УДК 004.65:61

МНОГОУРОВНЕВАЯ АРХИТЕКТУРА БЛОКЧЕЙНА ДЛЯ ХРАНЕНИЯ МЕДИЦИНСКИХ ДАННЫХ

В.А. ВИШНЯКОВ, М.О. КАЦКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 6 апреля 2026

Аннотация. Проанализированы международные разработки в области блокчейн-систем для здравоохранения. Предложена многоуровневая архитектура подсистемы блокчейн для хранения медицинских данных, объединяющая распределенное хранилище IPFS, гибридную блокчейн-инфраструктуру, систему атрибутивного управления доступом и клиентские приложения. Представлена структурная схема системы с описанием функциональных модулей. Разработан алгоритм работы системы, включающий регистрацию пользователей, загрузки данных, предоставления доступа и верификации транзакций.

Ключевые слова: блокчейн, медицинские данные, IPFS, архитектура, децентрализованное хранение, смарт-контракты, конфиденциальность, безопасность данных.

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.

Международные разработки

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.

Структура системы

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. Архитектура представлена на рис.1.

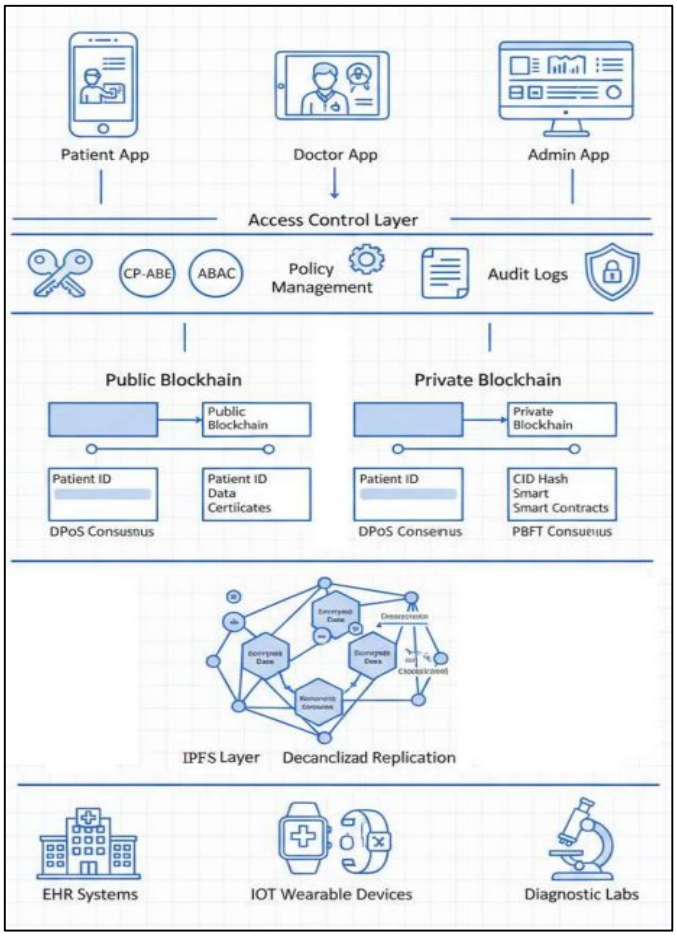

Рис. 1. Многоуровневая архитектура подсистемы блокчейн

Рассмотрим их назначение каждого уровня.

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.

Описание модулей

Шифрования и защиты данных обеспечивает криптографическую защиту медицинских данных на всех этапах обработки. Основные компоненты: для хранения в IPFS шифрование на основе CP-ABE или 128-битное AES с последовательностью ДНК-кодирования [9]; для передачи используется цифровой конверт RSA 2048 для безопасной передачи симметричных ключей; цифровая подпись RSA 1024 для обеспечения подлинности данных; ECDSA: генерация пар публичных и приватных ключей для устройств, пациентов и провайдеров; подпись транзакций для обеспечения подлинности и защиты от подделки; верификация подписей при получении данных [4]; стройство-прокси (Device Proxy): мониторинг низкопроизводительных IoT-устройств для выявления уязвимостей; непрерывная проверка типа устройства, производителя, версии прошивки, безопасности; обнаружение подозрительного поведения через тестирование на проникновение и поведенческий анализ [6].

Хранения IPFS реализует распределенное хранение медицинских данных с адресацией по содержимому. Основные функции: Content-Addressable Storage: данные идентифицируются по их криптографическому хешу (CID), что обеспечивает неизменяемость и возможность верификации [6]; Distributed Hash Table (DHT): распределенная хеш-таблица для хранения соответствия между CID и сетевыми адресами узлов, содержащих данные; кэширование и репликация: кэширование часто запрашиваемых данных на соседних узлах для снижения задержек и уменьшения нагрузки на сеть; Content Identifier (CID) Management: генерация и хранение CID для загружаемых данных; CID сохраняются в блокчейне, а данные – в IPFS [1].

Смарт-контракты реализуют автоматизированную логику управления доступом и обработки транзакций. Основные функции: управление доступом: смарт-контракты проверяют атрибуты пользователя и политики доступа перед предоставлением CID [8]; обработка согласий: автоматическое отслеживание предоставленных пациентом согласий на доступ к данным, их сроков действия и отзыва; аудит и журналирование: запись всех операций доступа в неизменяемый журнал блокчейна для последующего аудита; управление идентификаторами: создание и верификация уникальных идентификаторов пациентов и медицинских учреждений [8].

Управления идентификацией обеспечивает уникальную идентификацию пациентов и медицинских учреждений в распределенной системе. Основные функции: генерация уникальных идентификаторов: алгоритмы, обеспечивающие уникальность ID с низкой вероятностью дублирования [8]; связывание идентификаторов: возможность связывания идентификаторов пациента из разных систем для создания полной медицинской карты [2]; кросс-учрежденческая идентификация: обеспечение интероперабельности между различными медицинскими организациями; управление сертификатами: хранение публичных ключей и сертификатов учреждений в публичном блокчейне.

Аудит и мониторинг обеспечивает прозрачность и возможность проверки всех операций с медицинскими данными. Основные функции: *неизменяемый журнал доступа:* все операции доступа фиксируются в блокчейне и не могут быть изменены или удалены [1]; *анализ аномалий:* обнаружение подозрительных паттернов доступа для выявления потенциальных нарушений безопасности [6]; *генерация отчетов* о доступе для пациентов, врачей; *уведомления:* оповещение пациентов о каждом случае доступа к их данным.

Алгоритм работы системы

Разработаны алгоритмы взаимодействия учасников в рамках многоуровневой блокчейн архитектуры, обеспечивающие неизменность записей и управляемый доступ.

Алгоритм регистрации пользователя состоит из следующих шагов:

1. Пациент или врач загружает клиентское приложение и заполняет регистрационную форму.

2. Приложение генерирует пару криптографических ключей (приватный и публичный) с использованием ECDSA [6].

3. Приложение отправляет регистрационную информацию и публичный ключ в систему. Данные верифицируются, и создается уникальный идентификатор [8].

4. Идентификатор и публичный ключ записываются в публичный блокчейн. Создается запись в приватном блокчейне с начальными настройками доступа.

5. Пользователю предоставляется доступ к приложению с возможностью управления своими данными.

Алгоритм загрузки медицинских данных включает в себя этапы:

1. Загрузка данных (ЭМК, результаты анализов, изображения) медицинским учреждением или врачом через приложение.

2. Шифрования данных с использованием гибридной схемы (AES или CP-ABE) в соответствии с атрибутами доступа [9].

3. Передача зашифрованных данные в IPFS-сеть. IPFS вычисляет CID на основе содержимого и распределяет данные по узлам [8].

4. Возврат CID (Content Identifier) – уникальную ссылку на данные в IPFS.

5. Запись CID и метаданных в приватный блокчейн через смарт-контракт [8].

6. Добавление записи о факте создания новой записи (без раскрытия содержимого) в публичный блокчейн.

Алгоритм предоставления доступа к данным описывается следующим образом:

1. Пациент через приложение выбирает медицинского специалиста или учреждение для предоставления доступа.

2. Пациент определяет параметры доступа, объем данных, срок действия, цель использования [2].

3. Приложение формирует политику доступа в формате атрибутов (ABAC) или шифрует данные с политикой CP-ABE [12].

4. Смарт-контракт в приватном блокчейне регистрирует политику доступа и связывает ее с идентификаторами пациента и получателя.

5. Получатель уведомляется о предоставленном доступе через приложение. При необходимости получатель проходит дополнительную аутентификацию.

6. Все действия по предоставлению доступа фиксируются в аудиторском журнале блокчейна.

Алгоритм доступа к данным:

1. Врач или медицинское учреждение через приложение запрашивает доступ к данным пациента.

2. Припложение направляет запрос к смарт-контракту для проверки наличия действующего согласия.

3. Смарт-контракт проверяет политики доступа, соответствие атрибутов запрашивающего, срок действия согласия, объем разрешенных данных [9].

4. При успешной проверке смарт-контракт возвращает cid запрошенных данных.

5. Приложение запрашивает данные из IPFS по полученному CID. IPFS-сеть извлекает зашифрованные данные [4].

6. Данные расшифровываются с использованием ключей, соответствующих политике доступа, и отображаются врачу.

7. Факт доступа регистрируется в блокчейне с указанием времени, запрашивающего и объема данных.

Алгоритм отзыва доступа предусматривает слудующие ключивые шаги:

1. Пациент через приложение инициирует отзыв предоставленного доступа.

2. Приложение формирует транзакцию отзыва с указанием идентификатора.

3. Смарт-контракт деактивирует политику доступа, делая ее недействительной.

4. Смарт-контракт обновляет аудиторский журнал, фиксируя факт отзыва.

5. Получатель уведомляется об отзыве доступа. Последующие попытки доступа будут отклонены.

6. Может быть выполнено повторное шифрование данных с новыми политиками доступа.

Особое внимание в предложенном алгоритме работы системы уделено обеспечению конфидециальности, неименяемости записей и ограничениям в предоставление доступа.

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.

MULTILEVEL BLOCKCHAIN ARCHITECTURE FOR MEDICAL DATA STORING

U.A VISHNIAKOU, M.A. KATSKO

Abstract. International developments in the field of blockchain systems for healthcare are analyzed,. A multi-level architecture of the blockchain subsystem for storing medical data is proposed, combining IPFS distributed storage, hybrid blockchain infrastructure, attribute access control system and client applications. A structural diagram of the system with a description of the functional modules is presented. The system's algorithm has been developed, which includes the stages of user registration, data upload, access, and transaction verification. Keywords. blockchain, medical data, IPFS, architecture, decentralized storage, smart contracts, privacy, data security.)

Keywords. blockchain, medical data, IPFS, architecture, decentralized storage, smart contracts, privacy, data security.

Список литературы

1. Adapa, C. S. R. Enhancing Healthcare Data Integrity Through Blockchain-Based Master Data Management. An Architectural Framework / C. S. R. Adapa // Journal of Information Systems Engineering and Management. – 2026. – Vol. 11.
2. 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).
3. 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).
4. STORChain. A Clustered-MPT-Based Blockchain for Data Service and Efficient Storage in Healthcare / IEEE Transactions on Services Computing. – 2026.
5. 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.
6. CareChain. Secure and scalable dual blockchain and IPFS driven IoT ecosystem for next gen healthcare systems / Scientific Reports. – 2025.
7. 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).
8. 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).
9. 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. – Vol. 46. – No. 12. – P. 1206-1218.