УДК 004.9 **doi: 10.26906/SUNZ.2024.2.155**

О. В. Шматко, С. С. Сальніков

Харківський національний технічний університет радіоелектроніки, Харків, Україна

МОДЕЛЬ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ОБМІНУ ЕЛЕКТРИЧНИМИ МЕДИЧНИМИ КАРТКАМИ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Анотація. Актуальність. У сучасну цифрову епоху безпека даних стає першорядною турботою в різних секторах, особливо в охороні здоров'я. Критичний характер даних пацієнтів вимагає надійних механізмів захисту від несанкціонованого доступу та потенційного зловмисного використання. У цій статті розглядається мінливий ландшафт безпеки даних в секторі охорони здоров'я, підкреслюються уразливості, пов'язані з традиційними системами зберігання даних. В роботі пропонується модель системи для збору, зберігання та обміну електронними медичними картками (Electronic Health Records – EHR). В роботі досліджено технологію блокчейн як революційний підхід до вирішення проблем безпеки обміну конфіденційними медичними даними. **Метою даної роботи** є підвищення конфіденційності медичних даних, їх цілісності та доступності, а також забезпечення надійного обміну цими даними між медичними закладами та іншими учасниками за рахунок проєктування та розробки програмних компонентів для створення захищених систем передачі медичної інформації на основі технології блокчейн**. Об'єкт дослідження** включає в себе системи передачі медичної інформації, які забезпечують обмін даними між медичними закладами, спеціалістами та пацієнтами, забезпечуючи конфіденційність, цілісність та доступність цих даних. **Предметом дослідження** є методи та засоби проектування та розробки програмних компонентів, необхідні для створення і підтримки захищених систем передачі медичної інформації. Ці компоненти включають в себе програмне забезпечення для шифрування, аутентифікації, авторизації, а також механізми для забезпечення відмовостійкості та відновлення даних. **Результати.** У даній роботі запропоновано модель децентралізованої системи для збору, зберігання та обміну EHR. **Висновок.** Результати цього дослідження підкреслюють трансформаційний потенціал технології блокчейн у переосмисленні парадигм безпеки даних у секторі охорони здоров'я. Створюючи безпечну, прозору та ефективну платформу для управління EHR, запропонована модель не тільки підвищує конфіденційність та цілісність медичних даних, але й робить значний внесок у покращення якості надання медичної допомоги та результатів лікування пацієнтів. У міру просування вперед впровадження децентралізованих систем, заснованих на технології блокчейн, в охороні здоров'я являє собою багатообіцяючий шлях для вирішення складних проблем, пов'язаних з безпекою і конфіденційністю даних, тим самим прокладаючи шлях до більш стійкої і орієнтованої на пацієнта екосистемі охорони здоров'я.

Ключові слова: блокчейн, електронні медичні картки, смарт-контракти, Ethereum, MetaMask, архітектурна модель.

Вступ

Діагностичні дані пацієнтів збільшуються, кількість медичних інформаційних систем (МІС) зростає. Як результат, кількість інформації про пацієнта збереженої на цифрових носіях – збільшується [1, 2]. Потреба у функціональному змісті цих систем також зростає.

Незважаючи на те, що системи МІС зараз широко застосовуються в Україні, їх область застосування наразі включає лише первинну медицину. Значна частина лікарів досі використовують паперові носії у своїй роботі.

В Україні буде впроваджена електронна система охорони здоров'я eHealth, яка гарантує права пацієнтів щодо якості медичних послуг та оптимізує взаємодію між пацієнтом та лікарем шляхом автоматизації, медичного обліку та електронного управління медичною інформацією.

EHealth складається з центральної бази та великого розмаїття МІС. Центральна база даних Україні забезпечує прозорість витрат охорони здоров'я та можливість руху інформації без паперів з поступовим переходом до електронного обліку, включаючи електронні рецепти, електронні картки та електронні довідки, створювати нові електронні послуги, створення ділового середовища, створення інноваційних продуктів у медицині та просування медичного ринку ІТ загалом.

Завдяки швидкому доступу до всієї інформації про пацієнта, лікар отримує цілісне уявлення про ваше здоров'я, а повний анамнез в електронній формі допомагає поставити правильний діагноз. Більшість медичних послуг можна отримати, не виходячи з дому. Модель фінансування медичних закладів з допомогою системи eHealth кардинально змінилася. Діє принцип – «гроші йдуть за пацієнтом». Система дозволяє контролювати ефективність, з якою витрачаються державні кошти. Перш за все, eHealth охопить основну допомогу: лікарі загальної практики, терапевти та педіатри. Пацієнти підписують заяви від вибраних лікарів, а лікарі реєструють їх у системі. Це допоможе державі оплатити роботу лікаря з кожним пацієнтом.

Захист прав пацієнтів на конфіденційність медичних даних стає дедалі складнішим із появою електронних медичних записів (EHR), якими обмінюються на різних рівнях системи охорони здоров'я. Така розширена можливість підключення різних користувачів медичних даних збільшує ризик порушень, створюючи значну загрозу для закладів охорони здоров'я. Враховуючи делікатний характер медичних записів, будь-яке порушення конфіденційності може призвести до серйозних наслідків, включаючи наклеп, дискримінацію та невиправданий стрес як для пацієнтів, так і для опікунів. Забезпечення конфіденційності та цілісності медичних записів вимагає суворого контролю доступу до EHR, а також

збереження їх цілісності для запобігання несанкціонованим змінам або знищенню [3].

В роботі [4] описується структура безпеки, розроблена для створення захищеної, адаптованої та надійної системи EHR, що задовольняє нагальну потребу в передових заходах безпеки у світлі вразливостей, властивих існуючим системам. Автори узагальнюють існуючі дослідження безпеки EHR, що висвітлюють різні стратегії безпеки, що включають адміністративні, фізичні та технічні запобіжні заходи, необхідні для захисту складної екосистеми охорони здоров'я. Незважаючи на ці досягнення, існує чітка потреба в кращих рішеннях безпеки для конкретних установ, які відповідають мінливим вимогам майбутніх організацій охорони здоров'я.

Кілька досліджень [5-8] сприяють цьому дискурсу, представляючи рамки та моделі, які вирішують багатогранні проблеми безпеки в інформаційних системах охорони здоров'я. Наприклад, концептуальна основа, запропонована в роботі [9] підкреслює відмінності в методах безпеки в різних лікарнях і виступає за етичне управління електронними медичними записами в усьому спектрі охорони здоров'я. Тим часом у дослідженні [10] підкреслюється, що дотримання правил HIPAA є наріжним каменем забезпечення безпеки медичної інформації, що передбачає всебічне дотримання цих рекомендацій як стандарту для організацій охорони здоров'я.

Інші матеріали [11-13], пропонують клієнт-серверні моделі та їх дослідження в системах обміну медичними даними. Автори роботи [13] дають уявлення про пом'якшення внутрішніх загроз в медичних установах, використовуючи інструменти дерева атак для детального аналізу потенційних порушень безпеки.

Інноваційні рішення, такі як модель контролю доступу [14] на основі смарт-контрактів пропонують структуру фреймворку для зниження ризиків хакерських атак. Не менш заслуговують на увагу запропонована архітектура хмарних сховищ даних[15], яка може забезпечити підвищений ступінь безпеки для передачі інформації на аутсорсинг в середовищі хмарних обчислень із залученням численних незалежних хмарних провайдерів. Фреймворк включає в себе методи подвійного шифрування і фрагментації даних, які забезпечують безпечне поширення інформації в мультихмарному середовищі. В роботі [16] запропоновано гібридну архітектуру для доступу до записів пацієнтів із збереженням конфіденційності в хмарній системі. Пропонований фреймворк дозволяє пацієнтам керувати доступом до своїх медичних записів, полегшуючи безперешкодний обмін даними між ними медичні установи, забезпечуючи при цьому наявність протоколів екстреного доступу. Автори роботи [17] розглядають технологію розподіленого реєстру (DLT), відому як IOTA. IOTA вирішує проблеми пов'язані з масштабованістю та продуктивністю блокчейну, використовуючи структуру спрямованого ациклічного графіка (DAG), що полегшує паралельне додавання транзакцій. Це нововведення значно скорочує час підтвердження транзакції і дозволяє обробляти необмежену кількість транзакцій одночасно. Протокол обміну повідомленнями з замаскованою аутентифікацією (MAM) в IOTA забезпечує безпечну передачу зашифрованих потоків даних у вигляді транзакцій.

Аналіз останніх досліджень підкреслює необхідність застосування передових, спеціально розроблених заходів безпеки для зміцнення цілісності та конфіденційності систем EHR, тим самим захищаючи приватне життя пацієнтів і підвищуючи стійкість інформаційних систем охорони здоров'я до виникаючих загроз.

Виходячи з аналізу останніх досліджень і публікацій можна зробити висновок, що питання проєктування та розробки інформаційних систем для збору, зберігання та обробки електронних медичних карток на основі технології блокчейн є актуальним.

Метою цієї роботи є підвищення конфіденційності медичних даних, їх цілісності та доступності, а також забезпечення надійного обміну цими даними між медичними закладами та іншими учасниками за рахунок проєктування та розробки програмних компонентів для створення захищених систем передачі медичної інформації на основі технології блокчейн.

Основна частина

Традиційний підхід до використання технології зберігання та обробки медичних даних передбачає централізацію зберігання даних в хмарі, що викликає серйозні проблеми з безпекою доступу до даних і контролю за ними. У сфері охорони здоров'я, де дані пацієнтів є одночасно критичними та конфіденційними, забезпечення надійних заходів безпеки для інформації, що зберігається в хмарі, має першорядне значення [18]. Пацієнти повинні мати право диктувати дозволи на доступ до своїх даних, що вимагає створення безпечного та контрольованого середовища для зберігання даних у хмарі. Щоб вирішити ці проблеми безпеки, автори роботи звернулися до перевірених можливостей технології блокчейн. Серед безлічі блокчейн-платформ Ethereum виділяється своїми чудовими функціями безпеки, що робить його нашим вибором для цього додатка. Причини вибору Ethereum включають такі:

Налагоджена мережа Ethereum: завдяки своєму великому послужному списку мережа Ethereum є одночасно великою і перевіреною часом, забезпечуючи надійну і безпечну основу для додатків.

Функціональність і смарт-контракти: багатий набір функцій Ethereum, зокрема підтримка смарт-контрактів, забезпечує безпечне і децентралізоване зберігання даних, що робить його ідеальним вибором для нашої системи.

Активна підтримка спільноти: Ethereum отримує вигоду від надійної та активної спільноти, яка постійно досліджує інноваційні способи вдосконалення технології.

Використовуючи ці переваги, авторам розроблено смарт-контракт на базі Ethereum, призначений для полегшення спілкування між пацієнтами та лікарями. Цей смарт-контракт спрощує процес спостереження лікарів за своїми пацієнтами, підвищуючи ефективність і безпеку взаємодії пацієнта і лікаря.

Концептуальна архітектура запропонованої системи інтегрує технологію блокчейн в систему обміну медичними даними, як показано на рис. 1.

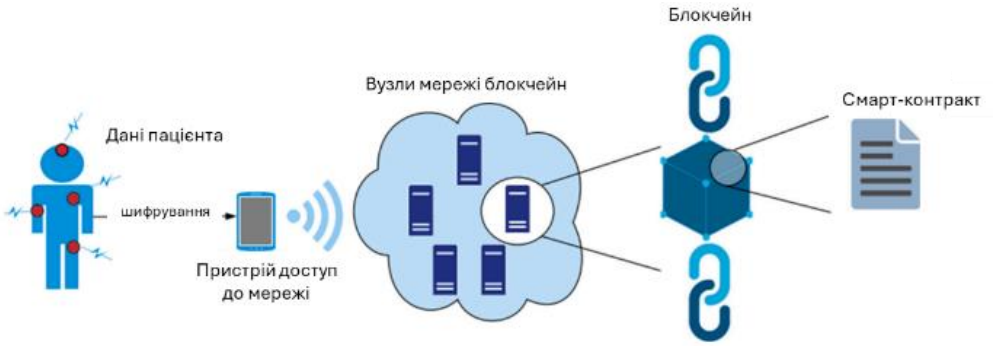


Рис. 1. Концептуальна архітектура системи, що пропонується (джерело: власна розробка)

В запропонованій моделі дані пацієнта надійно шифруються та зберігаються в хмарі, гарантуючи, що конфіденційна інформація залишається захищеною протягом усього процесу її зберіганні та обміну. На рис. 2 показана схема роботи системи всякий раз, коли пацієнт вибирає перегляд медичних записів за допомогою MetaMask або децентралізованого вебсайту системи обміну EHR. Отримуючи доступ до приватного ключа з гаманця Ethereum, користувач автоматично входить в систему.

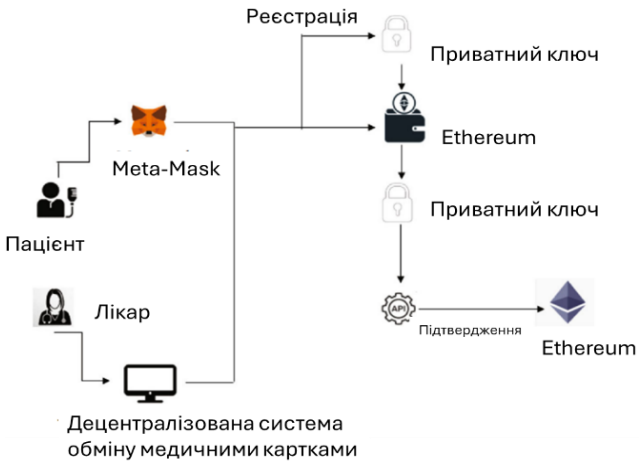


Рис. 2. Схема протоколу системи обміну EHR

Ethereum wallet - це гаманець для холодного зберігання. В результаті, порівняння з іншими гарячими гаманцями, небезпека компрометації досить низька. Крім того, якщо гаджет втрачено, пацієнтам можна просто видати новий, не піддаючись штрафу за втрату своїх медичних записів. Гаманець можна використовувати для підпису будь-яких документів або для інших потреб при перевірці особистості. Цей гаманець також можна використовувати для проведення багатосторонньої верифікації пацієнта. Він може бути використаний для створення системи контролю доступу до записів на основі ролей, а також системи розподіленої ідентифікації власності на основі блокчейна. У випадку невідкладної медичної допомоги може бути реалізований аналогічний багатосторонній механізм отримання дозволів для отримання доступу до записів пацієнтів.

На рис. 3 показана структурна схема. Дизайн, який ми пропонуємо, складається з чотирьох основних компонентів: Користувач додаток, протокол рукостискання блокчейна, хмара і загальнодоступна блокчейн-мережа. Система являє собою віртуальне представництво, яке служить двом цілям. По-перше, він надає користувачам доступ до інтерфейсів додатків. Лікарі та системні адміністратори - це два типи користувачів у нашій системі.

У кожного користувача є своя функція. В результаті користувальницький додаток надає різні інтерфейси користувача залежно від ролі користувач. По-друге, на основі введених користувачем даних користувальницький додаток створює початкову транзакцію. З метою підтвердження транзакція відправляється в протокол рукостискання блокчейна. Нарешті, користувальницький інтерфейс встановлює зв'язок між користувачами і протоколом рукостискання блокчейна.

Фундаментальним компонентом запропонованої архітектури є протокол blockchain handshake (BH). Цей компонент з'єднує сервер бази даних, блокчейн-мережу і хмарну систему медичних записів, яка діє як оболонка. Ця запропонована Архітектура використовує блокчейн-мережу Ethereum. Розподілена бухгалтерська книга, що з'єднує блокчейн-вузли, відома як публічна блокчейн-мережа. Блокчейн-вузли - це майнери, які відповідають за оновлення блокчейна на основі методу прийняття рішення. В якості альтернативи блокчейн-вузли приймають транзакції і використовують смарт-контракти мережі для їх аутентифікації. У запропонованому проекті хмара надає дві послуги, які аналогічні тим, які надаються існуючими хмарними сервісами.

Системи адміністрування EHR. Система адміністрування EHR розміщується в якості початкової служби. Зберігання даних-це наступна послуга. Всі медичні записи можуть бути збережені в базі даних. Система адміністрування EHR приймає транзакції з протоколу рукостискання блокчейна, виконує всі обов'язки, пов'язані з ними, і, нарешті, зберігає їх в хмарній базі даних. У відповідь на запити користувачів про доступ хмара надає необхідні дані. На рис. 3 показана структурна схема взаємодії компонентів системи. Дизайн, який пропонується в роботі, складається з чотирьох основних компонентів:

Додаток користувача, протокол рукостискання блокчейна, хмарне сховище і загальнодоступна блокчейн-мережа. Система являє собою віртуальне представництво, яке служить двом цілям. По-перше, воно надає користувачам доступ до інтерфейсів додатків. Лікарі та пацієнти - це два типи користувачів у нашій системі.

У кожного користувача є своя функція. В результаті користувальницький додаток надає різні інтерфейси користувача залежно від ролі користувач. По-друге, на основі введених користувачем даних користувальницький додаток створює початкову транзакцію. З метою підтвердження транзакція відправляється в протокол рукостискання блокчейна. Нарешті, користувальницький інтерфейс встановлює зв'язок між користувачами і протоколом рукостискання блокчейна. Фундаментальним компонентом запропонованої архітектури є протокол рукостискання блокчейн (blockchain handshake - BH). Цей компонент з'єднує сервер бази даних, блокчейн-мережу і хмарну систему медичних записів, яка діє як оболонка. Запропонована архітектурна модель використовує блокчейн-мережу Ethereum. Розподілений реєстр, що з'єднує блокчейн-вузли, відома як публічна блокчейн-мережа. Блокчейн-вузли - це майнери, які відповідають за оновлення блокчейна на основі методу прийняття рішення.

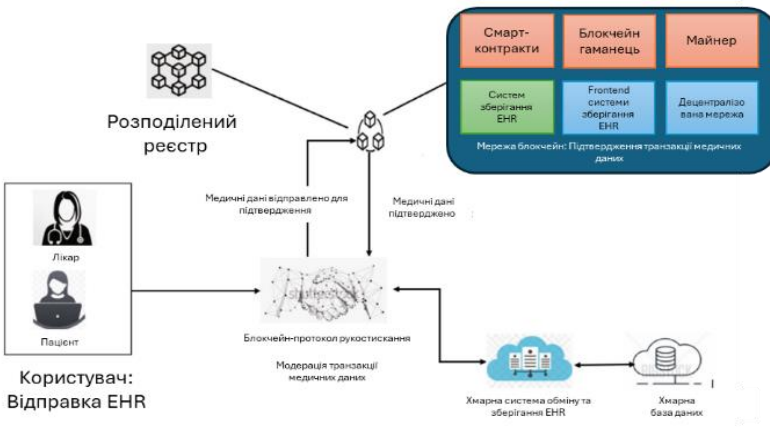


Рис. 3. Структурна схема взаємодії компонентів системи

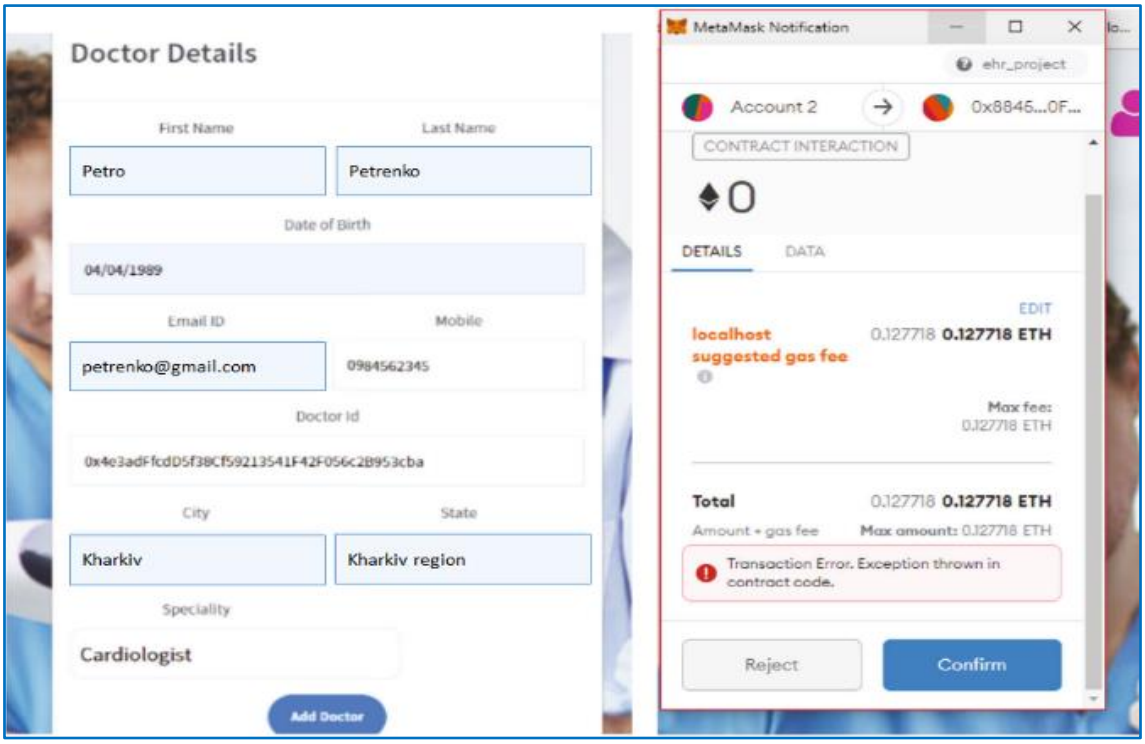
В якості альтернативи блокчейн-вузли приймають транзакції і використовують смарт-контракти мережі для їх аутентифікації.

У запропонованому проекті хмара надає дві послуги, які аналогічні тим, які надаються існуючими хмарними сервісами.

Системи адміністрування EHR. Система адміністрування EHR розміщується в якості початкової служби. Зберігання даних-це наступна послуга. Всі медичні записи можуть бути збережені в базі даних. Система адміністрування EHR приймає транзакції з протоколу рукостискання блокчейна, виконує всі обов'язки, пов'язані з ними, і, нарешті, зберігає їх в хмарній базі даних. У відповідь на запити користувачів про доступ хмара надає необхідні дані.

Розглянемо процес отримання доступу до даних в розробленій системі. Ця система побудована з використанням Truffle і Ganache, двох простих у використанні інструментів для створення локального блокчейна Ethereum. Сервер і внутрішня частина системи розроблено з використанням мови Solidity і Node.js. Для створення блокчейна і доступу до системи використовуються віртуальний інтерфейс Ethereum, MetaMask (в якості гаманця), Truffle (в якості IDE), використовуються Yarn (інтерфейс командного рядка), Ganache (створення облікового запису) та Local Web3 (веб-інтерфейс).

Додавання лікаря. На рис. 4 показаний процес додавання лікаря.



а б

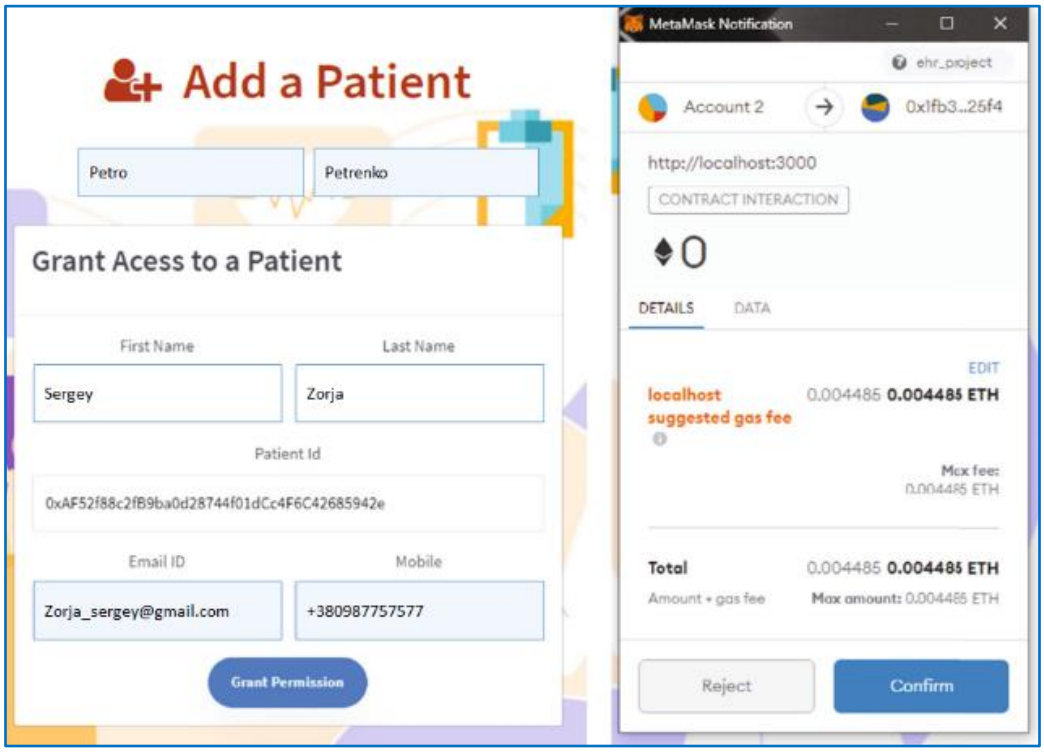
Рис. 4. Додавання даних про лікаря

На рис. 4, а показаний модуль реєстрації лікаря, де потрібно заповнити дані лікаря, такі як ім'я; дата народження; ідентифікатор електронної пошти; номер мобільного телефону; ідентифікатор лікаря, який є адресою облікового запису в Ganache Ethereum; Місто; Держава; і спеціальність. На рис. 4, б показано повідомлення про підтвердження від MetaMask, який використовується в якості смарт-контракту. За допомогою MetaMask буде збережена вся інформація про лікаря, і система отримає повідомлення з підтвердженням аутентифікації. Але, якщо користувач використовує невірну інформацію або адресу облікового запису, що вже існує, система видасть повідомлення про відмову в доступі. Нарешті, цей смарт-контракт забезпечує безпеку даних лікаря.

Додавання пацієнта. На рис. 5 описаний метод додавання пацієнт. На рис. 5, а показаний модуль реєстрації пацієнтів, що вимагає введення інформації про пацієнтів, наприклад імена, адреси електронної пошти, номери телефонів та ідентифікатори пацієнтів, які є адресою облікового запису Ganache Ethereum.

Після заповнення заповнивши всі прогалини необхідною інформацією, Користувач потрібно натиснути кнопку "Додати пацієнта", щоб зберегти дані, а потім переходити до наступного процесу. Підтверджуюче повідомлення від MetaMask, яке використовується в якості смарт-контракту, показано на рис. 5, б. Вся інформація про пацієнта буде збережена за допомогою MetaMask, і система отримає повідомлення з підтвердженням аутентифікації. Щоб зберегти всі дані, повідомлення MetaMask відображає на екрані детальний курс валюти Ethereum. Він зберігає всі дані в форматі валюти Ethereum. Система відобразить повідомлення про заборону доступу, якщо користувач введе невірну інформацію або та ж адреса облікового запису. Нарешті, безпека самого дані пацієнта захищені цим смарт-контрактом.

Рис. 6 ілюструє персональний блокчейн Ethereum, представлений Ganache.



а б

Рис. 5. Додавання даних про пацієнта

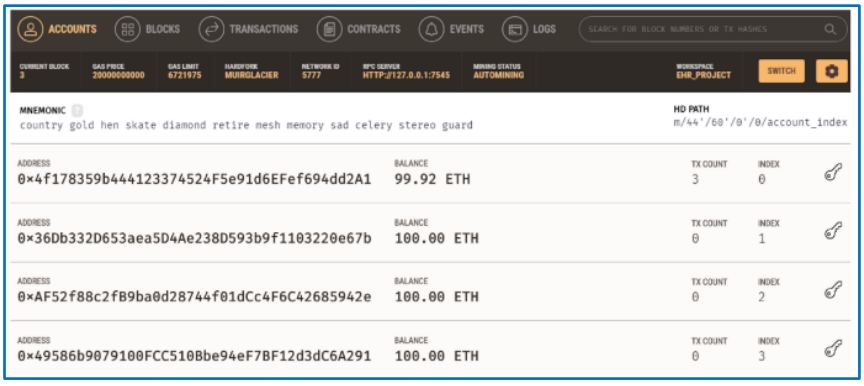


Рис. 6. Персональний блокчейн Ganache

Він був використаний для тестування і розгортання системи. Для тестування та локальної розробки Ganache пропонує кілька віртуальних облікових записів зі 100 ETH. Він забезпечує можливості, порівнянні з Ganache, при розгортанні в основній мережі Ethereum. Деякі з підроблених транзакцій виконуються віртуальними обліковими записами в додатку разом з хешами транзакцій і адресою контракту, на який вони були розгорнуті. Значення валюти кожної транзакції також відображається у стовпці.

Першим кроком на серверній частині є завантаження і установка Ganache з набору Truffle Suite.

Підключення до сервера за допомогою Смарт-контракту. На рис. 7 показано підключення системи за допомогою смарт-контрактів.

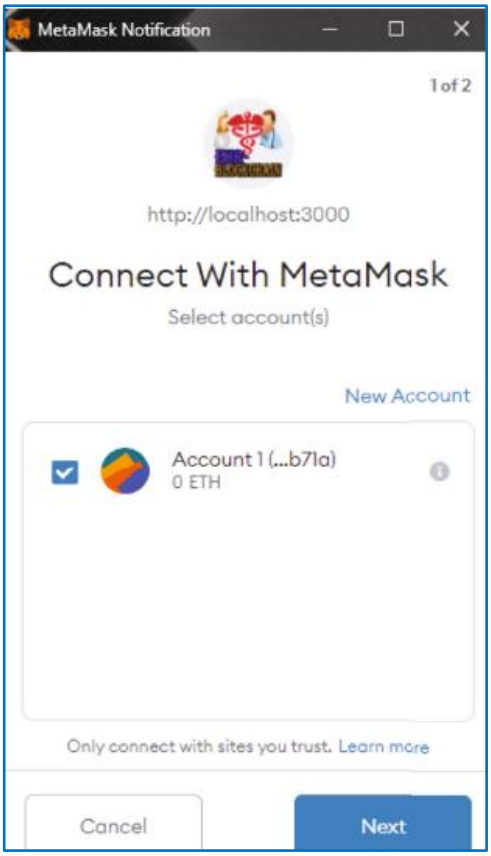
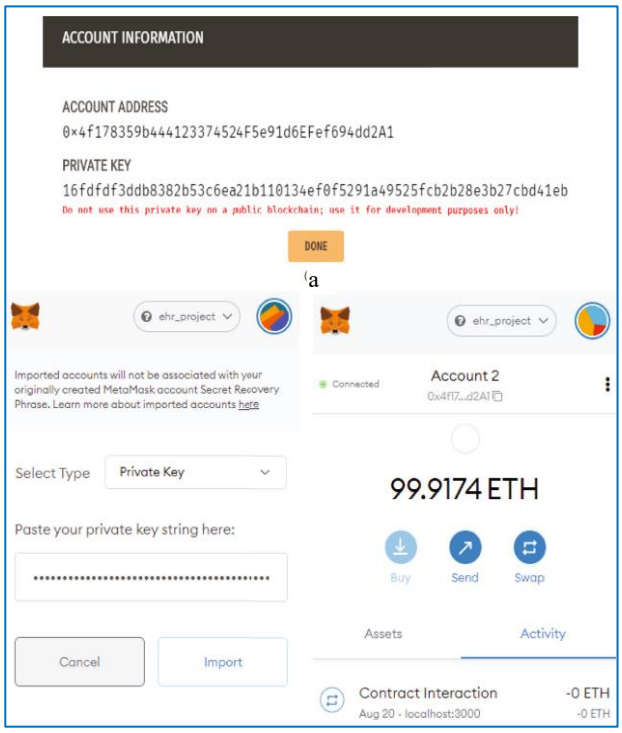


Рис. 7. Підключення до гаманця MetaMask

MetaMask використовується в якості смарт-контракту для підключення до системи. Створюються контракти, які надають метадані по назвах записів, доступі та цілісності даних. Додаються криптографічно підписані інструкції для управління цими характеристиками у блокчейн-транзакціях цієї системи. Використовуються лише операції, що забезпечують зміну даних функціональними можливостями переходу стану контракту для виконання політик. До тих пір, поки медична карта може зберігатися в електронному вигляді, ці контракти можуть бути створені для забезпечення дотримання будь-якого набору правил, що контролюють її.

Цей смарт-контракт, заснований на технології блокчейн, може бути розроблений таким чином, щоб включати в себе всі умови, такі як обробка різних дозволів та доступ до даних. Можна помітити, що в цій схемі задіяний ряд зацікавлених сторін, кожен з них виконує різні завдання. Це полегшить спілкування лікарів і пацієнтів. Смарт-контракти включають в себе правила авторизації даних. Це також може допомогти у відстеженні всіх дій, пов'язаних з унікальним ідентифікатором, від точки походження до точки відправки. Були створені усі функції і процедури, які включені в смарт-контракти. Для підвищення ефективності всі дані медичної карти зберігаються в локальній базі даних.

Створення облікового запису за допомогою Смарт-контракту. На рис. 8 показано покроковий процес створення облікового запису.



а б

Рис. 8. а – Ganache Ethereum (адреса облікового запису), б – додавання приватного ключа, с– створення облікового запису

На рис. 8, а показана інформація про обліковий запис Ganache Ethereum, який дозволяє користувачам використовувати браузер для доступу до децентралізованої системи без наявності повноцінного вузла блокчейна. На рисунку 8.b показано імпорт приватних ключів через MetaMask, який гарантує можливість реалізації контрактів. Захищений паролем Ethereum wallet - це частина програмного забезпечення, яке може використовуватися для зберігання секретних ключів і для підпису, авторизації та управління транзакціями з використанням електронних медичних карт. Секретні ключі лікаря і пацієнта будуть зберігатися в метамаск-гаманці, який може бути використаний скрізь, де потрібен дозвіл на використання закритого ключа. На рисунку 8.c показано ідентифікатор облікового запису із Ganache на гаманець Ethereum, де гаманець MetaMask потім підключиться до системи і буде функціонувати відповідно до

ehr_project. В запропонованій системі використовується блокчейн заради безпеки даних і прозорість. У цій архітектурі будь-які спроби незаконного використання заборонені. Таким чином, система вважається однією з найбезпечніших платформ порівняно з іншими платформами електронної охорони здоров'я.

Виконаємо порівняння архітектуи нашої системи з архітектурою існуючих систем охорони здоров'я. Порівняння базується на ключових характеристиках різних систем охорони здоров'я. Порівняння показано в табл. 1.

Кожна транзакція в мережі Ethereum вимагає витрат на газ. Іншими словами, газ - це свого роду готівкові гроші, які можуть бути використані для проведення будь-якої транзакції. Оскільки плата за газ в мережі Ethereum настільки висока, пропонується зберігаємо там не всі типи даних пацієнтів.

В результаті було прийнято рішення зберегти в Ethereum тільки окремі хмарні адреси, що тягне за собою невелику плату за газ.

З іншого боку, наша система є більш ефективною, ніж будь-яка інша система. Графік залежності плати за газ від розміру вхідних даних у байтах показано на рис. 9.

На цьому графіку можна наочно бачити, що при збільшенні розміру даних плата за газ автоматично збільшується. Таким чином, розмір даних, що зберігаються в блокчейн, повинен бути якомога менше.

Таблиця 1 – **Порівняльна таблиця між запропонованим методом та існуючими**

Параметри	Smart glucose monitoring system [19]	Secure her: healthblock [20]	Healthcare provisioning ecosystem [21]	Запропонована система
Дистанційне спостереження за пацієнтом	Ні	Ні	Так	Так
Дистанційне виявлення захворювань пацієнта	Ні	Ні	Ні	Ні
Використання датчиків	Так	Ні	Так	Так
Рекомендації щодо автентифікації користувача	Ні	Ні	Ні	Так
Зберігання даних в блокчейн	Так	Так	Так	Так
Використання криптографічних функцій	Ні	Так	Ні	Так

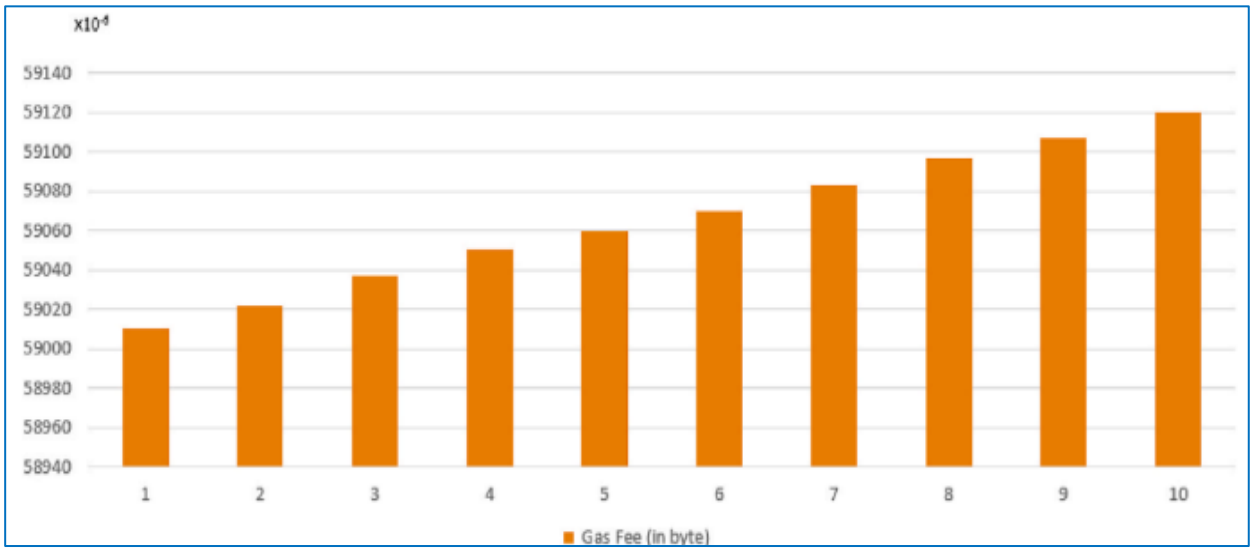


Рис. 9. Газ, який використовується під час транзакції в Ethereum

Висновки

У секторі охорони здоров'я безпека даних сьогодні набуває все більшого визнання. Отож, щоб подолати цю проблему, в роботі запропоновано використання технології блокчейн з метою забезпечення конфіденційності. Запропонована модель архітектури системи обміну медичними даними в першу чергу призначена для віддаленого догляду за пацієнтами, а також для пріоритетного захисту конфіденційних медичних записів пацієнтів. Для забезпечення безпеки даних в роботі запропоновано блокчейн на основі Ethereum, який вважається одним з найбільш ефективних методів, використовуваних для забезпечення безпеки даних. Також пропонується використання асиметричної криптографії для хешування даних, що робить транзакції більш безпечними, ніж у інших системах.

СПИСОК ЛІТЕРАТУРИ

1. Левківський, В. Л. (2023). Аналіз структури та функціональних можливостей медичних інформаційних систем україни. Вестник Херсонского национального технического университета, (3 (86)), 111-118.

2. Bedianashvili, g., Zhosan, h., & lavrenko, s. (2022). Modern digitalization trends of Georgia and Ukraine. Scientific Papers Series Management, Economic Engineering in Agriculture & Rural Development, 22(3).
3. Корчинський, І. О., & Фірман, Н. А. (2022). Цифрова медицина: особливості та проблеми становлення в Україні. Цифрова економіка та економічна безпека, (1 (01)/), 100-105.
4. Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177-183.
5. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & security, 97, 101966.
6. Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. Computer Communications, 153, 311-335.
7. Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in biology and medicine, 129, 104130.
8. Mayer, A. H., da Costa, C. A., & Righi, R. D. R. (2020). Electronic health records in a Blockchain: A systematic review. Health informatics journal, 26(2), 1273-1288.
9. Goodman, K. W. (2020). Ethics in health informatics. Yearbook of medical informatics, 29(01), 026-031.
10. Yigzaw, K. Y., Olabarriaga, S. D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., ... & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. Roadmap to Successful Digital Health Ecosystems, 335-362.
11. Ismail, L., Materwala, H., & Sharaf, Y. (2020, October). Blockhr–a blockchain-based healthcare records management framework: performance evaluation and comparison with client/server architecture. In 2020 International symposium on networks, computers and communications (ISNCC) (pp. 1-8). IEEE.
12. Li, W., Wang, S., Xie, W., Yu, K., & Feng, C. (2023). Large scale medical image online three-dimensional reconstruction based on WebGL using four tier client server architecture. Information Visualization, 22(2), 100-114.
13. Xu, L., Xu, C., Liu, J. K., Zuo, C., & Zhang, P. (2020). Building a dynamic searchable encrypted medical database for multi-client. Information Sciences, 527, 394-405.
14. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. IEEE Internet of Things Journal, 8(7), 5914-5925.
15. Seth, B., Dalal, S., Jaglan, V., Le, D. N., Mohan, S., & Srivastava, G. (2022). Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies, 33(4), e4108.
16. Guo, H., Li, W., Nejad, M., & Shen, C. C. (2022). A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. IEEE Transactions on Network and Service Management.
17. Golubnychy, D., Kolomiytsev, O., Tretyak, V., Kliuchka, Y., & Rybalchenko, A. (2022). Архітектура системи обміну медичними даними пацієнтів з лікарями на основі IOTA. Системи управління, навігації та зв'язку. Збірник наукових праць, 1(67), 57-61.
18. Ключка, Я. О., Шматко, О. В., Євсеєв, С. П., & Милевський, С. В. (2021). Peculiarities of blockchain technology introduction in the field of healthcare: current situation and prospects. Системи обробки інформації, (1 (164)), 33-44.
19. Rghioui, A., Lloret, J., Harane, M., & Oumnad, A. (2020). A smart glucose monitoring system for diabetic patient. Electronics, 9(4), 678.
20. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500.
21. Khang, A., Hahanov, V., Litvinova, E., Chumachenko, S., Hajimahmud, A. V., Ali, R. N., ... & Anh, P. T. N. (2023). The Analytics of Hospitality of Hospitals in a Healthcare Ecosystem. In Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem (pp. 39-61). CRC Press.

Received (Надійшла) 11.02.2024
Accepted for publication (Прийнята до друку) 17.04.2024

Model of decentralized electric medical card exchange system based on blockchain technology

O. Shmatko, S. Salnikov

Abstract. Topicality.. In today's digital age, data security is becoming a primary concern in various sectors, especially in healthcare.the critical nature of patient data requires robust protection mechanisms against unauthorized access and potential malicious use. This article examines the changing data security landscape in the healthcare sector and highlights vulnerabilities associated with traditional data storage systems. The paper proposes a model of a system for collecting, storing and exchanging electronic health records (EHR). The paper examines blockchain technology as a revolutionary approach to solving security problems for the exchange of confidential medical data. **The goal of this work** is to increase the confidentiality of medical data, its integrity and availability, as well as to ensure reliable exchange of this data between medical institutions and other participants by designing and developing software components for creating secure systems for transmitting medical information based on blockchain technology.. **The object of research** includes systems for the transmission of medical information, which ensure the exchange of data between medical institutions, specialists and specialists, ensuring the confidentiality, integrity and availability of this data.. **The subject of research** is methods and tools for designing and developing software components necessary for creating and maintaining secure medical information transmission systems. These components include software for encryption, authentication, authorization, and mechanisms for fault tolerance and data recovery. **Results.** In this paper, we propose a model of a decentralized system for collecting, storing, and exchanging EHR**. Conclusions.** The results of this study highlight the transformative potential of blockchain technology in rethinking data security paradigms in the healthcare sector. by creating a secure, transparent and efficient platform for managing EHR, the proposed model not only increases the confidentiality and integrity of medical data, but also makes a significant contribution to improving the quality of care and patient outcomes. As we move forward, the introduction of decentralized systems based on blockchain technology in healthcare represents a promising path to address complex challenges related to data security and Privacy, thereby paving the way for a more sustainable and patient-centered healthcare ecosystem.

Keywords: blockchain, electronic medical cards, smart contracts, Ethereum, MetaMask, architectural technology.