УДК 004.75

БЛОКЧЕЙН ДЛЯ МЕДИЦИНЫ: НОВАЯ МОДЕЛЬ ХРАНЕНИЯ И УПРАВЛЕНИЯ МЕДИЦИНСКИМИ ДАННЫМИ

Лаврова А.К. (ИТМО)

Научный руководитель - доктор экономических наук Максимова Т.Г. (ИТМО)

Введение. Современные медицинские информационные системы сталкиваются с проблемами конфиденциальности, безопасности и эффективности хранения данных. Одной из ключевых трудностей является фрагментированность информации, что затрудняет консолидацию и увеличивает затраты на администрирование. Централизованные хранилища подвержены риску несанкционированного доступа и утечек, что делает необходимым поиск новых моделей хранения.

Блокчейн-технологии обеспечивают децентрализованное и неизменяемое хранение медицинской информации, однако стандартные решения на основе Ethereum Virtual Machine (EVM) не подходят для медицины из-за открытого доступа, высокой стоимости транзакций и ограниченной масштабируемости. В исследовании рассмотрены методы оптимизации приватного блокчейна для медицины, включая соответствие законодательным нормам, увеличение скорости транзакций, усиление безопасности и устранение экономических барьеров.

Основная часть. Медицинские информационные системы должны соответствовать строгим законодательным требованиям, включая Федеральный закон №152-ФЗ [1] и международные стандарты Clinical Document Architecture (HL7 CDA) [2].

Архитектура включает в себя три основных компонента: блокчейн, изолированный централизованный сервер и клиентское приложение. Блокчейн используется в качестве защищенного хранилища, где фиксируются ключевые медицинские записи в зашифрованном виде, а также метаданные о взаимодействиях пользователей с системой. Децентрализованная структура хранения позволяет исключить возможность несанкционированного изменения данных, гарантируя их неизменяемость. В блокчейне также интегрирована логика управления доступом, включающая список авторизованных аккаунтов и их ролей (например, пациент, врач, администратор), что позволяет строго контролировать права пользователей в соответствии с принципами, описанными в работе [3]. В блокчейне также содержатся уникальные ключи дешифрования, доступ к которым осуществляется через механизм управления правами.

Централизованный сервер выполняет роль справочной системы, хранящей нефинансовую и административную информацию, которая не требует высокой степени защиты. В его базу данных записываются сведения о принадлежности врачей к медицинским учреждениям, а также вспомогательные данные, необходимые для взаимодействия системы с внешними сервисами. Такое разделение хранения позволяет снизить нагрузку на блокчейн.

Клиентское приложение выступает в роли интерфейса пользователя и обеспечивает взаимодействие с блокчейном и центральным сервером. При добавлении медицинских данных информация передается в блокчейн в зашифрованном виде. При необходимости пользователь может получить зашифрованные данные из сети и расшифровать их на клиентской стороне, используя соответствующие ключи. В случае необходимости получения дополнительной справочной информации клиент взаимодействует с централизованным сервером.

Использование стандартной архитектуры EVM привело бы к ряду ограничений, таких как низкая скорость транзакций, высокая нагрузка на вычислительные ресурсы и необходимость оплаты операций. Алгоритм Proof of Work (PoW) создавал бы значительные задержки, а Proof of Authority (PoA) требовал доверенных валидаторов, ограничивая гибкость системы [4]. Также критичной проблемой стала необходимость оплаты пользователями каждой транзакции, что неприемлемо в медицинских системах.

Для устранения этих недостатков в приватном блокчейне внедрен алгоритм Istanbul Byzantine Fault Tolerance (IBFT), который гарантирует финализацию транзакций и устраняет форки [5]. Время генерации блока сокращено до двух секунд, что ускорило обработку данных.

Оптимизированы параметры сети, а нулевая комиссия позволила исключить финансовые барьеры для пользователей.

Контроль доступа реализован через смарт-контракты, обеспечивающие разграничение прав участников. В результате приватный блокчейн стал безопасным и эффективным инструментом для хранения медицинских данных, соответствующим законодательным требованиям и готовым к интеграции с медицинскими учреждениями.

Выводы. Разработка модели хранения и управления медицинскими данными на основе блокчейна потребовала значительной оптимизации существующих решений для обеспечения безопасности, отказоустойчивости, высокой скорости обработки информации, а также соответствия международным стандартам и правовым документам. В ходе исследования выявлены ограничения публичных блокчейнов, такие как низкая скорость транзакций, необходимость оплаты газа пользователями и недостаточный уровень контроля доступа. Эти проблемы сделали стандартные EVM-решения неприменимыми в медицинской сфере, что обусловило необходимость разработки адаптированной конфигурации приватного блокчейна.

Предложенная архитектура основана на трехкомпонентной модели, включающей блокчейн, централизованный сервер и клиентское приложение. Блокчейн выполняет функции защищенного хранилища, обеспечивая неизменяемость данных и контроль доступа через смарт-контракты. Централизованный сервер содержит вспомогательную информацию, позволяя снизить нагрузку на сеть. Клиентское приложение передает зашифрованные данные в блокчейн, а при получении дешифрует их на стороне пользователя.

Важной частью работы стала оптимизация блокчейна для соответствия требованиям медицинской отрасли. Основные изменения включают переход на алгоритм консенсуса IBFT, сокращение времени генерации блока до двух секунд для увеличения скорости обработки данных, а также настройку нулевых комиссий, исключающих финансовые затраты пользователей. Дополнительно внедрены механизмы управления доступом через смарт-контракты, позволяющие строго контролировать права участников сети.

Разработанная система обеспечивает надежное хранение медицинских данных, прозрачность их обработки и защиту от несанкционированного доступа. Проведенная оптимизация позволила создать гибкую, высокопроизводительную и безопасную платформу, соответствующую законодательным требованиям и интегрируемую с медицинскими учреждениями.

Список использованных источников:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ // Официальное интернет-представительство президента России URL: http://www.kremlin.ru/acts/bank/24154 (дата обращения: 16.01.2025).
2. Dolin R. H. et al. The HL7 clinical document architecture //Journal of the American Medical Informatics Association. – 2001. – Т. 8. – №. 6. – С. 552-569.
3. Sookhak M. et al. Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues //Journal of Network and Computer Applications. – 2021. – Т. 178. – С. 102950.
4. Samuel C. N. et al. Choice of ethereum clients for private blockchain: Assessment from proof of authority perspective //2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). – IEEE, 2021. – С. 1-5.
5. Bains P. Blockchain consensus mechanisms: A primer for supervisors. – International Monetary Fund, 2022.