



Блокчейн для пациентов: перспективы применения в цифровом здравоохранении

Костров С. А., Потапов М. П., Кулибина О. В.

ФГБОУ ВО «Ярославский государственный медицинский университет», Ярославль, Российская Федерация

Аннотация

Данная статья посвящена анализу перспектив и вызовов интеграции блокчейн-технологий в систему управления медицинскими данными в контексте цифровой трансформации здравоохранения. Актуальность исследования обусловлена растущей потребностью в создании безопасных, прозрачных и пациентоориентированных инфраструктур для обработки медицинской информации. В работе представлена сравнительная характеристика публичных, частных и консорциумных блокчейн-платформ, среди которых консорциумная модель выделяется как наиболее перспективная для формирования экосистем обмена данными между различными участниками здравоохранения. Детально рассматриваются технологические аспекты, включая гибридную архитектуру хранения (сочетание блокчейна с распределёнными файловыми системами, такими как InterPlanetary File System), модели динамического и предикативного информированного согласия пациентов на основе смарт-контрактов, а также применение блокчейна в телемедицине и для управления электронными медицинскими картами нового поколения. В статье также систематизированы ключевые вызовы внедрения: необходимость преодоления противоречия между неизменностью блокчейна и правом на забвение, потребность в переходе к постквантовой криптографии, вопросы масштабируемости, энергоэффективности, правового регулирования и интеграции с существующими медицинскими информационными системами. Делается вывод, что успешная имплементация блокчейн-решений в российское здравоохранение требует скоординированного развития технологической инфраструктуры (с акцентом на отечественные платформы, такие как «Мастерчейн»), адаптации нормативно-правовой базы и целевой подготовки медицинских кадров, обладающих компетенциями в области цифровых технологий.

Ключевые слова: блокчейн; консорциумный блокчейн; цифровое здравоохранение; электронные медицинские карты; ЭМК; динамическое согласие; смарт-контракты; телемедицина; постквантовая криптография; распределённые файловые системы; пациентоориентированность

Для цитирования: Костров С. А., Потапов М. П., Кулибина О. В. Блокчейн для пациентов: перспективы применения в цифровом здравоохранении. *Пациентоориентированная медицина и фармация*. 2025;3(4):69–76. <https://doi.org/10.37489/2949-1924-0120>. EDN: PLGMEJ.

Поступила: 31.07.2025. В доработанном виде: 09.09.2025. Принята к печати: 15.10.2025. Опубликовано: 25.12.2025.

Blockchain for patients: perspectives of application in digital healthcare

Sergey A. Kostrov, Maxim P. Potapov, Olga V. Kulibina

Yaroslavl State Medical University, Yaroslavl, Russian Federation

Abstract

This article analyzes the prospects and challenges of integrating blockchain technologies into medical data management systems within the context of digital healthcare transformation. The study's relevance stems from the growing need to establish secure, transparent, and patient-centric infrastructures for handling medical information. The paper provides a comparative analysis of public, private, and consortium blockchain platforms, identifying the consortium model as the most promising for creating data exchange ecosystems among various healthcare stakeholders. Technological aspects are examined in detail, including a hybrid storage architecture (combining blockchain with distributed file systems like InterPlanetary File System), models for dynamic and predictive informed patient consent based on smart contracts, and the application of blockchain in telemedicine and next-generation electronic health record (EHR) management. The article also systematizes key implementation challenges: the need to reconcile blockchain immutability with the right to be forgotten, the imperative for a transition to post-quantum cryptography, as well as issues of scalability, energy efficiency, legal regulation, and integration with exist-

ing medical information systems. The conclusion emphasizes that the successful implementation of blockchain solutions in Russian healthcare requires coordinated development of technological infrastructure (focusing on domestic platforms like "Masterchain"), adaptation of the regulatory framework, and targeted training of medical professionals with competencies in digital technologies.

Keywords: blockchain; consortium blockchain; digital healthcare; electronic medical records; EMR; dynamic consent; smart contracts; telemedicine; post-quantum cryptography; distributed file systems; patient-centricity

For citation: Kostrov SA, Potapov MP, Kulibina OV. Blockchain for patients: perspectives of application in digital healthcare. *Patient-oriented medicine and pharmacy*. 2025;3(4):69–76. <https://doi.org/10.37489/2949-1924-0120>. EDN: PLGMEJ.

Received: 31.07.2025. **Revision received:** 09.09.2025. **Accepted:** 15.10.2025. **Published:** 25.12.2025.

Введение / Introduction

Современная медицина переживает период цифровой трансформации, в ходе которой блокчейн-технология выступает одним из ключевых катализаторов изменений, предполагая дальнейшую вовлеченность пациента в управление собственными медицинскими данными и процессами лечения [1, 2].

Актуальность данного исследования обусловлена растущей потребностью в безопасных, прозрачных и пациенто-контролируемых системах управления медицинскими данными.

Успешное внедрение блокчейн-технологий в здравоохранении требует многоуровневой системы подготовки кадров, интегрирующей теоретические основы с практическими навыками. Медицинским работникам для необходимо понимание принципов блокчейн-архитектуры, криптографических методов защиты данных, алгоритмов консенсуса и их применимости в медицинских системах. Особое внимание следует уделить изучению консорциумных блокчейнов как наиболее перспективной модели для здравоохранения.

Традиционные централизованные системы хранения данных уязвимы для кибератак, несанкционированного доступа и фальсификации информации.

Блокчейн представляет собой распределенную систему записи транзакций, где каждый блок содержит криптографически связанную информацию с предыдущими блоками, обеспечивая неизменность данных [3]. Несмотря на то, что технология блокчейн получила наибольшую известность как фундаментальная платформа для криптовалют, таких как Bitcoin, отождествление этих понятий является некорректным. Блокчейн представляет собой более общую технологию, потенциал применения которой значительно превосходит финансовую сферу. В частности, в здравоохранении данная технология открывает возможности для создания неизменяемых, децентрализованных, криптографически защищенных и хронологически верифицируемых реестров для постоянного хранения медицинской документации, включая врачебные заключения, выписки и рецепты [1, 2].

Цель данной статьи / Objective — провести анализ существующих и перспективных пациенто-ориентированных применений блокчейна в медицине, выделить ключевые технологические и организационные вызовы, а также обозначить направления дальнейших исследований.

Материалы и методы / Materials and methods

Выбор технологического решения по степени открытости является определяющим при выборе платформы. Выбор конкретного типа платформы определяется системными характеристиками, такими как уровень конфиденциальности, производительность, модель управления и степень децентрализации.

Выделяются три основных типа блокчейн-сетей: публичные, приватные и консорциумные (федеративные).

Публичные (public) блокчейны, неразрешённые (permissionless), представляют собой полностью открытые и децентрализованные сети. Любой желающий может присоединиться к сети, участвовать в процессе консенсуса, считывать данные и отправлять транзакции для включения в реестр [4].

Из-за своей прозрачности и низкой пропускной способности, публичные блокчейны в чистом виде плохо подходят для хранения медицинских данных. Так, сеть Bitcoin обрабатывает 5–7 транзакций в секунду, и имеет время формирования блока около 10 минут; Ethereum обрабатывает 20–25 транзакций в секунду, формируя блок за 5–6 минут, что совершенно недостаточно в национальных масштабах, изменяемых на сегодняшний день миллионами транзакций в сутки. Однако они могут использоваться для публичной верификации и неизменяемой фиксации времени (timestamping) хешей медицинских документов, которые хранятся вне цепи (off-chain), тем самым подтверждая их целостность и время создания без раскрытия самого содержимого [5–7].

Приватные (Private Blockchains), или разрешённые (permissioned), блокчейны управляются одной организацией, где центральная структура определяет, кто может присоединяться к сети, просматривать данные и выполнять транзакции. Этот тип



оптимален для внутренних процессов крупных медицинских организаций. Он может использоваться для создания защищённого внутреннего хранилища, управления доступом к электронным медицинским картам (ЭМК) внутри учреждения [5–7].

Консорциумные (Consortium), или федеративные, блокчейны представляют собой гибридную модель, управляемую группой предварительно определённых организаций, а не единственным субъектом или неопределённым кругом субъектов. Эта модель также является разрешённой (permissioned), но децентрализация достигается на

уровне консорциума. Эта модель выглядит на наш взгляд наиболее перспективной для большинства медицинских приложений, благодаря балансу между децентрализацией и контролем, позволит создавать безопасные сети для обмена данными между различными участниками системы здравоохранения, региональными и федеральными центрами, лабораториями, страховыми компаниями, исследовательскими институтами и регуляторными органами. Это обеспечивает интероперабельность при сохранении строгого контроля над доступом и конфиденциальностью данных [5–7].

Таблица. Сравнение блокчейн-платформ
Table. Comparison of blockchain platforms

Характеристика	Публичный блокчейн	Приватный блокчейн	Консорциумный блокчейн
Управление доступом	Открытый (Permissionless)	Закрытый (Permissioned)	Закрытый (Permissioned)
Участники	Любой желающий	Одна организация	Несколько организаций (консорциум)
Консенсус	Определяется всеми участниками (например, Proof-of-Work)	Контролируется владельцем сети (например, Proof-of-Authority)	Определяется членами консорциума (например, PBFT)
Скорость транзакций	Низкая	Высокая	Высокая
Конфиденциальность	Низкая (псевдонимная)	Высокая	Высокая (в рамках консорциума)
Примеры платформ	Bitcoin, Ethereum	Hyperledger Sawtooth, Geth (Go Ethereum), Waves Enterprise	Hyperledger Fabric, R3 Corda
Медицинские применения	Публичная верификация, timestamping	Внутренний аудит, управление данными внутри одной клиники	Межорганизационный обмен ЭМК, клинические исследования, цепочки поставок лекарств и др.

Электронные медицинские карты нового поколения / Next-generation electronic medical records

Традиционная модель управления электронными медицинскими картами (ЭМК) характеризуется централизованной архитектурой с фрагментированным распределением данных между различными медицинскими информационными системами (МИС), по различным учреждениям здравоохранения без возможности унифицированного доступа.

Блокчейн-решения предлагают пациенто-контролируемую модель, где пациент становится распорядителем своих данных и может селективно предоставлять доступ медицинским специалистам. В этой модели блокчейн функционирует как криптографически защищённый реестр разрешений доступа, а не как хранилище собственно медицинских данных. Используются два слоя функционирования [8, 9]:

On-chain компоненты (в блокчейне): метаданные о структуре и местоположении медицинских

записей, криптографические хеши документов для обеспечения целостности данных, смарт-контракты для управления разрешениями доступа, журналы аудита всех операций.

Off-chain компоненты (вне блокчейна): полные медицинские записи в зашифрованном виде, медицинские изображения и диагностические данные, персональные идентификационные данные пациентов.

Хранение больших объёмов медицинских данных, таких как снимки МРТ или КТ, непосредственно в блокчейне нецелесообразно и дорого. Более реалистичной является гибридная модель, при которой сами файлы хранятся в защищённом распределённом хранилище, а в блокчейн записываются только их хэши и метаданные, подтверждающие их целостность и историю доступа.

Для решения проблемы масштабирования необходимо применение распределённых файловых систем, таких как InterPlanetary File System (IPFS). IPFS обеспечивает контент-адресуемое хранение

файлов по криптографическим хешам, географически распределённую репликацию данных для обеспечения высокой доступности, версионирование медицинских записей с сохранением полной истории изменений [9].

Телемедицина и удалённый мониторинг пациентов / *Telemedicine and remote patient monitoring*

Возможности применения блокчейн не ограничиваются внутрибольничными и корпоративными решениями. Пандемия COVID-19 продемонстрировала важность телемедицинских решений и потребность в безопасной передаче данных между пациентами и медицинскими специалистами.

Базовые решения включают интеграцию IoT-устройств и носимых сенсоров для мониторинга состояния здоровья. Технология гарантирует, что эти данные будут записаны в реестр в неизменном виде непосредственно с устройства, что исключает возможность их подделки или случайного искажения, обеспечивая высокую достоверность информации для принятия клинических решений.

Смарт-контракты — это программируемые алгоритмы, которые автоматически исполняются при выполнении заранее определённых условий. В телемедицине они могут использоваться для автоматизации процессов, таких как проведение платежей за консультации или отправка уведомлений врачу при критических показателях с датчиков.

Во время телеконсультации врач может получить санкционированный доступ к полной и достоверной истории болезни, результатам анализов и данным с устройств мониторинга, независимо от того, в каком учреждении эти данные были созданы. Пациент при этом сохраняет полный контроль над своей информацией, используя приватные ключи для предоставления или отзыва доступа [7, 11]. С помощью смарт-контрактов гибко управляя доступом к своим данным, он может предоставить временный доступ лечащему врачу на период консультации или разрешить исследовательской организации использовать анонимизированные данные для научных целей. Все операции по доступу к информации фиксируются в блокчейне, обеспечивая полную прозрачность и подотчётность [10].

Динамическое управление информированным согласием пациентов / *Patient dynamic informed consent management*

Традиционные модели информированного согласия являются статичными и не адаптируются к изменяющимся потребностям лечения или исследований. Блокчейн-платформы позволяют реализовать динамическое согласие, где пациенты

через цифровой интерфейс могут детализированно и в ходе интерактивного взаимодействия управлять разрешениями на использование своих данных, позволяя ему принимать гранулированные решения по мере необходимости.

Для решения этих задач на базе Hyperledger Fabric была разработана, адаптированная для клинических исследований, система динамического согласия METORY [12]. Пациент изучает материалы исследования в приложении, после чего ставит электронную подпись; исследователь также подписывает форму. Каждый этап этого процесса записывается в реестр как транзакция.

При внесении изменений в протокол исследования создаётся новая версия формы согласия. Хеш-значение (уникальный цифровой отпечаток) документа записывается в блокчейн, это гарантирует, что даже малейшее изменение в документе будет зафиксировано, обеспечивая целостность данных. Участники получают уведомление и должны подписать обновлённую форму [13]. Так же платформа включает чат для общения между участником и исследователем во время и после процесса получения согласия.

Возможно дальнейшее развитие модели информированного согласия из динамического в проактивный (предикативный) режим: пациент не просто принимает/отклоняет запросы на изменения, а заранее определяет и формализует исчерпывающий набор правил и условий, при которых его медицинские данные могут быть использованы в будущем, даже для целей, которые ещё не сформулированы на момент дачи согласия. Технологической основой для реализации концепции «prosent» является синергия блокчейн-технологий и смарт-контрактов. Блокчейн обеспечивает необходимую инфраструктуру доверия, а смарт-контракты — логику для автоматизации. Так, например, платформа ConsentChain демонстрирует практическую реализацию динамического согласия для клинико-геномных исследований [13–15].

Сложности и вызовы внедрения блокчейн в медицине / *The challenges of implementing blockchain in medicine*

Фундаментальная характеристика блокчейна — неизменность — вступает в антагонизм с одним из прав субъекта данных, закреплённом в современных регуляторных актах — «правом на забвение». В контексте пациентоориентированной медицины это требует специализированных архитектурных решений. Например, расширенное применение распределённых файловых систем (IPFS) и хранение приложенных документов на сертифицированных серверах медицинских организаций, сопровождаемое возможностью удаления криптографического



ключа, делая практически невозможной расшифровку исходных записей. При этом в блокчейне сохраняется неизменяемая запись о самом факте существования данных и о транзакции, уничтожившей ключ доступа, обеспечивая полный аудиторский след, одновременно гарантируя целостность истории взаимодействий и удовлетворяя право пациента на забвение [16, 17]. Также необходимо учитывать, что участник, получавший ранее доступ к расшифрованному документу, имея его локальную копию, выходит за рамки контроля блокчейн-системы.

В условиях, когда конфиденциальность сохранённых данных необходимо обеспечить вперёд на десятилетия, принимая во внимание развитие цифровых технологий (в частности, квантовых вычислений, когда будущие атаки смогут ретроспективно дешифровать защищённые сегодня записи), внедрение устойчивого постквантового шифрования является необходимой превентивной мерой. Видится актуальным переход от современных стандартов, таких как эллиптическая криптография, к криптосистемам на основе решёток и других криптографических методов, таких как CRYSTALS-Kyber [18]. Криптография на основе решёток, помимо криптостойкости, имеет совместимость с гомоморфным шифрованием, позволяет производить произвольные вычисления непосредственно над зашифрованными данными, не производя их расшифрования.

Ещё один сдерживающим фактором являются высокие затраты энергетических ресурсов на проведение сложных вычислений (такие как механизм консенсуса Proof-of-Work, вызывающие экологические опасения. Ведётся разработка «зелёных» моделей с низким энергопотреблением, например механизм Proof-of-Stake, где право на создание нового блока предоставляется валидаторам пропорционально их доле владения (стейку) в сети, снижая вычислительные запросы и энергопотребление. В контексте медицинских консорциумных сетей, где участники известны и доверены, ещё большее распространение получили энергоэффективные алгоритмы Proof-of-Authority [19].

В практическом применении существующие МИС основаны на принципах централизованного управления данными, строгой иерархии компонентов и синхронном взаимодействии между модулями. Большинство медицинских учреждений в Российской Федерации эксплуатируют унаследованные информационные системы, характеризуются проприетарными форматами данных и ограниченными возможностями интеграции с внешними системами.

Правовая система России всё ещё находится на стадии адаптации к новым цифровым реалиям. Отсутствие чёткой законодательной базы, определяющей статус медицинских данных в блокчейн-системах,

и стандартов их использования является одним из главных препятствий [16]. Наблюдается конфликт между классическим юридическим определением документа как информации, зафиксированной на материальном носителе, и децентрализованной природой блокчейна. В распределённой сети медицинский документ — это не единичный файл, а логическая сущность, идентифицируемая своим криптографическим хешем, чьи реплики и их фрагменты могут одновременно существовать на множестве узлов. Информация находится в состоянии постоянной синхронизации и верификации, и её носителем выступает вся сеть целиком, а не отдельный её компонент. Правовой фокус должен сместиться с физической локализации на криптографическое доказательство целостности и происхождения информации [5, 16].

Технически наиболее интересной реализацией, для применения в условиях системы здравоохранения Российской Федерации, представляет платформа Мастерчейн, выполненная на базе Hyperledger Fabric и включённая в Реестр отечественного программного обеспечения. Она обеспечивающая работу алгоритмов ГОСТ-криптографии и архитектурные решения, соблюдающие ФЗ-152 «О персональных данных». Модульная структура платформы с использованием изолированных каналов и коллекций приватных данных позволяет создавать сложные консорциумные сети.

Заключение / Conclusion

Представленный анализ применения блокчейн-технологий в здравоохранении демонстрирует перспективность перехода от централизованных архитектур к пациентоориентированным моделям управления медицинскими данными. Блокчейн позволит обеспечить криптографически защищённую инфраструктуру для реализации динамического согласия пациентов, децентрализованного управления электронными медицинскими картами и безопасного обмена данными в телемедицинских приложениях.

Масштабируемость и производительность сегодня остаются важными ограничениями для широкого внедрения решений в российском здравоохранении. Публичные блокчейны, такие как Bitcoin и Ethereum, демонстрируют недостаточную пропускную способность для обработки миллионов медицинских транзакций в национальном масштабе. Консорциумные блокчейны, Мастерчейн и другие платформы на базе Hyperledger Fabric, представляют оптимальное решение, обеспечивающее баланс между децентрализацией и контролем при высокой производительности.

В краткосрочной перспективе необходимо акцентироваться на гибридной архитектуре, где медицинские данные и файлы большего объёма

хранятся в распределённых файловых системах типа IPFS, создавая экономически эффективную модель, а блокчейн обеспечивает согласованность ведения распределённого реестра, позволяя гарантировать целостность данных через криптографические хеши.

Долгосрочная безопасность медицинских данных требует превентивного перехода к постквантовым криптографическим алгоритмам. Внедрение криптосистем на основе решёток, таких как CRYSTALS-Kyber, обеспечит устойчивость к квантовым атакам при сохранении совместимости с гомоморфным шифрованием.

Отсутствие чёткой международной и отечественной законодательной базы, определяющей статус медицинских данных в блокчейн-системах, замедляет практическое внедрение технологии. Также необходима стандартизация протоколов взаимодействия между блокчейн-платформами и традиционными МИС.

Дальнейшее развитие должно концентрироваться на создании национальной консорциумной сети

с участием федеральных и региональных медицинских учреждений, страховых компаний, исследовательских организаций, других участников системы здравоохранения и контрагентов.

Помимо усиления контроля над личной медицинской информацией внедрение технологий повысит уровень доверия к медицинским сервисам за счёт прозрачности и возможности аудита.

Успешная имплементация блокчейн-решений в российском здравоохранении требует синхронизированного развития технологической инфраструктуры, правовой базы и непрерывного повышения компетенций медицинских специалистов в области цифровых технологий. Формирование нового типа медицинских специалистов — врачей-кибернетиков, интегрирующих клиническую экспертизу с глубокими знаниями информационных технологий, является задачей российского здравоохранения, решаемой, в том числе на базе ФГБОУ ВО «Ярославский государственный медицинский университет» Минздрава России и других ведущих медицинских вузов страны.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Участие авторов

Все авторы внесли существенный вклад в подготовку работы, прочли и одобрили финальную версию статьи перед публикацией. Потапов М. П. — планирование исследования, разработка концепции и постановка задачи, анализ; Костров С. А. — сбор, анализ, интерпретация данных, подготовка черновика рукописи; Кулибина О. В. — обработка материалов, коррекция текста, подготовка окончательной версии.

Финансирование

Работа выполнялась без спонсорской поддержки.

СВЕДЕНИЯ ОБ АВТОРАХ

Костров Сергей Александрович — ассистент кафедры медицинской кибернетики с курсом медицинской информатики, ФГБОУ ВО «Ярославский государственный медицинский университет», Ярославль, Российская Федерация

Автор, ответственный за переписку

e-mail: kosea@ysmu.ru

ORCID ID: 0009-0002-2936-7570

РИНЦ SPIN-код: 9186-8847

ADDITIONAL INFORMATION

Conflict of interests

The authors declare no conflict of interest.

Authors participation

All authors made a significant contribution to the preparation of the work, read and approved the final version of the article before publication. Potapov M. P. — research planning, concept development and problem statement, analysis; Kostrov S. A. — data collection, analysis, interpretation, preparation of the manuscript draft; Kulibina O. V. — materials processing, text correction, preparation of the final version.

Financing

The work was carried out without sponsorship.

ABOUT THE AUTHORS

Sergey A. Kostrov — assistant of the Department of Medical Cybernetics with a course in Medical Informatics, Yaroslavl State Medical University, Yaroslavl, Russian Federation

Corresponding author

e-mail: kosea@ysmu.ru

ORCID ID: 0009-0002-2936-7570

RSCI SPIN-code: 9186-8847

Потапов Максим Петрович — к. м. н., доцент, зав. кафедры медицинской кибернетики с курсом медицинской информатики, ФГБОУ ВО «Ярославский государственный медицинский университет», Ярославль, Российская Федерация

e-mail: mxp@mail.ru

ORCID ID: 0000-0002-4596-6517

РИНЦ SPIN-код: 2732-2232

Кулибина Ольга Валерьевна — к. м. н., доцент кафедры общей гигиены с экологией, ФГБОУ ВО «Ярославский государственный медицинский университет», Ярославль, Российская Федерация

e-mail: kulibinaov@mail.ru

ORCID ID: 0000-0002-6420-4745

РИНЦ SPIN-код: 6345-4443

Maxim P. Potapov — Cand. Sci. (Med.), Associate Professor, Head of the Department of Medical Cybernetics with a course in Medical Informatics, Yaroslavl State Medical University, Yaroslavl, Russian Federation

e-mail: mxp@mail.ru

ORCID ID: 0000-0002-4596-6517

RSCI SPIN-code: 2732-2232

Olga V. Kulibina — Cand. Sci. (Med.), Associate Professor of the Department of General Hygiene with Ecology, Yaroslavl State Medical University, Yaroslavl, Russian Federation

e-mail: kulibinaov@mail.ru

ORCID ID: 0000-0002-6420-4745

RSCI SPIN-code: 6345-4443

Список литературы / References

1. Elhussein A, Baymuradov U; NYGC ALS Consortium; Elhadad N, Natarajan K, Gürsoy G. A framework for sharing of clinical and genetic data for precision medicine applications. *Nat Med*. 2024 Dec;30(12):3578-3589. doi: 10.1038/s41591-024-03239-5.
2. Singh Y, Jabbar MA, Kumar Shandilya S, et al. Exploring applications of blockchain in healthcare: road map and future directions. *Front Public Health*. 2023 Sep 15;11:1229386. doi: 10.3389/fpubh.2023.1229386.
3. Siyal AA, Junejo AZ, Zawish M, et al. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography*. 2019;3(1):3. Doi: 10.3390/cryptography3010003.
4. Adanur Dedetürk B, Soran A, Bakir-Gungor B. Blockchain for genomics and healthcare: a literature review, current status, classification and open issues. *PeerJ*. 2021 Sep 30;9:e12130. doi: 10.7717/peerj.12130.
5. Гаппоев Р. А., Бурков В. О., Бастанова К. И. Блокчейн в здравоохранении: всесторонний обзор приложений и проблем безопасности. *Medicus*. 2025;4(70):81-88. EDN: NUFUVC. [Gappoev R. A., Burkov V. O., Bastanova K. I. Blockchain in healthcare: a comprehensive review of applications and security issues. *Medicus*. 2025;4(70):81-88. (In Russ.)].
6. Грачев В. Э., Сизова О. В. Перспективы использования технологии блокчейн в медицине. Сборник научных трудов вузов России "Проблемы экономики, финансов и управления производством". 2020;46:31-36. EDN: ODDEJU. [Grachev V. E., Sizova O. V. Prospects for the Use of Blockchain Technology in Medicine. Collection of scientific papers of Russian universities "Problems of Economics, Finance, and Production Management". 2020; 46:31-36. EDN: ODDEJU. (In Russ.)].
7. J. Hathaliya, R. Kakkar, R. Gupta, S. Tanwar and S. Agrawal, "Blockchain-based Access Control Mechanism for Patient Data Security in Telemedicine Systems," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489195.
8. K. K. Baseer, B. Jaya Naga Varma, B. Harish, E. Sravani, K. Y. Kumar and K. Varshitha, "Design and Implementation of Electronic Health Records using Ethereum Blockchain," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 784-791, doi: 10.1109/ICEARS56392.2023.10085012.
9. Kumar S, Bharti AK, Amin R. Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Security and Privacy*. 2021;e162. doi: 10.1002/spy2.162.
10. Mahdi SS, Ullah Z, Battineni G, et al. The Telehealth chain: a framework for secure and transparent telemedicine transactions on the blockchain. *Ir J Med Sci*. 2024 Oct;193(5):2129-2137. doi: 10.1007/s11845-024-03728-z. Epub 2024 Jun 3. Retraction in: *Ir J Med Sci*. 2025 Sep 25. doi: 10.1007/s11845-025-04091-3.
11. Vieira M, Velasco G, Carvalho S. A Decentralized Health Data Repository for Remote Patient Monitoring Using Blockchain and FHIR. In *Anais do VI Workshop em Blockchain: Teoria, Tecnologias e Aplicações*. 2023:85-98. Porto Alegre: SBC. doi:10.5753/wblockchain.2023.723.
12. Huh KY, Jeong SU, Moon SJ, et al. METORY: Development of a Demand-Driven Blockchain-Based Dynamic Consent Platform Tailored for Clinical Trials. *Frontiers in medicine*. 2022;9: 837197. Doi: 10.3389/fmed.2022.837197.
13. Lee AR, Koo D, Kim IK, et al. Opportunities and challenges of a dynamic consent-based application: personalized options for personal health data sharing and utilization. *BMC Med Ethics*. 2024 Aug 31;25(1):92. doi: 10.1186/s12910-024-01091-3.

14. Porsdam Mann S, Savulescu J, Ravaud P, Benchoufi M. Blockchain, consent and present for medical research. *J Med Ethics*. 2021 Apr 13;47(4):244-250. doi: 10.1136/medethics-2019-105963.
15. Albalwy F, Brass A, Davies A. A Blockchain-Based Dynamic Consent Architecture to Support Clinical Genomic Data Sharing (ConsentChain): Proof-of-Concept Study. *JMIR Medical Informatics*. 2021;9(11):e27816.
16. Заколдаев Д.А., Ямщиков Р.В., Ямщикова Н.В. Технология блокчейн в России: достижения и проблемы. *Российский социально-гуманитарный журнал*. 2018;2:93-107. Doi: 10.18384/2224-0209-2018-2-889.
17. Mackey TK, Kuo TT, Gummadi B, et al. 'Fit-for-purpose?' - challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Med*. 2019 Mar 27;17(1):68. doi: 10.1186/s12916-019-1296-7.
18. Yadav V, Hajarnis P, Minu R I. Unlocking Clinical Trial Efficiency and Security with Blockchain and Quantum Technology. In *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)*. 2025, January (pp. 161-165). IEEE.
19. Ahirao P, Shaikh B, Wahedna RZ. Blockchain Technology and Data Privacy: A Comprehensive Review and Future Perspective. In *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*. 2024, October (pp. 1-7). IEEE.