# БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ ЗАПИСЕЙ: ФЕДЕРАТИВНЫЙ БЛОКЧЕЙН И ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

С. А. Костров ✉, М. П. Потапов

Ярославский государственный медицинский университет, Ярославль, Россия

Статья посвящена анализу потенциала технологии распределенного реестра, в частности федеративного блокчейна, как основы для создания защищенной, прозрачной и управляемой пациентом экосистемы медицинских данных. Рассмотрена гибридная архитектура, при которой блокчейн используется для хранения неизменяемых метаданных и хешей, а объемные файлы (например, диагностические изображения) размещаются во внешних децентрализованных хранилищах, что гарантирует целостность данных без перегрузки сети. Ключевым аспектом исследования является анализ долгосрочных угроз, связанных с развитием квантовых компьютеров, которые ставят под угрозу существующие криптографические стандарты. Подчеркивается необходимость перехода на постквантовую криптографию для обеспечения будущей безопасности медицинских данных. Проведен сравнительный анализ ведущих мировых (CRYSTALS-Dilithium, Falcon) и перспективных отечественных («Гиперикум», «Шиповник») квантово-устойчивых алгоритмов криптографии.

**Ключевые слова:** блокчейн, постквантовая криптография, электронная медицинская запись, распределенный реестр, федеративные вычисления, биоэтика

**Вклад авторов:** М. П. Потапов — планирование исследования, анализ, редактирование; С. А. Костров — сбор, анализ, интерпретация данных, подготовка черновика рукописи.

✉ **Для корреспонденции:** Сергей Александрович Костров
Ул. Революцилнная, д. 5, г. Ярославль, 150000, Россия; kosea@ysmu.ru

**Статья поступила:** 13.08.2025 **Статья принята к печати:** 18.10.2025 **Опубликована онлайн:** 03.11.2025

**DOI:** 10.24075/medet.2025.019

# SECURITY OF ELECTRONIC HEALTH RECORDS: FEDERATED BLOCKCHAIN AND POST-QUANTUM CRYPTOGRAPHY

Kostrov SA ✉, Potapov MP

Yaroslavl State Medical University, Yaroslavl, Russia

The article presents a review on the potential of the distributed ledger technology (DLT), particularly federated blockchain, that can be used to create a secure, transparent and patient-managed ecosystem of medical data. The hybrid architecture reviewed uses the blockchain to store immutable metadata and hashes, and manage large amounts of data (for example, diagnostic images) on external cloud storage, which ensures the integrity of data without network overloading. The key aspect of the research is to analyze long-term threats posed by quantum computing that makes current cryptographic standards vulnerable. It is stressed that adoption of post-quantum cryptography (PQC) is required to ensure future security of medical data. An analysis was carried out to compare the leading global (CRYSTALS-Dilithium, Falcon) and Russian (Hypericum, Shipovnik) post-quantum cryptography algorithms.

**Keywords**: blockchain, post-quantum cryptography, electronic health record, distributed ledger, federated computing, bioethics

**Author contribution:** Potapov MP — research planning, analysis, editing; Kostrov SA — data collection, analysis and interpretation, preparing a draft manuscript.

✉ **Correspondence should be addressed:** Sergey A. Kostrov
Revolutsionnaya St., 5, Yaroslavl, 150000, Russia; kosea@ysmu.ru

**Received:** 13.08.2025 **Accepted:** 18.10.2025 **Published online:** 03.11.2025

**DOI:** 10.24075/medet.2025.019

В эпоху цифровизации здравоохранения хранение и управление электронными медицинскими записями стали важными не только с точки зрения техники, но и биоэтики. Актуальность этой проблемы обусловлена экспоненциальным ростом объемов медицинских данных, генерируемых в ходе диагностики и лечения, в том числе в ходе телемедицинских консультаций и носимыми устройствами. Основную массу составляют медицинские изображения, геномика и молекулярные исследования. По оценкам Всемирной организации здравоохранения, на здравоохранение приходится треть мировых данных, измеряемых зетабайтами [1]. Это усиливает риски утечек и несанкционированного доступа, поэтому объекты здравоохранения в экономически развитых странах отнесены к критической информационной инфраструктуре. Глобальные экономические потери от кибериндидентов в 2025 г., по прогнозам, достигнут 10 триллионов долларов [2, 3].

Для пациентов становятся важными не только качество и полнота медицинской информации, но и вопросы информационной безопасности, этические стандарты приватности, контроля доступа и использования данных. Традиционные централизованные системы хранения данных, применяемые в медицинских информационных системах, подвержены рискам, связанным с единой точкой отказа.

Наряду с внедрением технологий искусственного интеллекта, квантовыми вычислениями, усиленной криптографией большие перспективы для развития представляют блокчейн-технологии, обеспечивающие децентрализацию, криптографическую защиту и гибкую безопасность, контролируемую в том числе со стороны индивида.

Целью данной публикации является знакомство медицинского сообщества с технологией распределенного

реестра для хранения медицинских записей, в свете вопросов информационной безопасности, с акцентом на обеспечение требуемого уровня конфиденциальности посредством алгоритмов криптографии.

## МАТЕРИАЛЫ И МЕТОДЫ

В рамках подготовки статьи был реализован подход, включающий поиск в ведущих отечественных и зарубежных библиографических ресурсах, таких как eLibrary и PubMed, с использованием специализированных платформ для аналитики научных публикаций, включая Semantic Scholar, Consensus и Elicit, критический анализ и отбор релевантных источников. Включение публикаций осуществлялось по следующим критериям: соответствие изучаемой тематике, публикация в период с 2018 по 2025 г., наличие полного текста на русском или английском языках. Первичная оценка релевантности источников проводилась на основании аннотаций, с акцентом на соответствие тематике применения блокчейн в здравоохранении.

Корректность итоговых материалов проверялась коллективной экспертной рецензией авторов. Суммаризация и грамматическая корректура текста выполнялись с использованием OpenAI ChatGPT-4.1 и Google Gemini 2.5.

## РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

Среди населения широко распространено ошибочное представление о том, что понятие «блокчейн» является синонимом криптовалют, в то время как это лишь один из вариантов применения технологии. Главная ценность данной технологии заключается в обеспечении неизменяемости, проверяемости, доступности и защищенности записей, независимо от того, где она применяется: в экономике, логистике, управлении или медицине.

В отличие от традиционных централизованных систем, где контроль над данными принадлежит медицинским учреждениям, блокчейн предоставляет пациентам определенную автономию в управлении своими медицинскими записями [4].

Пользователь становится держателем закрытого криптографического ключа, используя который пациенты получают возможность:

- определять условия использования данных через смарт-контракты;
- отслеживать все операции с их данными благодаря неизменяемости блокчейна;
- отзывать разрешения на доступ в любой момент.

Основное свойство блокчейна заключено в невозможности несанкционированной модификации или утери данных, так как все транзакции фиксируются в неизменяемом реестре [4].

По видам технологий распределенного реестра, способных применяться для хранения медицинских записей, можно выделить публичные, приватные и федеративные (консорциумные) блокчейны. Публичные системы (не требующие разрешений, permissionless) — полностью децентрализованные сети с открытым доступом, где данные доступны всем участникам сети [5]. Приватные системы находятся под контролем одной организации, применимы к задачам, требующим централизованное управление и ускоренный консенсус, что, с одной стороны, обеспечивает быстрые транзакции и оптимизацию под клинические информационные потоки, более быстрое внедрение политик доступа, аудита и контроля соответствия, а с другой — проявляются минусы централизованных систем, риски сбоев и злоупотреблений, сложности масштабирования между учреждениями и регионами [6].

Федеративные (консорциумные, разрешенные, permissioned) блокчейны представляют собой сети с ограниченным доступом, управляемые заранее определенным кругом участников, например, медицинскими организациями, лабораториями и регуляторными органами, обеспечивая баланс между децентрализацией и контролем доступа. Федеративные блокчейны позволяют интегрировать различные медицинские учреждения в единую систему, обеспечивая совместимость и безопасность обмена медицинскими записями.

Также федеративные блокчейны обеспечивают более высокую скорость обработки транзакций и больший пропускной поток, так как количество узлов-валидаторов ограничено и контролируется. В публичных сетях скорость ниже из-за необходимости консенсуса среди большого и неизвестного числа участников [5].

В практике хранения электронных медицинских записей возможно использование таких технологических платформ, как Hyperledger Fabric. Они сочетают в себе смарт-контракты, контроль доступа на основе атрибутов (ABAC) и распределенное хранение данных через IPFS (файловая система) [7].

В российской практике наибольшее развитие среди проектов с технологией федеративного блокчейна получил продукт «Мастерчейн» Ассоциации ФинТех, став первой сертифицированной платформой, поддерживающей отечественные средства криптографической защиты информации, активно внедряется в банковскую сферу. В 2021 г. учрежден первый в России блокчейн-оператор «Системы распределенного реестра». Обрабатываемая в сети информация обладает юридической значимостью в России. С 2023 г. применяется ФНС России для хранения машиночитаемых доверенностей [8].

Публичные (общедоступные) блокчейны — такие как Bitcoin, Ethereum и др. — не являются предметом выбора для прямого применения в здравоохранении, их можно использовать для хранения хеш-сумм и ссылок на зашифрованные данные, частично решая вопрос конфиденциальности [7].

Прозрачность публичных блокчейнов — ценное преимущество для финансовых и логистических приложений, но оборачивается недостатком в медицине: даже если данные зашифрованы, уже сам факт их размещения в открытой сети может рассматриваться как утечка информации, поскольку, будучи сохраненными, они могут быть дешифрованы в дальнейшем с применением средств, не доступных в настоящее время [7, 9]. Например, широко применяемые методы криптографии на эллиптических кривых ECDSA, считающиеся высокозащищенными в традиционных системах, могут быть взломаны с применением алгоритма Шора, способного решить задачу вычисления закрытого ключа по открытому на квантовом компьютере за полиномиальное время [10].

Построение масштабируемого квантового компьютера, способного запускать алгоритм Шора с достаточным количеством кубитов (около 2000) и низким уровнем ошибок, приведет к компрометации механизмов

безопасности. Для систем здравоохранения необходимо обеспечение долгосрочной цифровой безопасности. В научном и технологическом сообществе ведутся активные разработки, направленные на переход к постквантовой (квантовоустойчивой) криптографии, схемам распределения ключей и новым протоколам консенсуса, не зависящим от уязвимых к алгоритму Шора математических задач [10].

Прежде всего, такие постквантовые алгоритмы основываются на так называемых решетках (lattice-based cryptography), стойкость которых обеспечивается сложностью математических задач (например, задача поиска самого короткого вектора (SVP) и задача обучения с ошибками (LWE)), допускающих только экспоненциальные атаки даже на квантовом компьютере. Типичными алгоритмами могут являться [11, 12]:

- NTRUEncrypt — один из первых и наиболее известных;
- CRYSTALS-Dilithium — современная легковесная схема цифровой подписи, рекомендованная в 2024 г. Национальным институтом стандартов и технологий США (NIST) и предлагаемая для замены ECDSA в качестве основного стандарта, демонстрирует оптимальный баланс между скоростью генерации ключей, подписания и проверки, а также умеренными размерами ключей и подписей [12];
- Falcon — рекомендуется NIST в качестве дополнительного выбора для специализированных случаев, когда важна максимальная компактность подписей и ключей, а также еще более высокая скорость проверки подписи [11].

Помимо криптографии на решетках определенный интерес представляют решения, основанные на изогении эллиптических кривых (isogeny-based cryptography), морфизме пути между двумя различными эллиптическими кривыми. Одним из известных алгоритмов на основе изогений был SIKE (Supersingular Isogeny Key Encapsulation), также участвовавший в конкурсе постквантовой стандартизации NIST. Однако в 2022 г. были найдены алгоритмы атаки, которые полностью его скомпрометировали. В данное время разработка прочих алгоритмов (SQISign — Short Quaternion and Isogeny Signature, CSIDH — Commutative Supersingular Isogeny Diffie-Hellman и др.) находится на уровне академических исследований, и они не готовы для широкого практического применения [13].

Kyber — передовой алгоритм постквантового шифрования, выбранный Национальным институтом стандартов и технологий США (NIST) в качестве основного стандарта для механизмов инкапсуляции ключей (KEM) в эпоху квантовых вычислений [12].

Отечественные разработки, к сожалению, пока существенно отстают от мировых стандартов. Национальные системы стандартов, включая ГОСТ 34.10-2012 и ГОСТ 34.10-2018, основываются также на операциях с группой точек эллиптической кривой и являются уязвимыми к квантовому криптоанализу. Академические исследования и разработки отечественных постквантовых алгоритмов еще ведутся [14–17]:

«Гиперикум» (Hypericum) — алгоритм цифровой подписи, разработанный специалистами компании QApp в рамках деятельности Технического комитета 26 Росстандарта (ТК 26), ведутся работы по использованию российской стандартизированной хеш-функции Стрибог (Streebog) для реализации постквантовой схемы цифровой подписи SPHINCS+ [17].

«Шиповник» — алгоритм, разработанный компанией «Криптонит», основан на сложности задачи декодирования случайного линейного кода. На данный момент неизвестны эффективные алгоритмы решения ни на классическом компьютере, ни на квантовом, теоретически невозможно подобрать даже на компьютерах будущего с миллионами рабочих кубитов. Однако большой размер подписи препятствует практическому применению в блокчейне.

Также интерес представляет алгоритм, представленный на конференции РусКрипто'2025 — «Облепиха», основан на теории решеток (задача LIP) и использует уменьшение размера подписи при сохранении высокого уровня стойкости.

«Гиперикум» и «Шиповник» являются кандидатами на включение в государственные стандарты криптографии России, имеются открытые реализации на языке C, доступные в том числе на GitHub: https://github.com/QAPP-tech/shipovnik_tc26 и https://github.com/QAPP-tech/hypericum_tc26 (табл.)

Помимо шифрования, применяемые в здравоохранении разрешительные (permissioned) системы, позволяют обеспечивать гибкий контроль доступа. На практике применяются гибридные модели, сочетающие ролевые и атрибутивные подходы (RBAC и ABAC), многоуровневые системы контроля доступа.

Ролевой контроль доступа (RBAC) — пациенты могут назначать различные роли (врач, медсестра, исследователь) с соответствующими уровнями доступа [18].

Атрибутивный контроль доступа (ABAC) — позволяет создавать более гибкие политики доступа на основе множества атрибутов: временных рамок, географического местоположения, типа данных и цели использования [18].

Технологические решения строятся на многоуровневых архитектурах, где пользовательский интерфейс интуитивно интегрирует управление разрешениями и просмотр медицинских данных. Уровень смарт-контрактов реализует бизнес-логику, включая выдачу, изменение и отзыв согласий, а также мониторинг всех операций.

Каждая транзакция, будь то запись о визите к врачу, выдача рецепта, результаты анализов, заключения и выписки может быть зафиксирована в цепи блоков, создавая неопровержимый и хронологически выверенный аудиторский след. Однако большая проблема заключается в том, что блокчейн не предназначен для хранения больших файлов. Попытка записать в блокчейн диагностические изображения (МРТ, КТ) или другие объемные данные приведет к экспоненциальному росту размера реестра, снижению производительности сети и непомерно высоким транзакционным издержкам [19].

В типовом сценарии блокчейн содержит хеши и метаданные, обеспечивающие неизменяемость и прозрачность транзакций, в то время как объемные медицинские файлы размещаются в децентрализованных файловых системах (например, IPFS). Такой подход гарантирует как высокую доступность данных, так и их целостность. Если файл в хранилище будет изменен хотя бы на один бит, его хеш изменится и перестанет соответствовать записи в блокчейне, что немедленно сделает фальсификацию очевидной при проведении проверки [5, 19].

Публичный ключ пациента функционирует как адрес или идентификатор в сети, который можно свободно передавать другим участникам, например, медицинским

**Таблица.** Сравнение постквантовых алгоритмов криптографии

| Характеристика | Гиперикум | Шиповник | Falcon | CRYSTALS-Dilithium |
|---|---|---|---|---|
| Разработчик | QApp (Россия) | Криптонит (Россия) | Международная группа | Международная группа |
| Криптографическая основа | Хеш-функции (схема SPHINCS+) | Теория кодирования (на базе протокола Штерна) | Решётки NTRU | Решётки (LWE) |
| Вычисляемая задача | Хеш-функции ГОСТ «Стрибог» | Декодирование случайного линейного кода | Поиск коротких векторов в NTRU-решётка | Обучение с ошибками в кольцах |
| Открытый ключ (байт) | 64 | 512 | 897 (Falcon-512)<br>1793 (Falcon-1024) | 1312 (Dilithium2)<br>1952 (Dilithium3)<br>2592 (Dilithium5) |
| Размер подписи (байт) | 18292–58460 | ~ 600000 | 752 (Falcon-512)<br>1462 (Falcon-1024) | 2420 (Dilithium2)<br>3293 (Dilithium3)<br>4595 (Dilithium5) |
| Производительность | Подпись и верификация относительно медленные | Быстрая генерация ключей и проверка подписи | Медленная генерация ключей при быстрой проверке подписи | Быстрая генерация ключей и проверка подписи |
| Особенности | Очень большие размеры подписи, медленная работа | Долгое создание подписи | Самые компактные подписи, высокая производительность, сложность реализации | Сбалансированные характеристики, простота реализации, хорошая производительность |

учреждениям или страховым компаниям, для запроса доступа к данным. Однако любая транзакция, включая предоставление разрешения на просмотр или изменение медицинских записей, должна быть подписана с помощью соответствующего приватного ключа [18].

Несмотря на преимущества, такая система возлагает на пациента большую ответственность. Критическим риском является утрата приватного ключа. В полностью децентрализованных (публичных) блокчейн-системах утеря приватного ключа необратима и равносильна полной и безвозвратной потере доступа к своим медицинским записям и контролю над ними. В федеративном блокчейне могут быть реализованы протоколы восстановления личности и ключей. Консорциум может выступать в роли доверенного арбитра: если пациент теряет свой ключ, он может пройти процедуру верификации личности, может быть выдан новый ключ для доступа к записям. Типичным является применение схем с мультиподписью, где для восстановления доступа требуется согласие нескольких доверенных сторон.

Необходимо непрерывное повышение цифровой грамотности: эффективное управление ключами, понимание принципов функционирования блокчейн-платформ остаются проблемой для значительной части врачей и пациентов. Низкий уровень осведомленности способствует формированию цифрового неравенства и снижает доступность новых решений как для отдельных граждан, так и для отдельных стран или регионов.

## ВЫВОДЫ

Технология распределенного реестра, в частности федеративный (консорциумный) блокчейн, представляет собой перспективное решение, способное кардинально повысить уровень защиты данных, обеспечить их целостность и предоставить пациентам контроль над своей информацией. Необходим баланс между полной децентрализацией публичных сетей и централизованным контролем приватных систем. Управление консорциумом доверенных участников (медицинскими организациями, лабораториями, страховыми компаниями, государственными регуляторами) соответствует структуре системы здравоохранения, а также способствует высокой скорости транзакций и пропускной способности. Гибридное хранение в децентрализованных файловых хранилищах и применение блокчейна для хранения хэшей и метаданных обеспечивает целостность без перегрузки сети.

Российские разработки, такие как платформа «Мастерчейн», уже демонстрируют потенциал этой технологии и ее юридическую значимость в банковской сфере и перспективы применения в здравоохранении и смежных областях.

Существующие криптографические стандарты, включая ГОСТ, уязвимы для квантового криптоанализа. Поэтому ключевой перспективой и одновременно вызовом становится переход на постквантовую криптографию. Разработка и стандартизация квантово-устойчивых алгоритмов, таких как международные CRYSTALS-Dilithium и Falcon, а также отечественные «Гиперикум» и «Шиповник», являются необходимым условием для построения по-настоящему защищенных медицинских систем будущего. Для масштабного практического применения необходимы совершенствование законодательства в области защиты данных, актуализация ГОСТов, сертификация средств криптографической защиты информации.

Успешное внедрение этих технологий зависит от решения не столько технических, сколько социальных и организационных задач, прежде всего — повышения цифровой грамотности врачей и пациентов. Без понимания принципов работы блокчейна и ответственного управления криптографическими ключами невозможно в полной мере реализовать его преимущества и избежать цифровых рисков.

**Литература**


1. Meeting Abstracts from the 5th National Big Data Health Science Conference. BMC Proceedings. 2024; 18(9). DOI: 10.1186/s12919-024-00292-3.
2. Broklyn, Peter and Shad, Ralph and Egon, Axel, The Evolving Thread Landscape Pf Ai-Powered Cyberattacks: A Multi-Faceted Approach to Defense and Mitigate. July 18, 2024. DOI: 10.2139/ssrn.4904878.
3. Dirksen S and Korah J. "GUARD: Graph-based Unknown Attack Recognition and Detection,"2024 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2024; 1–6. DOI: 10.1109/WIFS61860.2024.10810721.
4. Porsdam Mann S, Savulescu J, Ravaud P, & Benchoufi M. Blockchain, consent and prosent for medical research. Journal of medical ethics, 2020; 47(4): 244–250. Advance online publication. DOI: 10.1136/medethics-2019-105963.
5. Litvin AA, Korenev SV, Knyazeva EG, Litvin V. The Possibilities of Blockchain Technology in Medicine (Review). Modern Technologies in Medicine. 2019; 11(4): 191–199. DOI: 10.17691/stm2019.11.4.21. — EDN FKRPUE.
6. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC medical informatics and decision making, 2022; 22(1): 80. DOI: 10.1186/s12911-022-01815-8.
7. Hasnain M, et al. The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records. Frontiers in Public Health. 2023; 11. DOI: 10.3389/fpubh.2023.1272787.
8. Андрианова Н. Г. Основные направления использования технологии блокчейн в финансовой сфере. Аграрное и земельное право. 2024; 4 (232): 109–111. DOI: 10.47643/1815-1329_2024_4_109.
9. Liu C, Xiang F, Sun Z. Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain. Security and Communication Networks. 2022; 1. DOI: 10.1155/2022/8497628.
10. Huang Y, et al. Choosing Coordinate Forms for Solving ECDLP Using Shor's Algorithm. arXiv preprint arXiv:2502.12441. 2025.
11. Dam D -T, Nguyen T -H, Tran T -H, Le D -H, Hoang T -T and Pham C -K. "High-Efficiency Multi-Standard Polynomial Multiplication Accelerator on RISC-V SoC for Post-Quantum Cryptography," in IEEE Access. 2024; 12: 195015–195031, DOI: 10.1109/ACCESS.2024.3520592.
12. Li' A, Li Z, Tang J and Lu Y. "KDA: Kyber and Dilithium Accelerator for CRYSTALS Suite of Post-Quantum Cryptography in Hybrid Multipath Delay Commutator Pipelined Architecture". 2024 IEEE Asian Solid-State Circuits Conference (A-SSCC). Hiroshima. Japan. 2024; 1–3. DOI: 10.1109/A-SSCC60305.2024.10848993.
13. Castryck W, Decru T. (2023). An Efficient Key Recovery Attack on SIDH. In: Hazay C, Stam M. (eds) Advances in Cryptology — EUROCRYPT 2023. EUROCRYPT 2023. Lecture Notes in Computer Science. 2023; 14008. Springer, Cham. DOI: 10.1007/978-3-031-30589-4_15.
14. Komarova A, Korobeynikov A. Combined authentication schemes with increasing level of resistance and methods for improving the security of electronic signature schemes: Kombinirovannye skhemy autentifikacii s povyshennym urovnem stojkosti i metody povysheniya bezopasnosti skhem elektronnoj. Podpisi. Proceedings of the 12th International Conference on Security of Information and Networks. 2019; 1–8.
15. Назаренко, А. П., Дмитриев Е. В. Современное состояние постквантовой криптографии в России и за рубежом. Системы синхронизации, формирования и обработки сигналов. 2021; 12(6): 77–83. EDN FNKIVP.
16. Урбан Н. А., Мельникова Е. А. Применение алгоритмов на решётках в постквантовой криптографии. Современные информационные технологии и ИТ-образование. 2024; 20(1): 27–33. DOI: 10.25559/SITITO.020.202401.27-33. EDN BNHDRO.
17. Kiktenko EO, et al. SPHINCS + digital signature scheme with GOST hash functions. arXiv. 2019. DOI: 10.1063/5.0011441.
18. Guo H, et al. Access control for electronic health records with hybrid blockchain-edge architecture. 2019 IEEE international conference on blockchain (Blockchain). IEEE. 2019; 44–51. DOI: 10.48550/arXiv.1906.01188.
19. Rajasekharan A and Koshy R. "EMRChain: Electronic Medical Records Management System using Blockchain". 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) Pune. India. 2024; 1–6. DOI: 10.1109/ICBDS61829.2024.10837244.


**References**


1. Meeting Abstracts from the 5th National Big Data Health Science Conference. BMC Proceedings. 2024; 18(9). DOI: 10.1186/s12919-024-00292-3.
2. Broklyn, Peter and Shad, Ralph and Egon, Axel, The Evolving Thread Landscape Pf Ai-Powered Cyberattacks: A Multi-Faceted Approach to Defense and Mitigate. July 18, 2024. DOI: 10.2139/ssrn.4904878.
3. Dirksen S and Korah J. "GUARD: Graph-based Unknown Attack Recognition and Detection,"2024 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2024; 1–6. DOI: 10.1109/WIFS61860.2024.10810721.
4. Porsdam Mann S, Savulescu J, Ravaud P, & Benchoufi M. Blockchain, consent and prosent for medical research. Journal of medical ethics, 2020; 47(4): 244–250. Advance online publication. DOI: 10.1136/medethics-2019-105963
5. Litvin AA, Korenev SV, Knyazeva EG, Litvin V. The Possibilities of Blockchain Technology in Medicine (Review). Modern Technologies in Medicine. 2019; 11(4): 191–199. DOI: 10.17691/stm2019.11.4.21. — EDN FKRPUE.
6. Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): a qualitative study from physicians' perspectives. BMC medical informatics and decision making, 2022; 22(1): 80. DOI: 10.1186/s12911-022-01815-8.
7. Hasnain M, et al. The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records. Frontiers in Public Health. 2023; 11. DOI: 10.3389/fpubh.2023.1272787.
8. Andrianova NG. Osnovnyye napravleniya ispol'zovaniya tekhnologiy v finansovoy sfere. Agrarnoye i zemel'noye pravo. 2024; 4 (232): 109–111. DOI: 10.47643/1815-1329_2024_4_109109-111. Russian.
9. Liu C, Xiang F, Sun Z. Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain. Security and Communication Networks. 2022; 1. DOI: 10.1155/2022/8497628.
10. Huang Y, et al. Choosing Coordinate Forms for Solving ECDLP Using Shor's Algorithm. arXiv preprint arXiv:2502.12441. 2025.
11. Dam D -T, Nguyen T -H, Tran T -H, Le D -H, Hoang T -T and Pham C -K. "High-Efficiency Multi-Standard Polynomial Multiplication Accelerator on RISC-V SoC for Post-Quantum Cryptography", in IEEE Access. 2024; 12: 195015–195031. DOI: 10.1109/ACCESS.2024.3520592.
12. Li' A, Li Z, Tang J and Lu Y. "KDA: Kyber and Dilithium Accelerator for CRYSTALS Suite of Post-Quantum Cryptography in Hybrid Multipath Delay Commutator Pipelined Architecture". 2024 IEEE Asian Solid-State Circuits Conference (A-SSCC). Hiroshima. Japan. 2024; 1–3. DOI: 10.1109/A-SSCC60305.2024.10848993.
13. Castryck W, Decru T. (2023). An Efficient Key Recovery Attack on SIDH. In: Hazay C, Stam M. (eds) Advances in Cryptology — EUROCRYPT 2023. EUROCRYPT 2023. Lecture Notes in Computer Science. 2023; 14008. Springer, Cham. DOI: 10.1007/978-3-031-30589-4_15.
14. Komarova A, Korobeynikov A. Combined authentication schemes with increasing level of resistance and methods for improving

the security of electronic signature schemes: Kombinirovannye skhemy autentifikacii s povyshennym urovnem stojkosti i metody povysheniya bezopasnosti skhem elektronnoj. Podpisi. Proceedings of the 12th International Conference on Security of Information and Networks. 2019; 1–8.

15. Nazarenko AP, Dmitriyev Ye V. Sovremennoye sostoyaniye postkvantovoy kriptografii v Rossii i za rubezhom. Sistemy sinkhronizatsii, formirovaniya i obrabotki signalov. 2021; 12(6): 77–83. EDN FNKIVP. Russian.
16. Urban NA, Mel'nikova Ye A. Primeneniye algoritmov na reshotkakh v postkvantovoy kriptografii. Sovremennyye informatsionnyye tekhnologii i IT-obrazovaniye. 2024; 20(1): 27–33. DOI: 10.25559/SITITO.020.202401.27-33. EDN BNHDRO. Russian.
17. Kiktenko EO, et al. SPHINCS + digital signature scheme with GOST hash functions. arXiv. 2019. DOI: 10.1063/5.0011441.
18. Guo H, et al. Access control for electronic health records with hybrid blockchain-edge architecture. 2019 IEEE international conference on blockchain (Blockchain). IEEE. 2019; 44–51. DOI: 10.48550/arXiv.1906.01188.
19. Rajasekharan A and Koshy R. "EMRChain: Electronic Medical Records Management System using Blockchain". 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) Pune. India. 2024; 1–6. DOI: 10.1109/ICBDS61829.2024.10837244.