УДК 004.75:61

# АРХИТЕКТУРА ПОДСИСТЕМЫ БЛОКЧЕЙН ДЛЯ МЕДИЦИНСКИХ ДАННЫХ

*Кацко М.О.*, магистрант гр.467041

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Вишняков В.А. – д-р техн. наук, профессор*

**Аннотация.** Проанализированы существующие международные разработки в области блокчейн-систем, предназначенные для применения в сфере здравоохранения. Особое внимание уделено таким проектам, как Minima/Siemens/ARM (концепция "блокчейн-на-кристалле"), BlockTrack (разработка IIT Madras), Emtruth (проект NSF), а также архитектурным решениям TLSA, STORChain и CareChain. На основе полученных данных предложена оригинальная многоуровневая архитектура блокчейн-подсистемы, предназначенной для надежного хранения медицинских данных.

**Ключевые слова.** Блокчейн, IT-медицина, медицинские данные, IPFS, архитектура, децентрализованное хранение, смарт-контракты, конфиденциальность, функциональные модули.

## Введение

Цифровая трансформация здравоохранения привела к экспоненциальному росту объемов медицинских данных. Электронные медицинские карты (ЭМК), данные диагностического оборудования, результаты лабораторных исследований, информация с носимых устройств и телемедицинских платформ формируют сложные информационные массивы, требующие надежного хранения и защищенного обмена. Традиционные централизованные системы хранения медицинских данных сталкиваются с рядом фундаментальных проблем: рисками утечек и несанкционированного доступа, высокими затратами на обеспечение безопасности, сложностью интероперабельности между различными медицинскими учреждениями, а также отсутствием у пациентов контроля над собственными данными [1].

Технология блокчейн предлагает принципиально иной подход к организации хранения медицинских данных. Ее ключевые характеристики – децентрализация, неизменяемость записей, криптографическая защита и прозрачность транзакций, что делают ее идеальной основой для систем управления медицинской информацией [2]. Однако прямое хранение медицинских записей в блокчейне (on-chain storage) сталкивается с ограничениями по объему данных, высокой стоимостью транзакций и проблемами масштабируемости. Это обусловливает необходимость разработки гибридных архитектур, сочетающих блокчейн для обеспечения неизменяемости и контроля доступа с распределенными файловыми системами (IPFS) для хранения самих медицинских данных [3].

Целью настоящей работы является разработка многоуровневой архитектуры подсистемы блокчейн для хранения медицинских данных, объединяющей передовые международные подходы и обеспечивающей баланс между безопасностью, масштабируемостью и удобством использования для пациентов и медицинских учреждений.

## Основная часть

Проект STORChain (IEEE Transactions on Services Computing, 2026) представляет собой оптимизированную по хранению блокчейн-структуру, разработанную для медицинских данных. Ключевой инновацией является Clustered Merkle Patricia Tree (C-MPT) – кластеризованное дерево Меркла-Патриции, которое агрегирует транзакции схожих типов для максимальной эффективности хранения при сохранении возможности доказательства включения (Proof of Inclusion) [4]. STORChain включает: C-MPT структуру: объединение похожих типов транзакций в кластеры для уменьшения накладных расходов; Selective Transaction Pruning Strategy (STPS): стратегию выборочной обрезки транзакций для приоритизации и удаления устаревших исторических данных Делегированное доказательство доли (DPoS): алгоритм консенсуса с вероятностным механизмом выборов для повышения справедливости и инклюзивной узлов.

Трехуровневая архитектура TLSA (Wiley, 2025). Исследователи K. Maithili и S. Amutha предложили Tri-Layered Sharding Architecture (TLSA) – иерархическую модель, организующую сеть в три шардинговых уровня: Transaction Layer (уровень транзакций), Data Layer (уровень данных) и Location Layer (уровень расположения) [5].

Система CareChain, использующая два блокчейна (публичный для пациентов и приватный для медицинских работников) в сочетании с распределенным хранилищем IPFS [6]. Ключевые особенности CareChain: двойная блокчейн-структура: разделение данных пациентов и провайдеров для повышения конфиденциальности; IPFS распределенное хранение: снижение задержки транзакций и накладных расходов на хранение; ECDSA (Elliptic Curve Digital Signature Algorithm): подпись транзакций для обеспечения подлинности; устройство-прокси: мониторинг низкопроизводительных IoT-устройств для выявления уязвимостей. Результаты тестирования

показывают повышение устойчивости системы по сравнению с существующими моделями здравоохранения, а также улучшение требований к хранилищу, энергоэффективности, скорости транзакций, конфиденциальности и безопасности [6].

Minima, Siemens, ARM: блокчейн-на-кристалле (2025-2026), направлен на создание первого в мире промышленного микрочипа, способного выполнять полноценный узел блокчейна [7]. Результаты проекта: 100-кратное ускорение хеширования за счет SHA-3 аппаратного ускорителя; пятикратное снижение использования памяти после рефакторинга C++ кода; Возможность работы устройства как самостоятельного полного узла без обращения к облачной инфраструктуре [7].

Индийский институт технологий (IIT Madras) разработал BlockTrack – блокчейн-систему для мобильных приложений, которая в настоящее время проходит полевые испытания в университетской больнице [8]. Характеристики BlockTrack: децентрализованный обмен медицинскими данными для мобильных приложений; Уникальные идентификационные коды для пользователей с низкой вероятностью дублирования.

Проект Emtruth, поддержанный Национальным научным фондом США (NSF) на сумму почти 1 млн долларов, разрабатывает платформу для интеграции медицинских данных с использованием блокчейна и искусственного интеллекта [2]. Ключевые цели проекта: безопасное хранение данных любого типа из любых источников в неизменяемых блокчейнах; сохранение контроля данных за владельцем с возможностью безопасного предоставления доступа; трансформация и нормализация данных в гранулярные блокчейны для индивидуального или агрегированного моделирования.

В Университете ИТМО предложена трехкомпонентная архитектура, включающая блокчейн для хранения зашифрованных медицинских записей, централизованный сервер для справочной информации и клиентское приложение для управления доступом [3]. Особое внимание уделяется оптимизации EVM-блокчейна через адаптацию алгоритма консенсуса, снижение времени блока и устранение транзакционных комиссий.

На основе анализа международных разработок разработана многоуровневая архитектура подсистемы блокчейн для хранения медицинских данных, которая объединяет пять функциональных модулей, каждый из которых решает специфические задачи обеспечения безопасности, масштабируемости и доступности данных. Рассмотрим их назначение.

1. Источники данных (Data Sources Layer): медицинские учреждения, генерирующие электронные медицинские записи и диагностические изображения; IoT-устройства и носимые сенсоры, собирающие физиологические показатели в реальном времени; диагностические лаборатории, предоставляющие результаты анализов и исследований;

2. Распределенное хранилище IPFS (IPFS Layer): децентрализованное хранилище, адресуемое по содержимому; хранение зашифрованных медицинских записей, результатов исследований и данных IoT-устройств; генерация уникальных Content Identifiers для ссылок на данные; кэширование и репликация для повышения доступности и снижения задержек [6].

3. Блокчейн-инфраструктура (Blockchain Layer): гибридная архитектура, объединяющая публичный и приватный блокчейны [4]; публичный блокчейн: идентификаторы пациентов, сертификаты учреждений, информация о роуминге; приватный блокчейн: хеши записей (CID), транзакции доступа, аудиторские журналы, смарт-контракты; алгоритмы консенсуса: DPoS для масштабируемости, PBFT для приватных сетей [4].

4. Управление доступом (Access Control Layer): система атрибутивного управления доступом на основе CP-ABE и ABAC [7]; генерация и управление криптографическими ключами; определение политик доступа на основе атрибутов пациентов, врачей и учреждений; журналирование всех операций доступа для аудита;

5. Приложения (Application Layer): пациентское приложение: просмотр записей, управление доступом, предоставление согласий; врачебное приложение: доступ к записям пациентов, добавление заключений, назначение лечения; административное приложение: управление политиками, аудит, регистрация учреждений.

Представленная многоуровневая архитектура подсистемы блокчейн для хранения медицинских данных является комплексным и продуманным решением, направленным на обеспечение безопасности, масштабируемости и доступности конфиденциальной медицинской информации. Она эффективно интегрирует различные технологии, такие как децентрализованное хранилище IPFS, гибридный блокчейн и атрибутивное управление доступом, для создания надежной и прозрачной системы.

Ниже представлены описания основных компонентов системы:

1. Модуль шифрования и защиты данных обеспечивает криптографическую защиту медицинских данных на всех этапах обработки. Его основные компоненты включают шифрование на основе CP-ABE или 128-битное AES с последовательностью ДНК-кодирования [9] для хранения в IPFS, цифровой конверт RSA 2048 для безопасной передачи симметричных ключей, цифровую подпись RSA 1024 для обеспечения подлинности данных, ECDSA для генерации пар публичных и приватных ключей для устройств, пациентов и провайдеров, подпись транзакций для обеспечения подлинности и защиты от подделки, верификацию подписей при получении данных [4], а также стройство-прокси (Device Proxy) для мониторинга низкопроизводительных IoT-устройств.

2. Модуль хранения IPFS реализует распределенное хранение медицинских данных с адресацией по содержимому. Его основные функции включают Content-Addressable Storage, где данные идентифицируются по их криптографическому хешу (CID), обеспечивая неизменяемость и возможность

верификации [6], Distributed Hash Table (DHT) для хранения соответствия между CID и сетевыми адресами узлов, содержащих данные, кэширование и репликация для снижения задержек и уменьшения нагрузки на сеть, а также управление CID для загружаемых данных [1].

3. Модуль смарт-контрактов реализует автоматизированную логику управления доступом и обработки транзакций. Его основные функции включают управление доступом, где смарт-контракты проверяют атрибуты пользователя и политики доступа перед предоставлением CID [8], обработку согласий, аудит и журналирование для записи всех операций доступа в неизменяемый журнал блокчейна, а также управление идентификаторами для создания и верификации уникальных идентификаторов пациентов и медицинских учреждений [8].

4. Модуль управления идентификацией обеспечивает уникальную идентификацию пациентов и медицинских учреждений в распределенной системе. Его основные функции включают генерацию уникальных идентификаторов с низкой вероятностью дублирования [8], связывание идентификаторов для создания полной медицинской карты [2], кросс-учрежденческую идентификацию для обеспечения интероперабельности между различными медицинскими организациями, а также управление сертификатами для хранения публичных ключей и сертификатов учреждений в публичном блокчейне.

5. Модуль аудита и мониторинга обеспечивает прозрачность и возможность проверки всех операций с медицинскими данными. Его основные функции включают неизменяемый журнал доступа [1], анализ аномалий для обнаружения подозрительных паттернов доступа [6], генерацию отчетов о доступе для пациентов и врачей, а также уведомления о каждом случае доступа к данным.

Таким образом, система представляет собой интегрированное решение, обеспечивающее безопасность, прозрачность, надежность и удобство управления медицинскими данными в распределенной среде с использованием передовых технологий блокчейна, криптографии и распределенного хранения.

**Заключение**

Международные разработки демонстрируют высокую активность и значительные достижения. Предложенная многоуровневая архитектура объединяет лучшие мировые практики в единое решение. Пятиуровневая структура (источники данных, IPFS, блокчейн, управление доступом, приложения) обеспечивает разделение ответственности, масштабируемость и безопасность. Использование гибридной блокчейн-архитектуры позволяет сохранить прозрачность идентификации при обеспечении конфиденциальности медицинских записей.

Ключевыми компонентами системы являются: модуль шифрования на основе ECDSA и CP-ABE, обеспечивающий защиту данных; модуль IPFS для распределенного хранения с адресацией по содержимому; модуль смарт-контрактов для автоматизации управления доступом; модуль управления идентификацией для уникальной идентификации пациентов; модуль аудита для обеспечения прозрачности операций.

***Список использованных источников:***

*1. Emtruth, Inc. SBIR Phase II: A Platform for Health Care Data Integration Using Blockchain and Artificial Intelligence / NSF Award 2304102. – National Science Foundation, 2023. – URL: https://www.sbir.gov/awards/2304102 (дата обращения: 16.03.2026).*

*2.Лаврова, А. К., Максимова, Т. Г. Блокчейн для медицины: новая модель хранения и управления медицинскими данными / А. К. Лаврова, Т. Г. Максимова // Сборник тезисов докладов конгресса молодых ученых. – СПб : Университет ИТМО, 2025. – URL: h ttps://kmu.itmo.ru/digests/article/ 14096 (дата обращения: 16.03.2026).*

*3.STORChain: A Clustered-MPT-Based Blockchain for Data Service and Efficient Storage in Healthcare / IEEE Transactions on Services Computing. – 2026. – P. 685-699..*

*4.Maithili, K., Amutha, S. Optimizing Blockchain Scalability for Secure Patient Health Records With Tri-Layered Sharding Architecture (TLSA) / K. Maithili, S. Amutha // Transactions on Emerging Telecommunications Technologies. – 2025.*

*5.CareChain: Secure and scalable dual blockchain and IPFS driven IoT ecosystem for next gen healthcare systems / Scientific Reports. – 2025.*

*6.Minima Achieves Major Breakthrough: Blockchain-on-Chip Is Here / Minima Global. – 15 December 2025. – URL: https://minima.global/ru/post/minima-achieves-major-breakthrough-blockchain-on-chip-is-here (дата обращения: 16.03.2026).*

*7.IIT Madras. IIT Madras Develops Blockchain-based Healthcare Information Systems for Mobile Apps / Principal Scientific Adviser, Government of India. – 2026. – URL:h ttps://www.psa.gov.in/article/iit-madras-develops-blockchain-based-healthcare-information-systems-mobile-apps/2744 (дата обращения: 16.03.2026).*

*8.Sanober, A., Anwar, S. A secure and privacy preserving model for healthcare applications based on blockchain-layered architecture / A. Sanober, S. Anwar // International Journal of Computers and Applications. – 2024. – P. 1206-1218.*

UDC 004.75:61

# ARCHITECTURE OF A BLOCKCHAIN SUBSYSTEM FOR MEDICAL DATA

*Katsko M.A.*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Vishnyakov V.A. – Doctor of Technical Sciences, professor*

**Annotation.** Existing international developments in blockchain systems designed for healthcare applications have been analyzed. Particular attention has been paid to projects such as Minima/Siemens/ARM (the "blockchain-on-a-chip" concept), BlockTrack (developed by IIT Madras), Emtruth (an NSF project), as well as the architectural solutions TLSA, STORChain, and CareChain. Based on the obtained data, an original multi-layered architecture for a blockchain subsystem intended for reliable storage of medical data is proposed.

**Keywords.** Blockchain, IT medicine, medical data, IPFS, architecture, decentralized storage, smart contracts, privacy, functional modules.