

УДК 004.94:004.056.55

DOI: [10.26102/2310-6018/2026.61.10.008](https://doi.org/10.26102/2310-6018/2026.61.10.008)

Архитектурное размещение постквантовых цифровых подписей ML-DSA и SLH-DSA в блокчейн-системах

А.В. Родионов✉

Байкальский государственный университет, Иркутск, Российская Федерация

Резюме. Переход распределенных реестров к постквантовым цифровым подписям обычно сводят к замене алгоритма подписи. Однако в блокчейн-системе подпись определяет не только криптографическую проверку подлинности, но и размер транзакции, плотность блока, скорость роста цепочки, пропускную способность и время проверки блока. В работе экспериментально оценены архитектурные последствия размещения постквантовых подписей ML-DSA и SLH-DSA на четырех уровнях, а именно подписи каждой транзакции, гибридной подписи транзакции, подписи заголовка блока узлом-валидатором и подписи контрольной точки. Исследованы двадцать три схемы, включая две классические, три варианта ML-DSA, двенадцать вариантов SLH-DSA и шесть гибридных схем; выполнено шесть тысяч девятьсот измерений операций формирования ключей, формирования и проверки подписи, дополненных имитационным моделированием плотности блока и времени его проверки. Показано, что даже наиболее компактная постквантовая схема при размещении подписи в каждой транзакции снижает плотность блока и пропускную способность почти в пятнадцать раз, а для полного семейства хеш-основанных схем падение плотности достигает от тридцати до ста девяноста трех раз, тогда как при подписи заголовка блока или контрольной точки прирост роста цепочки не превышает полутора процентов. Основной результат состоит в том, что уровень архитектурного размещения подписи является самостоятельным фактором пригодности постквантовой схемы, поскольку одна и та же схема может быть неприемлема на уровне транзакции и практически применима на уровне блока или контрольной точки.

Ключевые слова: постквантовая криптография, цифровая подпись, блокчейн, распределенный реестр, цифровая подпись на основе решеток, цифровая подпись на основе хэш-функций, плотность блока.

Для цитирования: Родионов А.В. Архитектурное размещение постквантовых цифровых подписей ML-DSA и SLH-DSA в блокчейн-системах. *Моделирование, оптимизация и информационные технологии*. 2026;14(10). URL: <https://moitvvt.ru/ru/journal/article?id=2558>
DOI: 10.26102/2310-6018/2026.61.10.008

Architectural placement of post-quantum digital signatures ML-DSA and SLH-DSA in blockchain systems

A.V. Rodionov✉

Baikal State University, Irkutsk, the Russian Federation

Abstract. The migration of distributed ledgers to post-quantum digital signatures is commonly reduced to replacing the signature algorithm. In a blockchain system, however, the signature governs not only cryptographic authentication but also the transaction size, block density, chain growth rate, throughput and block verification time. This study experimentally assesses the architectural consequences of placing the post-quantum signatures ML-DSA and SLH-DSA at four levels, namely per-transaction signing, hybrid per-transaction signing, signing of the block header by a validator node, and signing of a checkpoint. Twenty-three schemes were examined, including two classical schemes, three ML-DSA variants, twelve SLH-DSA variants and six hybrid schemes; six thousand nine hundred measurements of key generation, signing and verification were performed and complemented by a simulation of block

density and verification time. It is shown that even the most compact post-quantum scheme, when the signature is placed in every transaction, reduces block density and throughput almost fifteenfold, while for the full family of hash-based schemes the density drop reaches thirty to one hundred ninety-three times, whereas signing the block header or a checkpoint increases chain growth by no more than one and a half percent. The principal result is that the architectural level of signature placement is an independent factor of the suitability of a post-quantum scheme, since the same scheme may be unacceptable at the transaction level yet practically applicable at the block or checkpoint level.

Keywords: post-quantum cryptography, digital signature, blockchain, distributed ledger, lattice-based signature, hash-based signature, block density.

For citation: Rodionov A.V. Architectural placement of post-quantum digital signatures ML-DSA and SLH-DSA in blockchain systems. *Modeling, Optimization and Information Technology*. 2026;14(10). (In Russ.). URL: <https://moitvvt.ru/ru/journal/article?id=2558> DOI: 10.26102/2310-6018/2026.61.10.008

Введение

Блокчейн-системы строят доверие к распределенному реестру на цифровых подписях и хеш-функциях¹. Развитие квантовых вычислений ставит под угрозу классические схемы цифровой подписи, стойкость которых опирается на сложность дискретного логарифмирования и разложения на множители. Алгоритм Шора при наличии масштабируемого квантового вычислителя позволяет восстанавливать закрытые ключи схем на эллиптических кривых и схем на основе RSA [1]. Для распределенных реестров эта угроза имеет особый характер, поскольку цепочка блоков по своему назначению хранит подписанные записи неограниченно долго, и компрометация алгоритма подписи задним числом обесценивает уже зафиксированную историю. Уязвимость действующих блокчейн-сетей к квантовым атакам показана в ряде работ [2, 3].

Ответом на угрозу стала стандартизация постквантовых схем². Решеточная схема ML-DSA, развивающая конструкцию CRYSTALS-Dilithium [4], закреплена стандартом FIPS 204³, а схема на основе хэш-функций SLH-DSA, основанная на SPHINCS+ [5], – стандартом FIPS 205⁴; оба документа опубликованы в 2024 году вместе с механизмом инкапсуляции ключей ML-KEM (FIPS 203)⁵. Стойкость этих схем установлена в ходе стандартизации, поэтому вопрос их криптографической пригодности можно считать решенным. Открытым остается вопрос о цене их применения в конкретных архитектурах.

Существующие подходы к постквантовой миграции распределенных реестров сосредоточены на алгоритмах и их интеграции в конкретные протоколы. Опубликованы обзоры криптографических примитивов для квантово-устойчивых блокчейнов [6], предложены схемы криптовалют на постквантовых подписях [7], выполнено практическое внедрение постквантового слоя в действующую блокчейн-сеть [8], систематизированы специальные виды подписей для постквантовых реестров [9]. Ограничение этих работ состоит в том, что цифровая подпись рассматривается в них как заменяемый криптографический примитив, тогда как в блокчейне она входит в тело

¹ Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin. URL: <https://bitcoin.org/bitcoin.pdf> (дата обращения: 25.06.2026).

² Computer Security Resource Center. *Post-Quantum Cryptography*. National Institute of Standards and Technology. URL: <https://csrc.nist.gov/projects/post-quantum-cryptography> (дата обращения: 25.06.2026).

³ *Module-Lattice-Based Digital Signature Standard: FIPS 204*. Gaithersburg: National Institute of Standards and Technology; 2024. 55 p. <https://doi.org/10.6028/NIST.FIPS.204>

⁴ *Stateless Hash-Based Digital Signature Standard: FIPS 205*. Gaithersburg: National Institute of Standards and Technology; 2024. 51 p. <https://doi.org/10.6028/NIST.FIPS.205>

⁵ *Module-Lattice-Based Key-Encapsulation Mechanism Standard: FIPS 203*. Gaithersburg: National Institute of Standards and Technology; 2024. 47 p. <https://doi.org/10.6028/NIST.FIPS.203>

каждой транзакции и напрямую определяет размер транзакции, число транзакций в блоке фиксированного объема, скорость роста цепочки и время проверки блока.

Классические подписи компактны. Открытый ключ и подпись Ed25519 [10] вместе занимают менее ста байт, сопоставимые размеры имеют подписи на эллиптических кривых, включая отечественный стандарт⁶, поэтому их вклад в размер транзакции практически незаметен. Постквантовые подписи устроены иначе [11]. Решеточные схемы увеличивают суммарный объем ключа и подписи до нескольких килобайт, а хеш-основанные – до десятков килобайт. Уровень размещения подписи (транзакция, блок или контрольная точка) до сих пор не выделялся как самостоятельный объект эксперимента, хотя именно частота подписываемого объекта и доля подписи в его размере определяют итоговую нагрузку на систему.

Объектом исследования является блокчейн-система с цифровыми подписями транзакций, блоков и контрольных точек. Предметом выступают архитектурные последствия размещения постквантовых подписей ML-DSA и SLH-DSA на различных уровнях такой системы. Исследовательское предположение состоит в том, что уровень размещения подписи является самостоятельным фактором пригодности постквантовой схемы, поскольку одна и та же схема может быть чрезмерно дорогой на уровне каждой транзакции и практически приемлемой на уровне блока или контрольной точки. Исследование намеренно изолирует уровень данных блокчейн-системы. Стойкость самих схем гарантирована стандартами, а безопасность системы в целом определяется конкретным протоколом и потому лежит вне границ работы, оценивающей измеримые архитектурные издержки при заданной модели транзакции и блока.

Цель исследования состоит в экспериментальной оценке архитектурных последствий размещения постквантовых цифровых подписей ML-DSA и SLH-DSA на различных уровнях блокчейн-системы и в определении условий, при которых эти схемы могут быть практически применимы без критического ухудшения плотности блока, роста цепочки и времени проверки. Для достижения цели поставлены задачи определить модель транзакции и блока, учитывающую размер открытого ключа и цифровой подписи; измерить время формирования ключей, формирования и проверки подписи для классических и постквантовых схем; оценить влияние размеров открытых ключей и подписей на размер транзакции и число транзакций в блоке фиксированного размера; оценить время проверки блока при разных режимах размещения подписи; сопоставить режимы подписи каждой транзакции, гибридной подписи, подписи блока валидатором и подписи контрольной точки; сформировать матрицу архитектурных решений по применению рассмотренных схем. Практическая значимость определяется полученной методикой выбора уровня размещения постквантовой подписи и матрицей архитектурных решений, применимыми при проектировании частных и консорциумных блокчейн-систем, ведомственных распределенных реестров и систем долговременного хранения цифровых доказательств.

Материалы и методы

Эксперимент охватил двадцать три схемы цифровой подписи: две классические (Ed25519 и ECDSA-P256), три варианта решеточной схемы ML-DSA (ML-DSA-44, ML-DSA-65, ML-DSA-87), двенадцать вариантов хеш-основанной схемы SLH-DSA и шесть гибридных схем вида Ed25519 + ML-DSA и Ed25519 + SLH-DSA. Для каждой схемы измерялись три операции (генерация ключей, формирование подписи и проверка подписи) по 100 повторов на операцию, чему предшествовали 10 разогревочных

⁶ ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Москва: Стандартинформ; 2012. 17 с.

прогонов. Всего получено 6900 сырых измерений. Измерения выполнялись на компьютере с 16-ядерным процессором Intel (архитектура x86-64) под управлением операционной системы Windows 11 в высокопроизводительном режиме питания в среде Python 3.13⁷. Классические схемы реализованы средствами библиотеки cryptography 49.0⁸, постквантовые — пакетом pqcrypto 0.4.0⁹ на основе эталонных реализаций проекта PQCclean¹⁰; бутстреп-оценки и рисунок получены средствами библиотек NumPy и Matplotlib. Поскольку постквантовые операции вызываются через программную обертку эталонных реализаций без платформенных оптимизаций, абсолютные значения времени следует считать консервативными. Выводы работы опираются прежде всего на соотношения величин и на размеры ключей и подписей, которые от среды не зависят.

Длина сообщения, на котором измерялись операции с подписью, составляла 256 байт. Все рассмотренные схемы зависят от длины сообщения только через его хеширование, а при размерах объектов принятой модели (от 200-байтового заголовка блока до транзакций в десятки килобайт) стоимость хеширования составляет микросекунды и пренебрежима на фоне времени самих операций, поэтому фиксированная длина сообщения репрезентативна. Статистическое описание включает среднее, медиану, стандартное отклонение, а также 5-й и 95-й процентиля. Доверительные интервалы оценивались методом бутстрепа по 2000 перевыборок как для средних значений, так и для медиан методом процентилей при фиксированном начальном состоянии генератора перевыборок. Корректность реализаций проверялась в положительном и отрицательных случаях. Корректная подпись должна успешно проходить проверку и не должна проходить ее при изменении сообщения, самой подписи или при подстановке чужого открытого ключа. Все схемы прошли эти проверки.

Имитационное моделирование блокчейн-слоя воспроизводило размещение подписей в транзакциях и блоках при 30 независимых прогонах на каждую расчетную ячейку и фиксировало как полную, так и выборочную проверку блока. Поскольку показатели плотности блока, роста цепочки и пропускной способности являются детерминированными функциями измеренных размеров ключей и подписей, полное семейство SLH-DSA дополнительно охарактеризовано расчетом из этих размеров, а чувствительность выводов к полезной нагрузке и интервалу контрольной точки исследована расчетным анализом на основе измеренных величин.

Размер транзакции в модели складывается из служебной части, полезной нагрузки, открытого ключа и цифровой подписи. Используется двоичная сериализация с префиксами длины для полей переменного размера. Служебная часть объединяет фиксированные поля транзакции (отправитель, получатель, сумма, метка времени, одноразовый номер, идентификатор схемы) и префиксы длины и составляет в сумме 41 байт. Размер транзакции $S_{\text{тр}}$ определяется выражением:

$$S_{\text{тр}} = S_{\text{сл}} + S_{\text{н}} + S_{\text{ок}} + S_{\text{цп}}. \quad (1)$$

где $S_{\text{сл}}$ – служебная часть транзакции (41 байт); $S_{\text{н}}$ – полезная нагрузка (128 байт); $S_{\text{ок}}$ – размер открытого ключа; $S_{\text{цп}}$ – размер цифровой подписи.

Число транзакций $N_{\text{тр}}$ в блоке с лимитом $L = 2$ МБ и заголовком $S_{\text{заг}} = 200$ байт вычисляется по формуле:

⁷ Python 3.13.0. Python. URL: <https://www.python.org/downloads/release/python-3130/> (дата обращения: 25.06.2026).

⁸ cryptography 49.0.0. PyPI. URL: <https://pypi.org/project/cryptography/49.0.0/> (дата обращения: 25.06.2026).

⁹ pqcrypto 0.4.0. PyPI. URL: <https://pypi.org/project/pqcrypto/0.4.0/> (дата обращения: 25.06.2026).

¹⁰ PQCclean. PQCclean: clean, portable, tested implementations of post-quantum cryptography. GitHub. URL: <https://github.com/PQCclean/PQCclean> (дата обращения: 25.06.2026).

$$N_{\text{тр}} = \left\lfloor \frac{(L - S_{\text{зар}})}{S_{\text{тр}}} \right\rfloor. \quad (2)$$

Рост цепочки при записи K транзакций оценивается произведением:

$$G = K \cdot S_{\text{тр}}. \quad (3)$$

Время проверки блока при размещении подписи в каждой транзакции оценивается линейно по медианному времени проверки одной подписи $t_{\text{пр}}$ по формуле:

$$T_{\text{бл}} \approx N_{\text{тр}} \cdot t_{\text{пр}}. \quad (4)$$

При оценке пропускной способности принят интервал формирования блока 10 с; пропускная способность вычисляется как отношение числа транзакций в блоке к этому интервалу. Лимит блока задан в двоичных единицах ($2 \text{ МБ} = 2 \times 2^{20}$ байт), тогда как рост цепочки выражается в десятичных гигабайтах ($1 \text{ ГБ} = 10^9$ байт). Падение плотности определяется как отношение числа транзакций, помещающихся в блок при базовой схеме Ed25519, к числу транзакций при рассматриваемой схеме.

Рассмотрены четыре режима размещения постквантовой подписи. В режиме А постквантовой схемой подписывается каждая транзакция. В режиме В каждая транзакция несет гибридную подпись, объединяющую классическую и постквантовую схемы. В режиме С постквантовую подпись на заголовок блока ставит узел-валидатор. В режиме D подпись ставится на контрольную точку, агрегирующую заданное число блоков (в эксперименте принято 100). В режимах А и В подпись входит в тело каждой транзакции и непосредственно влияет на её размер и плотность блока, тогда как в режимах С и D постквантовая подпись применяется к редко формируемому объекту, и её крупный размер амортизируется по множеству транзакций.

Результаты

В Таблице 1 приведены размеры открытого ключа и подписи, а также медианы и 95-е процентиля времени формирования и проверки подписи для представительного набора схем.

Таблица 1 – Размеры и время операций для представительных схем (длина сообщения 256 байт)
Table 1 – Sizes and operation times for representative schemes (256-byte message)

Схема	Откр. ключ, Б	Подпись, Б	ОК+П, Б	Форм., медиана, мс	Форм., 95 %, мс	Пров., медиана, мс	Пров., 95 %, мс
Ed25519	32	64	96	0,064	0,068	0,092	0,106
ECDSA-P256	65	71	136	0,064	0,093	0,080	0,102
ML-DSA-44	1312	2420	3732	0,315	0,702	0,080	0,085
ML-DSA-65	1952	3309	5261	0,436	1,023	0,129	0,131
ML-DSA-87	2592	4627	7219	0,539	1,253	0,240	0,396
SLH-DSA-SHA2-128s	32	7856	7888	827,790	917,042	0,808	0,830
SLH-DSA-SHA2-128f	32	17088	17120	40,051	41,495	2,278	2,330
SLH-DSA-SHA2-256s	64	29792	29856	1231,854	1270,491	1,655	1,705
Ed25519+ML-DSA-44	1352	2492	3844	0,361	0,706	0,177	0,182
Ed25519+SLH-DSA-SHA2-128s	72	7928	8000	800,213	836,568	0,892	0,914

Медианные оценки устойчивы. Для Ed25519 медиана времени проверки составляет 0,092 мс при интервале [0,092; 0,093]. Для ML-DSA-44 медиана формирования подписи равна 0,315 мс при интервале [0,279; 0,352], а медиана проверки

– 0,080 мс при интервале [0,080; 0,080]. Для SLH-DSA-SHA2-128s медиана формирования подписи составляет 827,8 мс при интервале [825,1; 832,5]. Схема ML-DSA-44 имеет сопоставимое или даже меньшее медианное время проверки по сравнению с Ed25519, но значительно увеличивает размер транзакции. Схема SLH-DSA имеет существенно более крупные подписи и в ряде вариантов существенно более медленное формирование подписи, поэтому не является универсальной заменой классических транзакционных подписей.

В Таблице 2 показано, как размер транзакции, число транзакций в блоке 2 МБ, падение плотности относительно Ed25519, рост цепочки на один миллион транзакций и пропускная способность при интервале блока 10 с изменяются при размещении подписи в каждой транзакции. Гибридные строки соответствуют режиму В. Соотношения плотности представлены на Рисунке 1.

Таблица 2 – Плотность блока, рост цепочки и пропускная способность при размещении подписи в каждой транзакции (блок 2 МБ, полезная нагрузка 128 байт)

Table 2 – Block density, chain growth and throughput for per-transaction signing (2 MB block, 128-byte payload)

Схема	Размер транзакции, Б	Транзакций в блоке	Падение плотности, раз	Рост цепочки, ГБ/млн тр.	Пропускная способность, тр/с
Ed25519	265	7913	1,0	0,265	791,3
ML-DSA-44	3901	537	14,7	3,901	53,7
ML-DSA-65	5430	386	20,5	5,430	38,6
ML-DSA-87	7388	283	28,0	7,388	28,3
SLH-DSA-SHA2-128s	8057	260	30,4	8,057	26,0
SLH-DSA-SHA2-128f	17289	121	65,4	17,289	12,1
SLH-DSA-SHA2-256s	30025	69	114,7	30,025	6,9
Ed25519+ML-DSA-44 (гибрид)	4013	522	15,2	4,013	52,2
Ed25519+SLH-DSA-SHA2-128s (гибрид)	8169	256	30,9	8,169	25,6

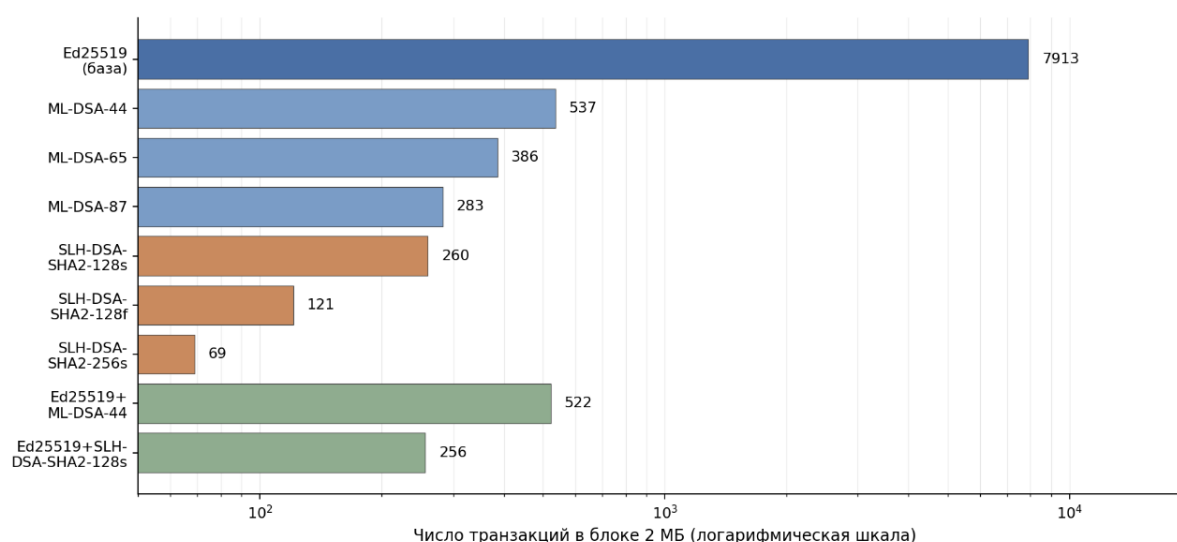


Рисунок 1 – Число транзакций в блоке 2 МБ при размещении подписи в каждой транзакции

Figure 1 – Number of transactions per 2 MB block under per-transaction signing

Даже наиболее компактная из рассмотренных постквантовых схем, ML-DSA-44, при размещении подписи в каждой транзакции уменьшает плотность блока и пропускную способность почти в 15 раз (с 791,3 до 53,7 транзакций в секунду при неизменном интервале блока). Режим уровня транзакции, следовательно, требует архитектурных мер: хранения открытых ключей по ссылке, изменения формата транзакции, пакетирования проверок, увеличения лимита блока или переноса части заверений на уровень блока.

Для решеточной схемы ML-DSA проверка блока оценивалась двумя способами: фактической проверкой блока в имитационной модели и линейной оценкой по формуле (4) для того же числа транзакций. Для ML-DSA-65 и ML-DSA-87 фактически проверялся полный блок. Для ML-DSA-44 проверялся блок из 400 транзакций, тогда как полный блок вмещает 537. Результаты сведены в Таблицу 3.

Таблица 3 – Время проверки блока для ML-DSA: фактическая проверка и линейная оценка
Table 3 – Block verification time for ML-DSA: actual verification and linear estimate

Схема	Транзакций в блоке	Факт., медиана, с	Факт., 95 %, с	Линейная оценка, с	Отношение факт/оценка
ML-DSA-44	400	0,0328	0,0332	0,0320	1,02
ML-DSA-65	386 (полный)	0,0518	0,0565	0,0499	1,04
ML-DSA-87	283 (полный)	0,0644	0,0672	0,0680	0,95

Линейная экстраполяция на полный блок дает для ML-DSA-44 около 0,043 с (537 транзакций). Для ML-DSA-65 и ML-DSA-87 линейная оценка полного блока совпадает с приведенной в таблице (0,050 и 0,068 с), а для базовой линии Ed25519 составляет 0,73 с при 7913 транзакциях. Расхождение между фактической проверкой и линейной оценкой находится в пределах примерно от -5 до $+4$ %, то есть линейная оценка достаточно точна. Вместе с тем меньшее абсолютное время проверки блока для ML-DSA по сравнению с Ed25519 не следует трактовать как рост производительности системы, поскольку оно связано прежде всего с резким уменьшением числа транзакций, помещающихся в блок фиксированного размера.

В Таблице 4 приведены результаты для режимов C и D. В режиме C узел-валидатор подписывает заголовок блока постквантовой схемой, транзакции сохраняют классическую подпись Ed25519. В режиме D постквантовая подпись ставится на контрольную точку, агрегирующую 100 блоков. Времена операций представляют собой медианы 100-повторных измерений из Таблицы 1, так как операции для заголовка блока и контрольной точки совпадают с транзакционными, а различие длины подписываемого объекта пренебрежимо.

Таблица 4 – Издержки постквантовой подписи на уровне блока (режим C) и контрольной точки (режим D)

Table 4 – Overhead of a post-quantum signature at the block level (mode C) and the checkpoint level (mode D)

Режим	Схема	Подпись, Б	Формир., медиана, мс	Пров., медиана, мс	Рост цепочки, ГБ/млн тр.	Прирост к базе, %
C	ML-DSA-44	2420	0,315	0,080	0,2655	0,18
C	ML-DSA-65	3309	0,436	0,129	0,2657	0,25
C	ML-DSA-87	4627	0,539	0,240	0,2659	0,34
C	SLH-DSA-SHA2-128s	7856	827,790	0,808	0,2660	0,38

Таблица 4 (продолжение)
Table 4 (continued)

C	SLH-DSA-SHA2-128f	17088	40,051	2,278	0,2672	0,82
C	SLH-DSA-SHA2-256s	29792	1231,854	1,655	0,2688	1,42
D	ML-DSA-44	2420	0,315	0,080	0,2650	< 0,01
D	SLH-DSA-SHA2-128s	7856	827,790	0,808	0,2650	< 0,01

Перенос постквантовой подписи на уровень блока меняет картину принципиально. Размер транзакции и плотность блока остаются на уровне базовой линии (7913 транзакций в блоке), а прирост роста цепочки даже для наиболее крупной из рассмотренных подписей SLH-DSA-SHA2-256s не превышает 1,5 %. Время формирования подписи заголовка, достигающее 1,23 с для SLH-DSA-SHA2-256s, выполняется валидатором один раз за интервал блока (10 с) и не входит в критический путь проверки транзакций. Проверка подписи заголовка занимает не более 2,3 мс на блок. В режиме контрольной точки издержки амортизируются ещё сильнее. При агрегировании 100 блоков дополнительная стоимость проверки в пересчете на транзакцию составляет доли наносекунды, а прирост роста цепочки не превышает тысячных долей процента. Схема SLH-DSA, непригодная для подписи каждой транзакции, на уровне блока и контрольной точки создаёт пренебрежимо малые издержки, что количественно подтверждает исследовательское предположение работы.

Имитационное моделирование охватывало репрезентативные варианты SLH-DSA, однако размеры открытых ключей и подписей измерены для всех двенадцати вариантов, а показатели плотности блока, роста цепочки и пропускной способности являются детерминированными функциями этих размеров и модели транзакции. В Таблице 5 приведен расчет для полного семейства. Варианты SHAKE совпадают с одноименными вариантами SHA2 по размерам ключей и подписей и потому дают те же значения. Различия между ветвями SHA2 и SHAKE проявляются только во времени операций.

Таблица 5 – Плотность блока и рост цепочки для полного семейства SLH-DSA, рассчитанные из измеренных размеров (варианты SHA2 и SHAKE совпадают по размерам)
Table 5 – Block density and chain growth for the full SLH-DSA family, computed from measured sizes (SHA2 and SHAKE variants coincide in size)

Вариант	Откр. ключ, Б	Подпись, Б	Транзакция, Б	Транзакций в блоке	Падение плотности, раз	Рост цепочки, ГБ/млн тр.
SLH-DSA-128s	32	7856	8057	260	30,4	8,057
SLH-DSA-128f	32	17088	17289	121	65,4	17,289
SLH-DSA-192s	48	16224	16441	127	62,3	16,441
SLH-DSA-192f	48	35664	35881	58	136,4	35,881
SLH-DSA-256s	64	29792	30025	69	114,7	30,025
SLH-DSA-256f	64	49856	50089	41	193,0	50,089

Расчет выявляет закономерность семейства. Быстрые (f) варианты платят за скорость формирования подписи её размером, так что подпись SLH-DSA-192f (35 664 байта) оказывается крупнее подписи SLH-DSA-256s (29 792 байта). Падение плотности для полного семейства лежит в диапазоне от 30,4 до 193,0 раза, поэтому вывод о

непригодности SLH-DSA для подписи каждой транзакции справедлив для любого варианта семейства, а не только для рассмотренных в имитационной модели.

Приведенные выше оценки падения плотности получены при полезной нагрузке 128 байт. Поскольку размер транзакции линейен по нагрузке, вклад подписи ослабевает с ее ростом. В Таблице 6 показано падение плотности при нагрузке от 128 байт до 16 КБ; числа транзакций в блоке вычислены по формуле (2).

Таблица 6 – Падение плотности блока в зависимости от полезной нагрузки транзакции (раз)
Table 6 – Block density drop as a function of transaction payload (times)

Схема	128 Б	512 Б	1 КБ	4 КБ	16 КБ
ML-DSA-44	14,7	6,6	4,1	1,9	1,2
ML-DSA-65	20,5	9,0	5,5	2,2	1,3
SLH-DSA-SHA2-128s	30,4	13,0	7,7	2,8	1,5

Для ML-DSA-44 штраф снижается с 14,7 раза при 128 байтах до 1,2 раза при 16 КБ. Оценка архитектурных последствий, таким образом, должна учитывать профиль нагрузки. В системах с легкими платежными транзакциями постквантовая подпись доминирует в размере транзакции, тогда как в документо-ориентированных реестрах, где полезная нагрузка составляет килобайты, режим подписи каждой транзакции существенно менее обременителен. Аналогично проверена чувствительность режима контрольной точки к интервалу агрегирования (Таблица 7). Амортизированные издержки строго обратно пропорциональны интервалу; расчёт выполнен по медианным временам проверки и измеренным размерам.

Таблица 7 – Издержки постквантовой подписи контрольной точки в зависимости от интервала агрегирования
Table 7 – Overhead of a post-quantum checkpoint signature as a function of the aggregation interval

Схема	Интервал, блоков	Амортиз. проверка, нс/тр.	Прирост роста цепочки, %
ML-DSA-44	1	10,1	0,178
ML-DSA-44	10	1,0	0,018
ML-DSA-44	100	0,10	0,0018
ML-DSA-44	1000	0,01	0,0002
SLH-DSA-SHA2-128s	1	102,1	0,376
SLH-DSA-SHA2-128s	10	10,2	0,038
SLH-DSA-SHA2-128s	100	1,0	0,0038
SLH-DSA-SHA2-128s	1000	0,10	0,0004

Даже при подписи каждого блока (интервал 1, что соответствует режиму С) амортизированная стоимость проверки не превышает 102 нс на транзакцию, а прирост роста цепочки – 0,38 %. Вывод о пренебрежимости издержек уровня блока и контрольной точки устойчив во всём практически значимом диапазоне интервалов.

Обсуждение

Полученные результаты позволяют разделить пригодность постквантовых схем по уровням размещения подписи и в рамках принятых допущений подтверждают исследовательское предположение. Решеточная схема ML-DSA является наиболее реалистичным постквантовым кандидатом для подписи каждой транзакции. Ее проверка не создает вычислительного узкого места, и ограничивающим фактором выступает не время операций, а размер подписи и открытого ключа, определяющий падение

плотности блока в 14,7–28,0 раза. По этой же причине в работе не рассматривалась пакетная проверка подписей: узким местом по результатам является размер, который пакетирование не изменяет, а стандарты FIPS 204 и FIPS 205 определяют только единичную проверку, поэтому сопоставление всех схем в режиме единичной проверки является сравнением в равных условиях. Вывод о цене уровня транзакции зависит от профиля нагрузки: при росте полезной нагрузки со 128 байт до 16 КБ штраф плотности для ML-DSA-44 снижается с 14,7 до 1,2 раза, поэтому для документо-ориентированных реестров режим подписи каждой транзакции существенно менее обременителен, чем для легких платежных транзакций.

Хеш-основанную схему SLH-DSA не следует рассматривать как универсальную транзакционную подпись. Ее рациональная область – редкие и долговременные подписи: заголовки блоков, контрольные точки, архивные заверения и инфраструктурные записи. Полученные результаты свидетельствуют, что в этих режимах крупный размер подписи и высокая стоимость ее формирования амортизируются по большому числу транзакций. Прирост роста цепочки остается в пределах 1,5 % на уровне блока и тысячных долей процента на уровне контрольной точки, причем вывод устойчив для любого варианта семейства и любого практически значимого интервала агрегирования. Консервативные предположения стойкости SLH-DSA, сводящиеся к свойствам хеш-функций, делают ее особенно уместной именно для долгоживущих заверений. Тем самым результаты дают количественную меру проблеме размера постквантовых подписей, которая в обзорных работах [6, 9] отмечалась преимущественно качественно. Гибридные подписи следует понимать как переходный режим миграции, а не как оптимальную долгосрочную архитектуру. Они одновременно несут классическую и постквантовую подписи, что повышает устойчивость к ошибкам перехода, но еще сильнее увеличивает размер транзакции. С этим согласуется опыт практического внедрения постквантового слоя в действующую сеть [8], где гибридное решение применялось именно как механизм переходного периода.

Главный методологический вывод состоит в том, что архитектурный уровень размещения подписи является самостоятельным фактором пригодности алгоритма. Для блокчейн-систем недостаточно сравнивать только время формирования и проверки подписи. Необходимо учитывать размер открытого ключа, размер подписи, размер транзакции, плотность блока, рост цепочки и частоту подписываемого объекта. Практическая значимость результатов реализована в методике выбора уровня размещения постквантовой подписи, опирающейся на совместный учет этих показателей, и в матрице архитектурных решений (Таблица 8). Согласно матрице, ML-DSA-44 может рассматриваться как начальный вариант для подписи каждой транзакции при условии оптимизации структуры транзакции и хранения открытых ключей; ML-DSA-65 и ML-DSA-87 целесообразны при повышенных требованиях к криптографической прочности ценой большей нагрузки на размер транзакции и рост цепочки; SLH-DSA целесообразна прежде всего для подписи блоков, контрольных точек и архивных заверений; гибридный режим уместен при миграции, но не как конечная архитектура. Матрица применима при проектировании частных и консорциумных блокчейн-систем, ведомственных распределенных реестров, образовательных блокчейн-реестров, реестров удостоверяющих записей, архивных журналов и систем долговременного хранения цифровых доказательств. Полученные результаты образуют инженерную основу для выбора режима размещения постквантовой подписи, но не заменяют формального анализа безопасности конкретного протокола.

Таблица 8 – Матрица архитектурных решений по размещению цифровой подписи
Table 8 – Decision matrix for digital signature placement

Схема	Статус	Уровень размещения	Влияние на плотность и рост	Рекомендуется	Не рекомендуется
Ed25519	классическая	транзакция	пренебрежимое	базовая схема в доквантовой фазе	долговременная стойкость против квантового противника
ECDSA-P256	классическая	транзакция	пренебрежимое	базовая схема в доквантовой фазе	долговременная стойкость против квантового противника
ML-DSA-44	постквантовая, решеточная	транзакция с архитектурными мерами	умеренное	наиболее реалистичный кандидат для уровня транзакции	применение без учета падения плотности блока
ML-DSA-65	постквантовая, решеточная	транзакция с архитектурными мерами	умеренное	уровень транзакции при повышенной прочности	применение без учета роста цепочки
ML-DSA-87	постквантовая, решеточная	транзакция с архитектурными мерами	умеренное-высокое	уровень транзакции при максимальной прочности	применение без учета роста цепочки
SLH-DSA-SHA2-128s	постквантовая, хеш-основанная	блок, контрольная точка, архив	высокое	редкие долгоживущие подписи, контрольные точки, архивные заверения	уровень транзакции
SLH-DSA-SHA2-128f	постквантовая, хеш-основанная	блок, контрольная точка, архив	высокое	редкие долгоживущие подписи, контрольные точки	уровень транзакции
SLH-DSA-SHA2-256s	постквантовая, хеш-основанная	блок, контрольная точка, архив	очень высокое	архивные заверения, долговременное хранение	уровень транзакции
Ed25519+ML-DSA-44	гибридная, устойчивая к миграции	гибридная транзакция	умеренное	переходный период миграции	целевое состояние
Ed25519+SLH-DSA-SHA2-128s	гибридная, устойчивая к миграции	гибридная транзакция	высокое	переходный период миграции	целевое состояние

Границы исследования определяются принятой моделью уровня данных. Полная модель, охватывающая сетевые задержки распространения блока, протокол консенсуса, мемпул и экономические стимулы, не строилась и составляет предмет отдельного исследования. Вместе с тем лимит блока фиксирован для всех режимов, поэтому задержки распространения блока сокращаются при сравнении режимов между собой, а сетевые издержки на передачу транзакции монотонно растут с ее размером, вследствие чего учет сетевого уровня мог бы лишь усилить выявленные различия. В этом смысле выводы работы консервативны.

Заключение

Выполнена экспериментальная оценка архитектурных последствий размещения постквантовых цифровых подписей ML-DSA и SLH-DSA на четырех уровнях блокчейн-системы. Эксперимент охватил 23 схемы и 6900 измерений криптографических операций и был дополнен имитационным моделированием плотности блока и времени его проверки, а также расчетным анализом полного семейства SLH-DSA и чувствительности к полезной нагрузке и интервалу контрольной точки. Все поставленные задачи решены: построена модель транзакции и блока, измерены времена операций, оценены плотность блока, рост цепочки, пропускная способность и время проверки блока, сопоставлены четыре режима размещения, сформирована матрица архитектурных решений.

Установлено, что ML-DSA является наиболее реалистичным постквантовым вариантом для уровня транзакции, однако даже ML-DSA-44 при полезной нагрузке 128 байт снижает плотность блока и пропускную способность почти в 15 раз, причем с ростом нагрузки штраф уменьшается вплоть до 1,2 раза при 16 КБ. Падение плотности для полного семейства SLH-DSA достигает 30–193 раз, что исключает его применение на уровне транзакции, тогда как на уровне блока прирост роста цепочки не превышает 1,5 %, а на уровне контрольной точки – тысячных долей процента. Гибридные схемы пригодны для переходного периода, но не как конечная архитектура. Главный результат состоит в экспериментальном обосновании того, что уровень размещения подписи определяет практическую пригодность постквантовой схемы в блокчейн-системе, а постквантовая миграция является архитектурной задачей, а не только задачей замены криптографического алгоритма. Дальнейшие исследования целесообразно направить на построение полной системной модели с учетом консенсуса и сетевых задержек, на алгоритмы пакетной проверки решеточных подписей и на измерения с платформенно-оптимизированными реализациями для уточнения абсолютных временных оценок.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*. 1997;26(5):1484–1509. <https://doi.org/10.1137/S0097539795293172>
2. Aggarwal D., Brennen G., Lee T., Santha M., Tomamichel M. Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger*. 2018;3. <https://doi.org/10.5195/ledger.2018.127>
3. Kearney J.J., Perez-Delgado C.A. Vulnerability of Blockchain Technologies to Quantum Attacks. *Array*. 2021;10:100065. <https://doi.org/10.1016/j.array.2021.100065>
4. Ducas L., Kiltz E., Lepoint T., et al. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2018;2018(1):238–268. <https://doi.org/10.13154/tches.v2018.i1.238-268>

5. Bernstein D.J., Hülsing A., Kölbl S., Niederhagen R., Rijneveld J., Schwabe P. The SPHINCS⁺ Signature Framework. In: *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 11–15 November 2019, London, UK*. New York: ACM; 2019. P. 2129–2146. <https://doi.org/10.1145/3319535.3363229>
6. Fernández-Caramés T.M., Fraga-Lamas P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*. 2020;8:21091–21116. <https://doi.org/10.1109/ACCESS.2020.2968985>
7. Gao Y.-L., Chen X.-B., Chen Y.-L., Sun Y., Niu X.-X., Yang Y.-X. A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. *IEEE Access*. 2018;6:27205–27213. <https://doi.org/10.1109/ACCESS.2018.2827203>
8. Allende M., López León D., Cerón S., et al. Quantum-Resistance in Blockchain Networks. *Scientific Reports*. 2023;13(1). <https://doi.org/10.1038/s41598-023-32701-6>
9. Buser M., Dowsley R., Esgin M., et al. A Survey on Exotic Signatures for Post-Quantum Blockchain: Challenges and Research Directions. *ACM Computing Surveys*. 2023;55(12):251. <https://doi.org/10.1145/3572771>
10. Bernstein D.J., Duif N., Lange T., Schwabe P., Yang B.-Y. High-Speed High-Security Signatures. *Journal of Cryptographic Engineering*. 2012;2(2):77–89. <https://doi.org/10.1007/s13389-012-0027-1>
11. Bernstein D.J., Lange T. Post-Quantum Cryptography. *Nature*. 2017;549(7671):188–194. <https://doi.org/10.1038/nature23461>

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

Родионов Алексей Владимирович, кандидат технических наук, заведующий кафедрой математического моделирования и цифровых технологий, Байкальский государственный университет, Иркутск, Российская Федерация.
e-mail: avr-v@yandex.ru
ORCID: [0000-0003-0451-2655](https://orcid.org/0000-0003-0451-2655)

Aleksei V. Rodionov, Candidate of Engineering Sciences, Head of the Department of Mathematical Modeling and Digital Technologies, Baikal State University, Irkutsk, the Russian Federation.

Статья поступила в редакцию 02.07.2026; одобрена после рецензирования 11.09.2026; принята к публикации 13.10.2026.

The article was submitted 02.07.2026; approved after reviewing 11.09.2026; accepted for publication 13.10.2026.