

ПРИМЕНЕНИЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ МЕДИЦИНСКИХ ДАННЫХ

М.В. Логвинович, С.А. Мигалевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Блокчейн-технологии обладают большим потенциалом в сфере здравоохранения, обеспечивая децентрализованное и безопасное хранение медицинских данных. Традиционные централизованные системы часто сталкиваются с проблемами утечек и несанкционированного доступа, что делает блокчейн перспективным решением. В статье рассматривается интеграция блокчейна с IPFS для хранения медицинских записей и применение модели управления доступом на основе атрибутов (ABAC). Предложенный подход позволяет повысить безопасность, прозрачность и эффективность обмена медицинской информацией между учреждениями.

Ключевые слова: блокчейн; здравоохранение; медицинские данные; безопасность; децентрализованное хранение; IPFS; атрибутивное управление доступом; защита конфиденциальности; прозрачность; обмен данными.

APPLICATION OF BLOCKCHAIN TO ENSURING PRIVACY AND SECURITY OF MEDICAL DATA

M.V. Logvinovich, S.A. Migalevich

*Educational Institution "Belarusian State University of Informatics and Radioelectronics",
Minsk, Belarus*

Abstract. Blockchain technology has great potential in the healthcare sector, providing decentralized and secure storage of medical data. Traditional centralized systems often face issues of data breaches and unauthorized access, making blockchain a promising solution. This paper discusses the integration of blockchain with IPFS for medical record storage and the application of Attribute-Based Access Control (ABAC). The proposed approach enhances security, transparency, and the efficiency of medical data exchange between institutions.

Keywords: blockchain; healthcare; medical data; security; decentralized storage; IPFS; attribute-based access control; privacy protection; transparency; data exchange.

Введение

С развитием технологий блокчейн находит все большее применение в сфере здравоохранения, обеспечивая децентрализованное и безопасное хранение медицинских данных. Централизованные системы хранения подвержены угрозам утечек и нарушений конфиденциальности, что требует перехода к более безопасным и эффективным методам. Блокчейн, благодаря своей дистрибутивной структуре, обеспечивает неизменность данных и их защиту от подделки. Интеграция смарт-контрактов и моделей доступа на основе атрибутов (ABAC) позволяет не только повысить безопасность, но и внедрить точный контроль доступа к медицинской информации. Это позволяет эффективно управлять данными, минимизируя риски и улучшая качество обслуживания пациентов [1].

Основная часть

В условиях быстрорастущего объема медицинской информации и возрастающих угроз кибербезопасности, переход к более защищенным и эффективным методам хранения данных становится необходимостью. Блокчейн представляет собой решение, позволяющее изменить существующую модель управления медицинской информацией.

Блокчейн можно рассматривать как защищенный цифровой реестр, в котором информация хранится в виде цепочки блоков. Каждый новый блок содержит хеш предыдущего, что делает невозможным изменение уже записанных данных без согласия всех участников сети. Это свойство обеспечивает высокий уровень защиты от несанкционированного доступа. В отличие от централизованных систем, блокчейн не зависит от единой точки отказа, так как информация распределяется между множеством узлов в сети.

Ключевым аспектом использования блокчейна в сфере здравоохранения является его способность гарантировать безопасность и конфиденциальность медицинских данных. Совмещение блокчейна с межплатформенными решениями, такими как IPFS (InterPlanetary File System), позволяет надежно хранить медицинские записи в распределенном виде, а их хеши записывать в блокчейн для предотвращения фальсификации. Для контроля доступа может применяться модель управления доступом на основе атрибутов, которая позволяет гибко регулировать права пользователей в зависимости от их роли (пациент, врач, администратор и т. д.).

На рис. 1 показана возможная архитектура системы хранения и управления медицинскими данными с применением блокчейна:

Схема иллюстрирует процесс управления медицинскими данными с использованием блокчейн-технологий. Пользователи (пациенты, врачи, администраторы) получают доступ к информации через модель ABAC, которая определяет их права. Медицинские записи хранятся в распределенной файловой системе IPFS, а их неизменяемые хеши фиксируются в блокчейне с помощью API. Это гарантирует целостность данных и защищает их от подделки.

Одним из значимых преимуществ блокчейна в здравоохранении является его прозрачность. Каждый доступ к медицинским данным может фиксироваться в блокчейне, что позволяет создавать полную историю их изменений. Это особенно важно для аудита и отслеживания возможных манипуляций с медицинской информацией. Такой подход способствует предотвращению мошенничества и улучшению взаимодействия между различными медицинскими учреждениями.

Кроме того, использование блокчейна может повысить эффективность обмена медицинскими данными между больницами, лабораториями и частными клиниками.

Децентрализованная сеть позволяет создать единую защищенную платформу для обмена медицинскими данными, обеспечивая их доступность и целостность без риска утечек.

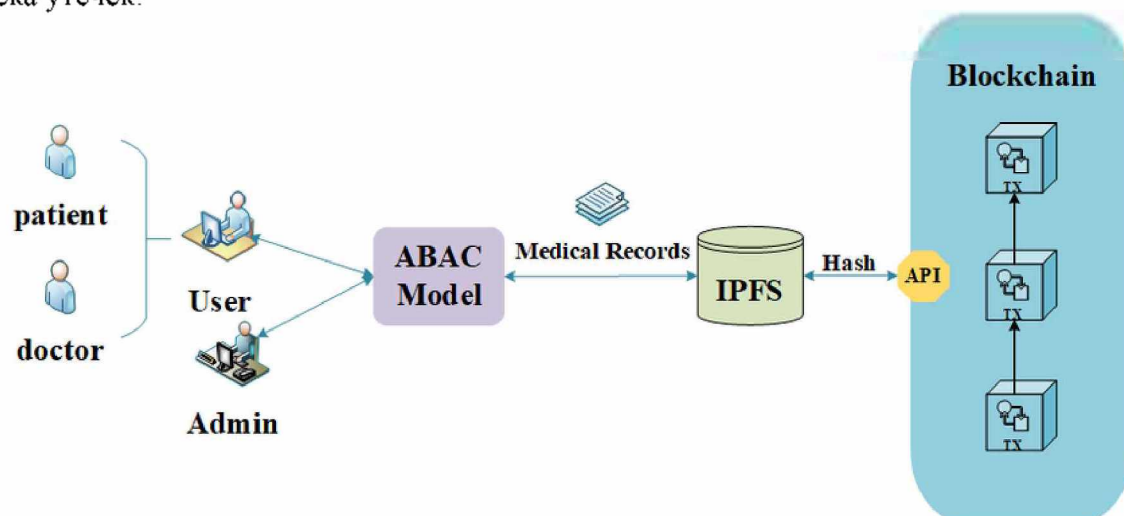


Рис. 1. Интеграция блокчейна и IPFS для хранения медицинских данных
Fig 1. Integration of Blockchain and IPFS for Storing Medical Data

Заключение

Блокчейн представляет собой перспективное решение для повышения безопасности и конфиденциальности медицинских данных. Его децентрализованная природа, в сочетании с криптографическими механизмами и моделями управления доступом, обеспечивает высокий уровень защиты информации. Интеграция с IPFS и моделями управления доступом позволяет создать надежную инфраструктуру для хранения и обработки медицинских записей. Внедрение таких решений в медицинские системы поможет минимизировать риски утечек данных, улучшить контроль доступа и повысить доверие пациентов к цифровым технологиям в здравоохранении.

Список использованных источников / References

1. Sun Z., Han D., Li D., Wang X., Chang C.-C., Wu Z. (2022) A Blockchain-based Secure Storage Scheme for Medical Information. EURASIP Journal on Wireless Communications and Networking, 40 (2022).

Сведения об авторах

Мигалевич С.А., магистр технических наук, старший преподаватель кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», migalevich@bsuir.by.
Логвинович М.В., студент 4 курса факультета компьютерных систем и сетей, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», maxiqastflower21@gmail.com.

Information about the authors

Migalevich S., Master of Technical Sciences. Senior Lecturer at the Department of Computer Science, Educational Institution "Belarusian State University of Informatics and Radioelectronics", migalevich@bsuir.by.
Logvinovich M., fourth-year student of the Faculty of Computer Systems and Networks, Educational Institution "Belarusian State University of Informatics and Radioelectronics", maxiqastflower21@gmail.com.