УДК 004.056.5

Ю. В. Баришев
В. С. Ланова

СМАРТ-КОНТРАКТИ ДЛЯ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ МЕДИЧНИХ ДАНИХ

Вінницький національний технічний університет;

Анотація
Виконано аналіз доцільності використання блокчейну в сфері медицини. Проаналізовано практики його застосування. Запропоновано структуру базових смарт-контрактів для розподіленого зберігання медичних даних, задля уникнення підробки та порушенню медичної таємниці. Визначено перспективи подальшого дослідження.
Ключові слова: блокчейн, смарт-контракти, бази даних, безпека медичних даних, сімейні лікарі.

Abstract
The blockchain implementation application analyses for the medicine field were performed. The common practices of its usage were analyzed. The structure of the basic smart contracts for distributed storage of medical data was proposed to avoid fraud and violation of the medical privacy. The perspectives of the further research were determined.
Keywords: blockchain, smart contracts, databases, medical data security, family doctors.

Вступ

Існують різноманітні тенденції та практики, запропоновані для моніторингу та ведення записів пацієнтів, а також надання відповідей усім установам у певний період [1]. Саме тому для забезпечення захисту медичних даних необхідно використовувати сучасні технології, зокрема і блокчейн. Він допомагає зберегти дані та забезпечує їх незмінність [2]. Але для впровадження блокчейну в електронний документообіг медичних установ, необхідно розробити смарт-контракти на основі яких відбуватиметься структурування та зберігання цих даних. В межах даного дослідження, як такі медичні дані було обрано відомості з практики сімейних лікарів.

Переваги технології блокчейн сприяли його впровадженню в різних країнах. Так, в Європі добре себе зарекомендував естонський проект e-health загального реєстру даних пацієнтів, запущений в 2016 році [3]. У Британії два роки тому стартував блокчейн-проект безпечного зберігання особистих даних пацієнтів Medicalchain [3]. Однак, дані системи не адаптовані до форм документів прийнятих в Україні, тому актуально розробити смарт-контракти, які враховують цю специфіку.

Метою буде покращення безпеки медичних даних, шляхом розробки смарт-контрактів. Для того, аби успішно досягти поставленої мети, необхідно розв’язати такі задачі: проаналізувати предметну область діяльності сімейних лікарів, розробити смарт-контракти на основі мови Solidity.

Результати дослідження

Кожна людина хоче, щоб її дані були захищеними та конфіденційними. Особливої уваги заслуговує сфера охорони здоров’я, куди звернувшись за медичною допомогою чи консультацією, людина переслідує мету не тільки отримання кваліфікованих послуг, а й захисту відповідної інформації про неї [4]. Відповідно до ст. 39-1 Основ законодавства України про охорону здоров’я «на таємницю про стан свого здоров’я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні», дані повинні бути захищеними, цілісними та конфіденційними [5].

Аналіз предметної області показав, що в практиці сімейної медицини зустрічаються такі типи відомостей:

- Історія хвороби;
- Медична карта пацієнта;

- Направлення на обстеження;
- Дані про обстеження;
- Призначення лікування;
- Видача рецепту;
- Карта щеплень.

В даному дослідженні будуть розглянуті лише медична карта пацієнта, направлення на обстеження та історія хвороби. В подальших дослідженнях планується розглянути всі інші вищезгадані відомості. Для початку слід створити смарт-контракт з історією хвороби пацієнта, який породжує медичну карту пацієнта та направлення на обстеження. Слід проаналізувати дані, які варто додавати в блокчейн, а які слід залишити конфіденційними. Контракти будуть взаємодіяти між собою, тобто referralForExamination буде пов'язаним з medicalCard та становитиме частину medicalHistory. Приклад написання коду зображено на рис. 1.

```
pragma solidity ^0.8.0;

contract medicalHistory {
    uint entryRecordsNumber;
    string[] records;
    address patient;
}
contract referralForExamination {
    string specialist;
    uint id_of_the_referral;
    string previous_diagnosis;
}
contract medicalCard {
    uint id_of_the_patient;
    uint age;
    string[] cognenital_defects;
}
```

Рис. 1. Приклад створення перших смарт-контрактів

Для зберігання медичних записів за адресою смарт-контракту пацієнта, слід зазначити mapping, куди буде передаватись історія хвороби, медична карта та інформація про направлення. Також слід передбачити блокування контракту, якщо сталось так, що пацієнт помер, щоб нові дані в направлення неможливо було додавати. Як видно з рисунку 1, ці смарт-контракти мають члени-дані, але не мають методів, тому пропонується розробити такі методи для medicalHistory:

- getPatientAddress;
- getRecords;
- addRecord.

Для прикладу, на рис.2 показано додавання методу addRecord до масиву даних, який містить записи.

```
function addRecord(string r) {
    records.push(r);
    entryRecordsNumber++;
    return records;
}
```

Рис. 2. Приклад реалізації методу додавання даних до смарт-контракту

Аналогічним чином можна додати методи до інших смарт-контрактів, використовуючи схожі функції, в яких додаються елементи в масив. Надано перевагу Ethereum-подібним засобам розробки.

Розробку смарт-контрактів виконано в онлайн-компіляторі Remix.

Висновки

Таким чином було проаналізовано сферу, в якій працюють лікарі, дані, з якими працює сімейний лікар. Проаналізовано відомості, які доцільно записати в блокчейн, який є загальнодоступним середовищем зберігання даних. Цей аналіз показав, що частину відомостей варто залишити конфіденційними. Таким чином, в подальшому необхідно буде реалізувати гібридну структуру даних задля зберігання такого роду відомостей. Виконано початкову розробку смарт-контрактів, які породжують проаналізовані вище дані. Визначено найкращі для виконання поставленої задачі засоби розробки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ashfaq, M.; Manzoor, A.; Ali, L.; Sheikh, K.A. Quality of Service as a Predictor of Customer Satisfaction in Healthcare Sector. *IBT J. Bus. Stud.* 2020, *16*, 71–87.
2. S. Kushch, Y. Baryshev, S. Ranise. Blockchain Tree as Solution for Distributed Storage of Personal ID Data and Document Access Control. *Sensors* 2020, 20(13), 3621. 17 p. URL: https://www.mdpi.com/1424-8220/20/13/3621 (accessed 07.03.2023).
3. Блокчейн технології в медицині: плюси і як впровадити в Україні. Нові лідери URL: https://novilidery.com/news/blokcheyn-tekhnologii-v-medicini-plyusi-i-yak-vprovaditi-v-ukraini (дата звернення: 07.03.2023)
4. Ямненко Т. М., Літвінова І. Ф. Захист персональних даних у сфері охорони здоров'я (Кримінально-правові аспекти). *Юридичний вісник. Повітряне і космічне право*. 2019. № 1. С. 185-191.
5. Закон України «Основи законодавства про охорону здоров'я» № 2801- XII чинний від 19.11.1992 р. редакція від 27.10.2022. URL: http://zakon.rada.gov.ua/laws/show/2801-12. (дата звернення: 07.03.2023).

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Ланова Владислава Сергіївна — студентка групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: lanovaia02y@gmail.com

Yurii Baryshev —PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua.

Vladyslava Lanova — student of 1БС-20б group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : lanovaia02y@gmail.com.