візантійським атакам [27]. Медичні установи можуть накопичувати бали довіри за рахунок безперервного майнінгу в обмін на EMR. Пропонована система репутації повинна накопичувати Репутаційні бали за рахунок великої кількості невірних обчислень. Для отримання права голосу споживається велика кількість енергії. Шахназ та ін. пропонують засновану на блокчейне дрібнозернисту систему доступу, яка надає різні права доступу пацієнтам, лікарям, медсестрам і адміністраторам [28]. Доступ до електронних звернень реєструється в моделі, запропонованій в [29], і для пошуку інформації без дешифрування даних в ланцюжку використовується метод шифрування з можливістю пошуку. Цей метод захищає конфіденційність даних і забезпечує швидкість виконання запиту. Метод також використовує управління доступом на основі ролей. Порівняння різних моделей показано в табл. 2. Як видно з таблиці, майже всі ці моделі використовують автономне сховище. Це пов'язано з невеликою ємністю блокчейна, яка обмежує ємність сховища даних. Це проблема, яку потрібно вирішити в майбутньому

Таблиця 2 – **Порівняння систем зберігання даних на основі блокчейн**

Посилання	Тип блокчейну	Методи зберігання	Шифрування даних
[23]	публічний	мережеве сховище	ні
[24]	публічний	автономне сховище	так
[25]	приватний	автономне сховище	так
[26]	гібридне	автономне сховище	ні
[27]	публічний	автономне сховище	так
[28]	публічний	автономне сховище	ні
[29]	публічний	автономне сховище	так

IOMT включає різні медичні пристрої, які використовують комп'ютерні мережі для підключення та визначення параметрів симптомів пацієнтів. IOMT має великі переваги для лікування пацієнтів із захворюваннями, а виявлення фізичних ознак дозволяє якомога швидше виявити захворювання та звернутися за медичною допомогою [30]. Однак на ринку існує безліч продуктів IOMT без єдиних стандартів управління, і це загрожує витоком інформації [31]. Блокчейн пропонує рішення для забезпечення безпеки медичної IOMT [32]. Чен та ін. розробили систему збору даних на основі IOMT для забезпечення безпечного зберігання та обміну медичними даними [33]. Система може збирати дані з декількох медичних пристроїв одночасно, щоб забезпечити збір медичних записів пацієнта в режимі реального часу під час операції. Система спроектована як схема анонімного обміну медичними даними на базі хмарного сервера з алгоритмом повторного шифрування через проксі. Такий підхід підвищує безпеку обміну приватними медичними даними. Система реалізована на основі Hyperledger Fabric, дозволеної блокчейн-архітектури, з архітектурою розгортання двоканальної структури і кодом медичного ланцюжка, призначеним для управління даними і контролю доступу. Цей метод використовує алгоритм консенсусу kafka. Цей послідовний алгоритм може призвести до збою половини вузлів, але він не може дозволити зловмисним вузлам. Це робить систему більш вразливою до атак.

Нова технологія безпечної аутентифікації на основі блокчейна була запропонована Джафаром для підвищення безпеки конфіденційних медичних даних, що передаються між пацієнтами та лікарнями [34]. Цифровий підпис Lamport Merkle (LMDS) виконує тут генерацію та перевірку підпису, щоб забезпечити безпечну передачу конфіденційних медичних даних у медичних мережах Інтернету речей на основі хмарних серверів. Розумні контракти дозволяють сторонам-учасникам (тобто пацієнтам та лікарям) встановлювати умови та автоматизувати операції через хмарний сервер, зменшуючи роботу третіх сторін. Смарт-контракти також мають різні адреси і облікові записи в блокчейне, так що кожен пристрій Інтернету речей може переглядати і виконувати свої інструкції, тим самим знижуючи накладні витрати на зв'язок. Алькаралле та ін. представити нову модель захищеної передачі зображень та діагностики за допомогою глибокого навчання та блокчейну для IoMT [35]. Запропонована модель включає кілька процесів, зокрема збір даних, захищені транзакції, шифрування хеш-значення та класифікацію даних. На початковому етапі дані про пацієнта збираються за допомогою інструментів Інтернету речей, а потім шифруються за допомогою алгоритму GO-FFO. Крім того, хеші в блокчейні шифруються і стискаються за допомогою технології NIS-BWT. Нарешті, процес класифікації виконується за допомогою моделі DBN. Покращений алгоритм шифрування, хоча і більш безпечний, вимагає більше часу для шифрування та дешифрування, ніж інші алгоритми. У системі, запропонованій Suyel [36], передбачений API-інтерфейс. Цей інтерфейс генерує та підтримує дані про стан здоров'я між медичним працівником та пацієнтом. Крім того, смарт-контракти в повній мірі використовуються в пропонованій системі для запобігання

шкідливої поведінки шляхом встановлення безпечних правил за допомогою смарт-контрактів. Метод використовує лише просту автентифікацію. Якщо вузлів можна присвоїти деталізовані властивості. Це могло б зробити модель більш досконалою. Ху та ін. припускають, що багато досліджень iomt, засновані на блокчейне, в даний час зосереджені на перевірці криптографічних алгоритмів. Час від часу слід приділяти більше уваги недійсним підписам, щоб зменшити ймовірність відмови перевірки. Порівняння моделей iomt на основі блокчейну показано в табл. 3. Смарт - контракти на блокчейні відіграють важливу роль в IOMT. Смарт-контракти не вимагають участі третіх осіб і можуть автоматично виконувати поставлені завдання при виконанні умов. Зазвичай модель використовує криптографічні алгоритми для підвищення безпеки.

Таблиця 3 – **Порівняння моделей IOMT на основі блокчейна**

Посилання	Тип блокчейн	шифрування даних	смарт-контракт	Основа блокчейн
[33]	приватний	так	немає	Повторне шифрування, анонімний обмін
[34]	загальнодоступний	так,	так	Цифровий підпис Лампорта Меркла
[35]	загальнодоступне	так,	так	Шифрування після класифікації даних
[36]	загальнодоступне	так	так	Сховище сертифікатів унікальних даних
[37]	приватний	так	немає	Механізм цифрової верифікації

Конфіденційність медичних даних перешкоджає роботі машинного навчання на основі даних. Федеративне навчання-це новий метод штучного інтелекту, який захищає конфіденційність даних при побудові моделей штучного інтелекту. Федеративне навчання дозволяє декільком вузлам спільно вивчати модель публічно, і між вузлами передаються лише градієнти та втрати, а не самі дані, що може забезпечити хороший захист даних. Однак вузлам потрібно передати дані до центральної установи для наступного обчислення. Блокчейн може бути хорошою альтернативою центральній установі і дозволяє уникнути нечесності центральної структури.

В рамках цієї роботи для управління ключами пропонується метод повторного шифрування через проксі (PRE). Повторне шифрування проксі - сервера-це метод, тоді як проксі-сервер перетворює зашифрований текст у (CA), який зашифрований за допомогою pkA, до зашифрованого тексту B (CB), який можна розшифрувати за допомогою skB, що використовують ключ повторного шифрування (rkA→B). Проксі вимагає лише зашифрованого тексту A та ключа шифрування, який створюється за допомогою skA і pkb поза проксі. Таким чином, власник тексту A може ділитися секретними даними, не розкриваючи секретний ключ або секретні дані. Ключова концепція полягає в тому, щоб розкрити проксі якомога менше даних, оскільки це ненадійна платформа, і дозволити йому виконати зміну ключа з skA на skB для розшифровки зашифрованого тексту A.

Наведений нижче алгоритм пояснює алгоритм повторного шифрування проксі-сервера, який може бути використаний нашій роботі.

1) Генерація ключа:

Нехай $G_1 = \langle g \rangle$ циклічна група простого порядку q. Приватний ключ пацієнта $sk_a = a \epsilon Z_q^*$ вибраний випадковим чином, відкритий ключ $pk_a = g^a$. Особистий ключ лікаря $sk_b = b \epsilon Z_q^*$ вибраний випадковим чином, відкритий ключ $pk_b = g^b, r \in Z_q^*$, обрано випадковим чином, $Z = e(g, g)$:

$$rk_{A \to B} = (g^b)^{1/a} = g^{b/a} \epsilon Z_q^*.$$

2) Шифрування:

Нехай $m \in G_2$. Зашифрований текст

$$C_a = (Z^r \cdot m, g^{ra}) .$$

Розшифровка (пацієнт):

$$m = \frac{Z^r \cdot m}{e(g^{ra}, g^{1/a})} = \frac{Z^r \cdot m}{Z^r} .$$

Повторне шифрування:

$$C_a \to ProxyServer \to C_b ;$$

$$(Z^r \cdot m, g^{ra}) \to (Z^r \cdot m, e(g^{ra}, rk_{A \to B})) ;$$

$$C_b = \left((Z^r \cdot m, e\left(g^{ra}, g^{\frac{b}{a}}\right) \right) ;$$

$$C_b = (Z^r \cdot m, Z^{rb}) .$$

Розшифровка (лікар):

$$m = \frac{Z^r \cdot m}{(Z^{rb})^{1/b}} .$$

В роботі пропонується використання Hyperledger Fabric release 2.2, для створення блокчейн-мережі з N одноранговими вузлами (P1, P2,..., PN), де N більше або дорівнює 3, і вузлом обслуговування замовлень. Вузли є основними елементами мережі, оскільки вони зберігають книги (L) та розумні контракти (S). В ідеалі кожна однорангова інфраструктура повинна керуватися іншою корпорацією. У цьому сенсі вони можуть представляти N зацікавлених сторін таких як: уряд, організації охорони здоров'я, інститути громадянського суспільства, лікарні та інші, — що діють в інтересах підтримки і розвитку сфери охорони здоров'я. Таким чином, вузли надають мережеві послуги, такі як запис та читання книг для адміністраторів та користувачів, що стосуються цих сторін. Теоретично для N не існує верхньої межі, відмінної від тієї, що накладається апаратним та програмним забезпеченням, що використовує протокол консенсусу.

Вузли пов'язані зі своїми відповідними клієнтськими вузлами *(CL_1, CL_2,..., CL_N)*-елементами поза мережею, які дозволяють додатку підключатися до блокчейну, тобто зовнішній додаток отримує доступ до реєстру і смарт-контрактів через з'єднання клієнт-одноранговий вузол. Крім того, Hyperledger Fabric розглядає канал (C) як основний канал зв'язку, за допомогою якого однорангові вузли та клієнти можуть створити консорціум із чітко визначеною політикою, забезпечуючи таким чином механізм ізоляції активів та транзакцій від решти мережі. У цьому контексті кожен смарт-контракт і відповідний реєстр можуть бути окремо викликані по певному каналу тільки користувачами,

раніше зареєстрованими в консорціумі, тим самим забезпечуючи сумісність і конфіденційність.

Однорангові вузли призначаються консорціуму: уряду, організаціям охорони здоров'я, інститутам громадянського суспільства та лікарням у нашому прикладі — відповідними центрами сертифікації *(CA_1, CA_2,..., CA_N)*, елементами, які генерують інфраструктуру відкритих та приватних ключів для видачі посвідчень особи за допомогою цифрових сертифікатів. Всякий раз, коли один з членів Консорціуму встановлює однорангове з'єднання з клієнтом для доступу до ресурсів блокчейна, органи сертифікації підтверджують каналу цифрову ідентифікацію заявника і її/його права на використання необхідного смарт-контракту. Нарешті, вузол обслуговування замовлень забезпечує взаємодію між одноранговими вузлами під час надсилання транзакції та забезпечує узгодженість книги після виконання узгодженого протоколу. У Hyperledger Fabric політика схвалення здійснюється в результаті три етапного процесу:

1) пропозиція
2) замовлення та упаковка
3) перевірка та фіксація.

На рис. 2 представлений архітектура системи, що пропонується в роботі.

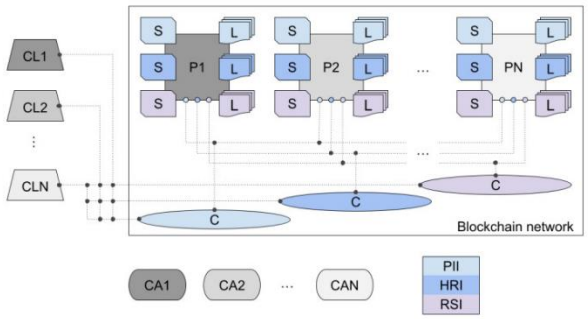

Рис. 2. Архітектура системи, що пропонується:
HRI: інформація про медичну документацію;
PII: інформація про особу; C: канал;
RSI: інформація про обмін записами;
P: одноранговий вузол; S: розумний контракт;
L: книга; CL: клієнт; CA: центр сертифікації
(джерело: власна розробка)

Розробка нашої блокчейн-мережі з урахуванням N партнерів по схваленню і їх відповідних клієнтів і центрів сертифікації. Кожен канал пов'язаний з певним набором реєстрів і смарт-контрактів, які відповідно називаються особистою інформацією, інформацією про стан здоров'я та інформацією про обмін записами. В ідеалі кожен потрійний одноранговий центр сертифікації-клієнт-центр сертифікації повинен керуватися іншою організацією чи установою.

Для підтримки розробки архітектурної моделі буде реалізовано прототип системи заснованої на блокчейні для обміну медичними даними пацієнтів.

При використанні 3-однорангової мережі наш перший тест налаштований на виконання робочого навантаження від 100 до 2500 одночасних відправлень метаданих про стан здоров'я з кроком в 100 кроків по кожному смарт-контрактом шаблонів PII, HRI і RSI. Ми обмежуємо наш тест 2500 запитами, оскільки Hyperledger Fabric стандартно налаштований на виконання максимум 2500 одночасних запитів. Сценарії написання налаштовані на використання 5 працівників, які відправляють одночасно 10 000 транзакцій, загальна сума кожної з яких становить 50 000. Сценарії читання налаштовані на паралельне використання одних і тих же 5 працівників, але для випадкового запиту записів протягом 600 секунд безперервної роботи. Контролер швидкості підтримується в режимі фіксованого завантаження, починаючи з 50 tps і 500 tps для транзакцій запису і читання відповідно, і збільшуючись до досягнення максимальних швидкостей. Оскільки PII, HRI та RSI призначені для зберігання лише зашифрованих текстів, у нашому тесті всі змодельовані подання метаданих про стан здоров'я генеруються випадковим чином у вигляді рядків фіксованої довжини для кожного поля смарт-контракту. Порожня блокчейн-мережа створюється в кожному навантажувальному тесті, щоб гарантувати рівні умови. Наше тестове середовище складається з комп'ютера з процесором Intel Xeon E-2246g (12 МБ кеш-пам'яті, 3,60 ГГц, 6 ядер, 12 потоків), графічним адаптером NVIDIA Quadro P1000 і оперативною пам'яттю об'ємом 16 ГБ, що працює під управлінням 64-розрядної операційної системи Ubuntu 18.04.5 LTS.

Результат роботи прототип системи відображає не тільки час виконання кожного компонента в пропонованій нами системі на основі блокчейна, але також відображає час виконання всієї системи одним користувач. Час, необхідний для операції збереження та вилучення, обчислюється на основі синтетичного навантаження МД розміром 128, 512 КБ, 2, 8, 32 і 128 МБ. Для зберігання МД в пропонованій системі на основі блокчейна клієнт-власник МД і сервер шлюзу управляють операцією сховища. Середній час виконання кожного з підпроцесів двох елементів показано в табл. 4 і 5 відповідно.

У табл. 4 представлені детальні дані про час виконання запитів клієнта-власника МД. Клієнт-власник МД виконує п'ять процесів, включаючи хешування, шифрування, генерацію ключів повторного шифрування, підписання та надсилання даних на сервер шлюзу для збереження МД. Згідно з табл. 4, час виконання трьох процесів, включаючи хешування, шифрування та надсилання даних, залежить від розміру даних МД, в той час як час виконання процесів генерації ключа повторного шифрування і підпису залишається незмінним. Таким чином, час виконання для трьох процесів (тобто хешування, шифрування та надсилання даних) можна визначити за допомогою щільності ймовірності Функція (PDF) та час виконання решти двох процесів (Генерація ключа повторного шифрування і підписання) можуть бути представлені у вигляді константи.

Сервер шлюзу також виконує п'ять основних процесів, включаючи Перевірка підпису, завантаження даних, локальне зберігання даних, підписання та зберігання файлу журналу в блокчейні. Як показано в табл. 5, час виконання лише одного процесу, який є завантаженням даних, залежить від розміру МД, в той час як час виконання інших процесів

залишається практично постійним. Щоб отримати МД в пропонованій системі на основі блокчейна, користувальницький клієнт і сервер шлюзу виконують операцію вилучення. Середній показник час виконання кожного з підпроцесів цих двох елементів також показано в табл. 6 і 7 відповідно.

Таблиця 4 – **Час виконання операцій клієнтом-власником МД**

Розмір даних	Час хешування	Час шифрування	Час генерації ключа повторного шифрування	Час підпису	Час відправки даних
128 КБ	10.29	91.18	24.16	1.16	152.73
512 КБ	18.24	94.01	24.66	1.15	173.87
2 МБ	40,63	101,19	26,15	1,18	268,95
8 МБ	65,60	142,03	26,88	1,16	421,67
32 МБ	241,80	303,79	27,00	1,31	645,70
128 МБ 1	946.10	1828.21	27.10	1.42	2200.36

Таблиця 5 – **Час виконання операцій сервером-шлюзу**

Розмір даних	Час перевірки підпису	Час завантаження	Час збереження локальної копії	Час входу на сервер	Час блокування
128 ГБ	0,07	157,41	31,57	1,24	3372,79
512 ГБ	0,07	221,65	24,66	1,15	3173,87
2 МБ	0,07	273,65	38,40	1,30	3365,34
8 МБ	0,08	457,51	33,82	1,49	3238,70
32 МБ	0.06	654.280	28.62	1.60	2935.02
128 МБ	0.07	2150.87	38.71	1.58	3381.05

Таблиця 6 – **Час виконання операцій в процесі отримання МД користувачем-клієнтом**

Розмір даних	Час пошуку МД по блокчейн	Час підтвердження підпису (власник, сервер)	Час підпису користувача	Час відправки запиту	Час розшифровки
128 КБ	785,69	0,07, 0,04	1,33	115,36	3,20
512 КБ	820,48	0,07, 0,04	1,29	124,30	6,04
2 МБ	751,15	0,07, 0,04	1,31	110,77	16,63
8 МБ	770,61	0,07, 0,04	1,23	136,25	59,41
32 МБ	823,37	0,07, 0,04	1,75	127,79	238,90
128 МБ	796,67	0,07, 0,04	1,39	128,77	1814,79

Таблиця 7 – **Час виконання операцій на сервері-шлюзу для процесу вилучення МД**

Розмір даних	Час перевірки підпису користувача	Час збереження журналу в блокчейн	Час повторного шифрування	Час завантаження даних
128 КБ	0.11	3304.62	30.59	38.02
512 КБ	0.10	3288.55	31.50	78.27
2 МБ	0.10	3308.91	34.28	152.31
8 МБ	0.11	3398.48	58.75	214.84
32 МБ	0.13	3367.66	79.70	469.33
128 МБ	0.12	3372.62	80.65	1093.03

Згідно з табл. 6 час виконання розшифровки залежить тільки від розміру даних. Сервер шлюзу також виконає чотири основних процеси, включаючи перевірку підпису, збереження файлу журналу на блокчейні, відбувається завантаження даних і повторне шифрування. Час виконання двох процесів, включаючи завантаження даних і повторне шифрування, залежить від розміру даних, як показано в табл. 7. Щоб отримати МД, Користувач-клієнт виконує шість основних процесів, включаючи пошук в блокчейне, перевірку підпису власника, Перевірка підпису сервера, підписання, надсилання запиту на сервер шлюзу і розшифровку отриманих МД. Згідно з табл. 4-7 для оцінки середнього часу роботи використовуються найближчі середні дані (32 МБ даних). Час, необхідний клієнту-власнику МД для виконання операції зі сховищем, становить 1219,606 мс, а час обслуговування сервера шлюзу при виконанні операції зі сховищем становить 3619,578 мс.

Таким чином, середній час роботи системи для операції зберігання становить приблизно 4839,184 мс або 4,84 с. Час, необхідний для користувача клієнту для виконання операції вилучення, становить 1191,919 мс, а час обслуговування сервера шлюзу для виконання операції вилучення становить 3916,822 мс. В результаті час роботи системи для операції вилучення становить приблизно 5108,741 мс або 5,19 с. ці результати показують середню продуктивність для одного користувача.

Архітектурна модель моделюється з урахуванням робочого навантаження, і результат моделювання порівнюється з результатом, що спостерігається в системі-прототипі. При виконанні прототипу середній час відгуку для операції зберігання становить 4,84 сек, тоді як середній час відгуку для операції зберігання становить 5,0 с.

Таким чином, моделювання передбачало середній час відгуку з відносною похибкою 3,3% для

операції зберігання. Середній час відгуку на операцію вилучення, що виконується системою-прототипом, становить 5,11 с, в той час як середній час відгуку для операції вилучення, яке оцінюється архітектурною моделлю, становить 5,3 с. моделювання передбачає середній час відгуку з відносною похибкою 3,7% для операції вилучення. Таким чином, моделювання передбачало час відгуку, близький до результату, що спостерігається в системі-прототипі.

Висновки

У роботі пропонується архітектурна модель системи обміну медичними даними на основі блокчейн. В роботі реалізовано прототип системи для дослідження ключових параметрів запропонованої архітектури. Робота прототипу системи була перевірена на пакетах медичних даних, що складаються з даних різних розмірів, включаючи 128КБ,512 КБ, 2, 8, 32 і 128 МБ. Результуючий час виконання ділиться на дві групи. У першій групі час кожного виконання змінюється залежно від розміру пакету МД та часу виконання. У другій групі час виконання залишається майже таким же. Таким чином, час виконання першої групи моделюється за допомогою функції PDF, тоді як час виконання другої групи моделюється з їх початковими значеннями як константа. Архітектурна модель оцінює, що запропонована модель системи може реагувати протягом 4 хвилин на 165000 звернень в день. Однак результат моделювання зі швидкістю надходження 3,8 запити в секунду показує, що час відгуку для всіх операцій становить <20 хв, і 50% цих відгуків знаходяться в межах 8 хвилин від аварійних вимог. Результат моделювання зі швидкістю прибуття 15,2 в секунду показує, що тільки 30% часу реагування укладається в 8 хвилин, відведених на екстрену допомогу, однак використання системи кожну 1 годину для всіх людей може бути дуже рідкісним випадком.

Запропонований прототип системи має деякі обмеження. Блокчейн hyperledger виконується з фіктивним консенсусом. Мережа між кожним комп'ютером моделюється без істотних мережевих затримок.. Однак, запропонована архітектурна модель забезпечує основу для майбутніх досліджень оптимальної конфігурації системи, таких як нефункціональні властивості.

Список літератури

1. Häyrinen Kristiina, Saranto K, Nykänen Pirkko. Definition, structure, content, use and impacts of electronic health records: a review of the research literature. Int J Med Inform. 2008 May;77(5):291–304. doi: 10.1016/j.ijmedinf.2007.09.001.S1386-5056(07)00168-2
2. Hripcsak G, Albers DJ. Next-generation phenotyping of electronic health records. J Am Med Inform Assoc. 2013 Jan 01;20(1):117–21. doi: 10.1136/amiajnl-2012-001145. http://europepmc.org/abstract/MED/22955496 .amiajnl-2012-001145
3. Ludwick DA, Doucette J. Adopting electronic medical records in primary care: lessons learned from health information systems implementation experience in seven countries. Int J Med Inform. 2009 Jan;78(1):22–31. doi: 10.1016/j.ijmedinf.2008.06.005.S1386-5056(08)00092-0
4. Zahabi M, Kaber DB, Swangnetr M. Usability and Safety in Electronic Medical Records Interface Design: A Review of Recent Literature and Guideline Formulation. Hum Factors. 2015 Aug;57(5):805–34. doi: 10.1177/0018720815576827.0018720815576827
5. Mikkelsen G, Aasly J. Concordance of information in parallel electronic and paper based patient records. International Journal of Medical Informatics. 2001 Oct;63(3):123–131. doi: 10.1016/s1386-5056(01)00152-6
6. Thiru K, Hassey A, Sullivan F. Systematic review of scope and quality of electronic patient record data in primary care. BMJ. 2003 May 17;326(7398):1070. doi: 10.1136/bmj.326.7398.1070. http://europepmc.org/abstract/MED/12750210 .326/7398/1070
7. Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc. 2006;13(2):121–6. doi: 10.1197/jamia.M2025. http://europepmc.org/abstract/MED/16357345 .M2025
8. Archer N, Fevrier-Thomas U, Lokker C, McKibbon KA, Straus SE. Personal health records: a scoping review. J Am Med Inform Assoc. 2011;18(4):515–22. doi: 10.1136/amiajnl-2011-000105. http://europepmc.org/abstract/MED/21672914 .amiajnl-2011-000105
9. Roehrs A, da Costa Cristiano André, Righi RDR, de Oliveira Kleinner Silva Farias. Personal Health Records: A Systematic Literature Review. J Med Internet Res. 2017 Jan 06;19(1):e13. doi: 10.2196/jmir.5876.
10. Rudin RS, Motala A, Goldzweig CL, Shekelle PG. Usage and Effect of Health Information Exchange. Ann Intern Med. 2014 Dec 02;161(11):803. doi: 10.7326/m14-0877
11. Williams C, Mostashari F, Mertz K, Hogin E, Atwal P. From the Office of the National Coordinator: the strategy for advancing the exchange of health information. Health Aff (Millwood) 2012 Mar;31(3):527–36. doi: 10.1377/hlthaff.2011.1314.31/3/527
12. Cimino JJ, Frisse ME, Halamka J, Sweeney L, Yasnoff W. Consumer-mediated health information exchanges: the 2012 ACMI debate. J Biomed Inform. 2014 Apr;48:5–15. doi: 10.1016/j.jbi.2014.02.009. https://linkinghub.elsevier.com/retrieve/pii/S1532-0464(14)00046-X .S1532-0464(14)00046-X
13. Zhuang Y, Sheets LR, Chen Y, Shae Z, Tsai JJ, Shyu C. A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. IEEE J. Biomed. Health Inform. 2020 Aug;24(8):2169–2176. doi: 10.1109/jbhi.2020.2993072.
14. Gordon WJ, Catalini C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Comput Struct Biotechnol J. 2018;16:224–230. doi: 10.1016/j.csbj.2018.06.003. https://linkinghub.elsevier.com/retrieve/pii/S2001-0370(18)30028-X .S2001-0370(18)30028-X
15. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput Struct Biotechnol J. 2018;16:267–278. doi: 10.1016/j.csbj.2018.07.004. https://linkinghub.elsevier.com/retrieve/pii/S2001-0370(18)30037-0 .S2001-0370(18)30037-0
16. Murphy DR, Satterly T, Rogith D, Sittig DF, Singh H. Barriers and facilitators impacting reliability of the electronic health record-facilitated total testing process. Int J Med Inform. 2019 Jul;127:102–108. doi: 10.1016/j.ijmedinf.2019.04.004.S1386-5056(18)31386-8

17. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020 Feb;50:102407. doi: 10.1016/j.jisa.2019.102407
18. Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society. 2018 May;39:283–297. doi: 10.1016/j.scs.2018.02.014.
19. Zhang A, Lin X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst. 2018 Jun 28;42(8):140. doi: 10.1007/s10916-018-0995-5.10.1007/s10916-018-0995-5
20. Cao S, Zhang G, Liu P, Zhang X, Neri F. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences. 2019 Jun;485:427–440. doi: 10.1016/j.ins.2019.02.038.
21. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin: Open Source P2P Money. 2008. [2021-04-23]. https://bitcoin.org/bitcoin.pdf .
22. Ferdous MS, Chowdhury MJM, Hoque MA. A survey of consensus algorithms in public blockchain systems for crypto-currencies. Journal of Network and Computer Applications. 2021 May;182:103035. doi: 10.1016/j.jnca.2021.103035.
23. Kuo T, Zavaleta Rojas H, Ohno-Machado L. Comparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inform Assoc. 2019 May 01;26(5):462–478. doi: 10.1093/jamia/ocy185.
24. McGhin T, Choo KR, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications. 2019 Jun;135:62–75. doi: 10.1016/j.jnca.2019.02.027.
25. Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Implementing Blockchains for Efficient Health Care: Systematic Review. J Med Internet Res. 2019 Feb 12;21(2):e12439. doi: 10.2196/12439. https://www.jmir.org/2019/2/e12439/ v21i2e12439
26. Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. J Med Syst. 2019 Sep 14;43(10):320. doi: 10.1007/s10916-019-1445-8.10.1007/s10916-019-1445-8 [PubMed: 31522262] [CrossRef: 10.1007/s10916-019-1445-8]
27. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD); August 22-24; Vienna, Austria. 2016. pp. 25–30
28. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016 Oct;40(10):218. doi: 10.1007/s10916-016-0574-6.10.1007/s10916-016-0574-6
29. Roehrs A, da Costa Cristiano André, da Rosa Righi Rodrigo. OmniPHR: A distributed architecture model to integrate personal health records. J Biomed Inform. 2017 Jul;71:70–81. doi: 10.1016/j.jbi.2017.05.012.
30. Ichikawa D, Kashiyama M, Ueno T. Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR Mhealth Uhealth. 2017 Jul 26;5(7):e111. doi: 10.2196/mhealth.7938. https://mhealth.jmir.org/2017/7/e111/ v5i7e111
31. Mannaro K, Baralla G, Pinna A, Ibba S. A Blockchain Approach Applied to a Teledermatology Platform in the Sardinian Region (Italy) Information. 2018 Feb 23;9(2):44. doi: 10.3390/info9020044
32. Kovalenko, A. and Kuchuk, H. (2022), "Methods to Manage Data in Self-healing Systems", Studies in Systems, Decision and Control, Vol. 425, pp. 113–171, doi: https://doi.org/10.1007/978-3-030-96546-4_3
33. Ji Y, Zhang J, Ma J, Yang C, Yao X. BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. J Med Syst. 2018 Jun 30;42(8):147. doi: 10.1007/s10916-018-0998-2.10.1007/s10916-018-0998-2 [PubMed: 29961160] [CrossRef: 10.1007/s10916-018-0998-2]
34. Kleinaki A, Mytis-Gkometh P, Drosatos G, Efraimidis PS, Kaldoudi E. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. Comput Struct Biotechnol J. 2018;16:288–297. doi: 10.1016/j.csbj.2018.08.002. https://linkinghub.elsevier.com/retrieve/pii/S2001-0370(18)30040-0 .S2001-0370(18)30040-0
35. Jamil F, Hang L, Kim K, Kim D. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. Electronics. 2019 May 07;8(5):505. doi: 10.3390/electronics8050505.
36. Patel V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics J. 2019 Dec;25(4):1398–1411. doi: 10.1177/1460458218769699.
37. Jamil F, Ahmad S, Iqbal N, Kim D. Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals. Sensors (Basel) 2020 Apr 13;20(8):2195. doi: 10.3390/s20082195. https://www.mdpi.com/resolver?pii=s20082195 .s2008215.

Received (Надійшла) 02.04.2024
Accepted for publication (Прийнята до друку) 05.06.2024

Development and research of an architectural model of a blockchain-based personal data exchange system.

Olexander Shmatko, Dmytro Kulinich, Tetiana Gorbach

Abstract. Abstract. Relevance. Modern society is facing a growing need for secure, reliable and transparent exchange of personal data of patients in the field of healthcare. Protecting the confidentiality and integrity of medical information is a priority to ensure quality and efficient medical care. Blockchain technologies provide a promising tool for solving this problem by enabling the creation of a decentralized and secure system for the exchange of personal patient data. **The purpose** of this work is to ensure a high level of security and confidentiality of medical data, as well as to increase the efficiency of healthcare processes by developing software components of a system for exchanging personal data of patients based on blockchain technologies. **The object of research** is the system of exchange of personal data of patients in the healthcare sector. **The subject of the** study is software components based on blockchain technologies designed to ensure the security, transparency and efficiency of medical information exchange. **Results.** This paper proposes an architectural model of a secure and efficient health data exchange system that can be widely implemented in the healthcare sector. **Conclusion.** The introduction of a secure personal data exchange system based on blockchain technology in the healthcare sector will help improve the quality of medical care and provide faster access to important data for medical personnel. Theoretical significance lies in expanding knowledge about the use of blockchain technologies in the healthcare sector and the security and confidentiality of medical information. This study can serve as a basis for further research in this area and contribute to the development of new methods and approaches to the exchange of medical data.

Keywords: blockchain, personal data of patients, IoTM, smart contracts, Ethereum, model of medical data exchange system.