УДК 658.512.2.011.56:612.846

ПРОЕКТУВАННЯ BLOCKCHAIN-СЕРВІСУ ДЛЯ МЕДИЧНОГО ОБСЛУГОВУВАННЯ

Комлева О. О.
к.т.н., доцент каф. СПЗ Комлева Н.О.
Одеський Національний Політехнічний Університет, УКРАЇНА

АНОТАЦІЯ. Розглянуті питання, пов'язані з проектуванням сервісу, заснованому на технології blockchain, який дозволить зробити процес медичного обслуговування зручним, прозорим і захищеним від фальсифікації завдяки децентралізованому доступу к даним і специфічним засобам и методам захисту інформації.

Вступ. Blockchain – це технологія, яка дозволяє здійснювати довірчий обмін цінними ресурсами в мережі без посередників. Ключовими характеристиками blockchain є: постійна доступність, сильна цілісність даних, відсутність центральної точки контролю та громадська відповідальність в масштабах всієї мережі [1]. Одним з поширених засобів захисту у технології blockchain є електронний цифровий підпис (ЕЦП), який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

Мета роботи. Метою роботи є підвищення якості проведення медичного обслуговування за рахунок впровадження технології blockchain та відповідних криптографічних алгоритмів. Суб'єктами цього процесу виступають громадяни та медичні заклади.

Основна частина роботи. Розроблюваний сервіс має бути інструментом, що забезпечує можливість швидко та безпечно отримати медичні дані клієнта, дізнатися про умови в медичній установі та усю необхідну інформацію, які можуть надати дві сторони: клієнт (пацієнт) та медичні заклади різної клініко-інструментальної спрямованості. Ці дані можуть бути використані далі для співпраці між усіма сторонами. Найближчим аналогом розроблюваної системи є Etherisc Social Insurance – це децентралізований додаток, що демонструє модель соціального забезпечення, що реалізується на Ethereum blockchain. Модель є легкою, високоефективною та забезпечує основне охоплення таких подій, як важкі захворювання.

Сервіс поділяється на такі компоненти: клієнтська частина для медичної установи, клієнтська частина для пацієнта. Для програмної реалізації даної розробки було обрано операційну систему Linux, мови програмування JavaScript (Web3.js) and Python, Solidity (Ethereum), систему управління базою даних – MongoDB (NoSQL, використовує JSON). Такі мови та технології були обрані для зручної та легкої взаємодії з Ethereum – blockchain платформою для створення розподілених децентралізованих додатків, що забезпечує надійність, універсальність, можливість створення зручного і сучасного інтерфейсу програми, застосування сучасних методів і алгоритмів програмування [2].

Заголовок блоку включає в себе свій хеш, хеш попереднього блоку, хеші транзакцій і додаткову службову інформацію. Хеш блоку транзакцій являє собою випадкову послідовність цифр і букв і є гарантією того, що якщо в блоці даних зміниться хоча б один біт, кожен вузол швидко зможе дізнатися про спробу фальсифікації історії транзакцій. Блокчейн традиційно використовує алгоритм шифрування SHA-256. Створений блок буде прийнятий іншими учасниками мережі, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується. Так як результат хешування (функції SHA-256) є незворотним, алгоритму отримання бажаного результату не існує – ця операція виконується випадковим перебором. Коли варіант знайдений, вузол розсилає отриманий блок іншим підключеним вузлам, які перевіряють його. Якщо помилок немає, то блок вважається доданим в ланцюжок, а наступний блок включає в свій заголовок його хеш.

На рисунку 1 у наглядному вигляді представлена діаграма компонентів екосистеми Ethereum, на якій показано взаємодію між клієнтською частиною, децентралізованим додатком, Ethereum вузлами та системами контролю версій. Smart Contract можна зчитати або записати за

допомогою JSON/RPC, з яким взаємодіє пакет Web3.js. Децентралізований додаток включає в себе фронт-енд, що реалізований за допомогою HTML, CSS & JavaScript, смарт-контракт описується розробниками. Ethereum вузли розповсюджені на світовому “Інтернеті” – Ethereum World Computer – так називають мережу blockchain, що знаходиться на платформі Ethereum. Для реалізації схем ЕЦП використовують еліптичні криві, що описуються рівнянням Вейерштрассе та не є сингулярними, бо це значно знижує стійкість обраної схеми [3].

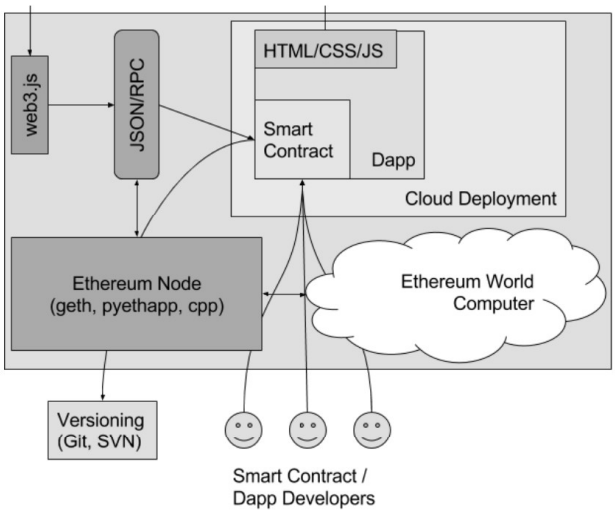

Рис. 1 – Діаграма компонентної взаємодії сервісу та Ethereum

На рисунку 2 показана взаємодія користувача з середовищем розробки відповідних смарт-контрактів, реалізовано запити щодо написання, обробки та компіляції контракту на стороні середовища, а також дії щодо транзакцій.

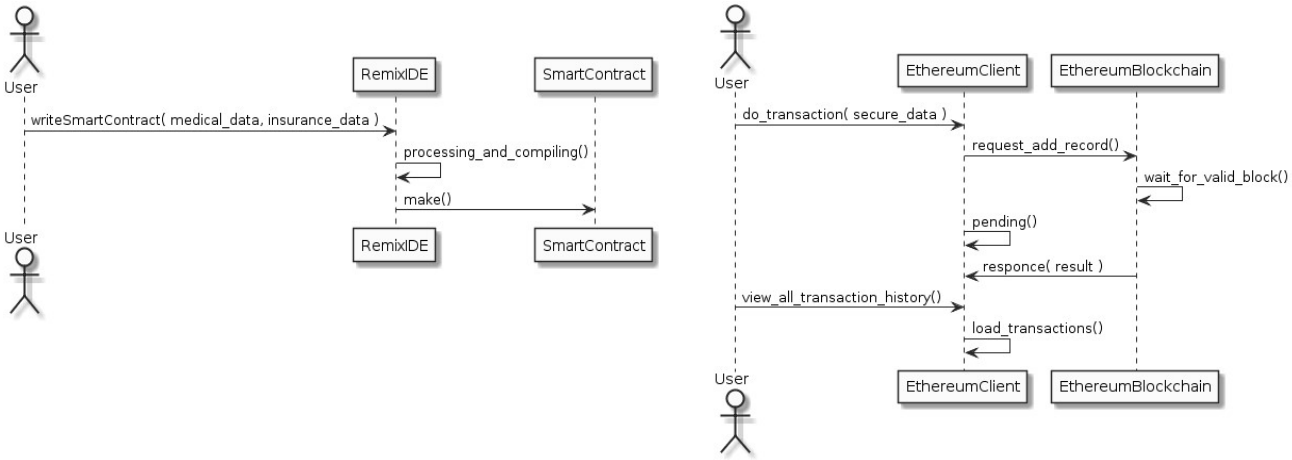

Рис.2 – Діаграми послідовностей для написання контракту та для роботи з транзакціями

Висновки. Переваги розглянутого blockchain-сервісу дозволяють зробити висновок про безсумнівну доцільність його застосування для підвищення якості проведення медичного обслуговування. Завдяки йому можливо відстежити усі медичні дані клієнта та зменшити ймовірність шахрайства та втрати конфіденційності даних з використанням контрольного журналу транзакцій. Цьому же сприяє і децентралізований спосіб зберігання медичних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Что такое Blockchain (блокчейн)? Технология, платформа, транзакции. / [Електронний ресурс]. – Режим доступу: https://mining-cryptocurrency.ru/blockchain/#i-7

2. Чернега К.С., Комлевая Н.О. Применение технологии blockchain для повышения защищенности процесса проведения медицинского страхования. – Штучний інтелект. – Київ, 2017. – № 3-4. – С. 197 – 202.

3. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.