

УДК 004.652

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ КОНТРОЛЮ ОБІГУ МЕДИЧНИХ ПРЕПАРАТІВ НА БАЗІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Марченко Ігор, Петров Сергій

Сумський державний університет

Анотація

Метою даної роботи є усунення головного недоліку існуючих методів контролю обігу медичних препаратів, а саме неможливості забезпечення цілісності даних та ризик порушення лікарської таємниці. В роботі запропоновано інформаційний підхід, що базується на технології блокчейн та має перевагу над існуючими методами, які використовують централізовані або розподілені сховища даних. Розроблено смарт-контракт на базі реалізації блокчейну Ethereum, який позбавлений таких недоліків як реплікація даних та можливості компрометації даних при їх передачі.

Abstract

The purpose of this research work is address the weaknesses in existing systems, such as data integrity and observing medical confidentiality in order to control prescription medicine. This research provides blockchain-based approach for storing and managing user data. This technology is better than using centralized and/or distributed databases. Prescription medicine flow was fully implemented in terms of blockchain technology as Ethereum smart-contract.

Медична галузь гостро потребує розробку та впровадження та посилення контролю обігу медичних препаратів. На даний момент для інформатизації процесів взаємодії лікаря та пацієнта в Україні запроваджується система eHealth [1], що являє собою агрегацію декількох систем менеджменту інформаційних операцій пацієнтів, між якими, на даний момент, відсутній експорт даних. Одним з недоліків системи eHealth те, що кожна лікарня власноруч обирає систему менеджменту, котрою вона буде користуватися. При зміні місця проживання, а, відповідно, і лікарні неможливо мігрувати дані пацієнта. Таким чином ми не маємо можливості контролювати ситуацію в цілому. Іншим важливим аспектом – є обов'язкова наявність персонального комп'ютера для роботи даних систем.

Законодавчо в Україні робота даних систем регулюється постановою КМУ: «Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям», що делегує відповідальність за зберігання та цілісність інформації на компанію, що надає програмне забезпечення. Таким чином, з точки зору правового аспекту всі наведені вище системи мають ключовий недолік: у випадку компрометації доступу до бази даних, права пацієнта про нерозголошення особистої інформації та лікарську таємницю будуть порушені [2], що посилює відповідальність власників системи щодо забезпечення цілісності даних.

Серед запропонованих систем функціонал електронних рецептів знаходиться лише на стадії концепту. А для її роботи необхідна наявність персонального комп'ютеру в аптеці, та підключення її до тієї ж системи, в якій видано рецепт.

Концепція електронних рецептів є класичним підходом, що ґрунтується на простому прийомі – оцифровці існуючих інформаційних потоків, але враховуючи високу залежність людства від безпеки персональних даних вимагає використовувати принципово нові підходи в тому числі і перегляду існуючих потоків даних та процесів їх обробки. Суттєві зміни європейського законодавства що поводитьися радою європейського парламенту GDPR вже з травня 2018 року вимагає обов'язкового шифрування всіх персональних даних, вважаємо що конкретна вимога щодо

гарантування цілісності буде наступною. Забезпечити останнє може така технологія як блокчейн [3].

Зазначимо, що класичні паперові рецепти не забезпечують достатньої надійності та цілісності даних. Наступним кроком у розвитку підходів до зберігання даних є використання баз даних, які за ступенем розподіленості розділяють на централізовані та розподілені [4]. Головним недоліком централізованих баз даних є низька ступінь відмовостійкості, розподілені бази даних позбавлені цього недоліку. При цьому всі види класичних баз даних не можуть забезпечити достатню ступінь цілісності даних. Так, наприклад, на випадок технічного збою необхідно створювати резервні копії даних. Розвитком розподілених баз даних є технологія блокчейн, що в простому розумінні, представляє собою репліковану розподілену базу даних, записи в якій неможливо змінити. Домінуючою сферою використання блокчейну на даний час є зберігання транзакцій криптовалют.

На даний момент існує велика кількість проєктів на базі блокчейну, що не пов'язані з криптовалютами:

- авторизація за допомогою блокчейну
- зберігання файлів
- документообіг
- авторство та право володіння цифровим об'єктом
- продаж коштовностей
- голосування
- онлайн ігри

Всі ці проєкти з'явилися в зв'язку з необхідністю мати незалежну та надійну базу даних. При цьому відмова одного з вузлів, на якому зберігаються дані жодним чином не впливає на роботу системи в цілому.

На даний момент існує два найбільших публічних блокчейни, доступних для використання: Bitcoin та Ethereum. Головною відмінністю між ними є можливість виконувати смарт-контракти у блокчейні Ethereum [5]. Базовим елементом блокчейну є вузол з унікальною адресою. Операція зміни стану блокчейну називається – транзакція. Всі транзакції безпосередньо зберігаються в блокчейні. Зазначимо, що недоліком публічних блокчейнів є плата за транзакції, а саме - за збереження інформації та відносно низька швидкість їх виконання.

Кожен вузол може представляти собою клієнта системи, або інтерфейс що реалізує логіку взаємодії між вузлами – смарт-контракт. Якщо транзакція направлена на адресу за якою розташовано смарт-контракт будуть виконані його методи. Приклад смарт контракту наведено нижче.

```
pragma solidity ^0.4.0;
```

```
contract TestContract {
    address owner;

    function TestContract() public {
        owner = msg.sender;
    }

    function getOwner() public constant returns (address) {
        return owner;
    }
}
```

За своєю структурою смарт-контракт нагадує звичайний об'єктно-орієнтований клас з його полями, методами та модифікаторами доступу. Відмінність полягає у тому, що в

блокчейні існують операції, котрі не змінюють його внутрішній стан, а тому і не потребують оплати. Такі операції повинні бути позначені модифікатором constant. Контракт при створенні зберігає адресу клієнта, що його завантажив в блокчейн, а тому є його власником, а за допомогою методу getOwner() повертає це значення.

Розглянемо можливість використання блокчейну для реалізації системи контролю обігу медичних препаратів. Під транзакцією в термінах нашої системи будемо розуміти будь-яку взаємодію між клієнтом та блокчейном.

Використання публічного блокчейну доцільно оскільки це забезпечую децентралізацію даних та їх цілісність, при цьому необхідно мінімізувати кількість операцій, які змінюють внутрішній стан блокчейну оскільки вони потребують оплати.

Блокчейн накладає певні обмеження на зберігання даних [6], тому в ньому є сенс зберігати лише ті дані зміна яких небажана:

- факт оформлення рецепту у лікаря;
- факт видачі ліків аптекарем.

Лікар генерує транзакцію що заносить в блокчейн інформацію про те, кому і що саме він виписав. Дані транзакції неможливо сфальсифікувати, а тому при покупці медикаментів аптекар може бути впевненим в тому, що йому представлено рецепт в такому вигляді, як його виписав лікар.

Для кожного рецепту будемо зберігати адресу клієнту, якому він виданий та скільки разів можливо придбати ліки з цього рецепту. При кожному придбанні, аптекар авторизується у системі та шляхом зчитування qr-коду з екрану мобільного пристрою, за допомогою одноразового паролю, або за допомогою NFC зменшує цю кількість на одиницю. Факт цього придбання зберігається в блокчейні у вигляді транзакції.

Завдяки цьому кожен рецепт пройде ланцюг від виписки його лікарем до видачі в аптеці, що відкидає ймовірність підробки документів на видачу ліків. Окрім того, при виявленні факту неправомірних дій будь-якої сторони можливо відстежити шлях та осіб, які були при цьому задіяні.

Враховуючи всі приведені вище переваги блокчейну над класичними способами зберігання даних було вирішено використовувати реалізацію, що базується саме на ньому. Така реалізація має наступні переваги: відмовостійкість та цілісність даних. Серед недоліків даної системи виділимо низьку швидкість транзакцій в блокчейні, яка не впливає на роботу додатку.

Список використаних джерел:

1. Головна | Офіційний сайт електронної системи охорони здоров'я eHealth [Electronic resource]. URL: <https://portal.ehealth-ukraine.org/> (accessed: 01.03.2018).
2. Про затвердження Порядку надання... | від 11.10.2002 № 1519 [Electronic resource]. URL: <http://zakon0.rada.gov.ua/laws/show/1519-2002-п> (accessed: 01.03.2018).
3. Satoshi Nakamoto, Kornmesser S., Satoshi Nakamoto. Bitcoin // [Www.Bitcoin.Org](http://www.Bitcoin.Org). 2008.
4. Date C.J. An Introduction to Database Systems // An Introd. to Database Syst. 1995.
5. Wood G. Ethereum: a secure decentralised generalised transaction ledger // Ethereum Proj. Yellow Pap. 2014. P. 1–32.
6. Types — Solidity 0.4.21 documentation [Electronic resource]. URL: <http://solidity.readthedocs.io/en/develop/types.html> (accessed: 06.03.2018).