quantus

квантовая безопасность, зашифрованные деньги

ОПУБЛИКОВАНО
21 марта 2026 г.

ВЕРСИЯ
0.3.3

КЛАССИФИКАЦИЯ
public

Настоящий whitepaper предоставляется исключительно в информационных целях и не является предложением о продаже, запросом предложения о покупке или рекомендацией по любым ценным бумагам, инвестициям или финансовым продуктам. Читателям следует самостоятельно провести должную проверку и проконсультироваться с квалифицированными специалистами перед принятием инвестиционных решений. Quantus Network не даёт заявлений и гарантий относительно точности или полноты содержащейся здесь информации.

СОДЕРЖАНИЕ

01

введение

квантовая угроза

Традиционные блокчейны сталкиваются с экзистенциальной угрозой со стороны криптографически значимых квантовых компьютеров (CRQC). Криптографические основы блокчейнов опираются на сложность задачи дискретного логарифмирования (DLP), а квантовые алгоритмы, в частности алгоритм Шора, могут решать DLP экспоненциально быстрее, чем классические компьютеры. Эта уязвимость может позволить квантовым противникам выводить закрытые ключи из открытых, что даёт им возможность подделывать транзакции и расшифровывать конфиденциальные финансовые данные.

> без упреждающих обновлений, устойчивых к квантовым вычислениям, криптоэкономика на триллионы долларов рискует внезапной девальвацией из-за таких атак.

уникальное ценностное предложение

Названная по латинскому слову, означающему «сколько», Quantus Network обеспечивает масштабируемые и квантово-безопасные частные деньги. Quantus — не универсальная

платформа смарт-контрактов. Как ресторан с небольшим меню идеально отточенных блюд, Quantus предлагает:

— Постквантовые подписи для всех транзакций

— Постквантовые подписи и шифрование (ML-DSA и ML-KEM) для защиты пиринговых соединений

— Постквантовые доказательства с нулевым разглашением для масштабирования

— Счета повышенной безопасности, чтобы сдерживать кражи и допускать исправление ошибок

— Читаемые контрольные фразы для простой проверки адресов

Решение сфокусироваться на масштабируемых квантово-безопасных частных деньгах обусловлено угрозой CRQC для отрасли и неспособностью Bitcoin справиться с этими вызовами.

02

квантовая угроза для блокчейна

основы квантовых вычислений

Квантовые компьютеры используют такие принципы, как суперпозиция и запутанность, чтобы выполнять вычисления, недоступные классическим машинам. В отличие от классических битов, которые равны 0 или 1, кубиты могут находиться в нескольких состояниях одновременно, обеспечивая экспоненциальный параллелизм для ряда задач. Эта способность создаёт экзистенциальные риски для криптографических систем, лежащих в основе блокчейн-финансов: алгоритмы, разработанные для квантового оборудования, подрывают предпосылки безопасности большей части криптографии с открытым ключом.

Алгоритм Шора, представленный в 1994 году Питером Шором, даёт метод с полиномиальным временем работы для факторизации больших целых и решения задачи дискретного логарифмирования на квантовом компьютере. Он опирается на квантовые преобразования Фурье (QFT), чтобы находить период функции, позволяя эффективно обращать односторонние функции с секретом, лежащие в основе таких схем, как RSA или криптография на эллиптических кривых (ECC). Для блокчейн-финансов это означает, что атакующий с

достаточно мощным квантовым компьютером (оценочно ~2000 логических кубитов [6][7][8][9]) может выводить закрытые ключи из открытых за полиномиальное время $O(n^3)$: экстремальное ускорение, которое делает уязвимые системы устаревшими за одну ночь. [1]

Алгоритм Гровера, предложенный Ловом Гровером в 1996 году, даёт квадратичное ускорение для неструктурированного поиска, сокращая время поиска с O(n) до O(√n) операций. Хотя он не столь разрушителен, как Шор для асимметричной криптографии, Гровер затрагивает симметричные примитивы — хеш-функции и шифрование AES, фактически сокращая уровень безопасности вдвое (например, 256-битный ключ ведёт себя как 128-битный против квантовых атак). Эту атаку смягчают удвоением битовой стойкости, а не сменой криптографической схемы. Кроме того, квадратичное ускорение Гровера мало применимо из-за высоких требований к кубитам и гейтам: нужны миллиарды последовательных операций при ограниченном параллелизме, что делает его нереалистичным для практических взломов даже на будущем оборудовании. [2]

четыре категории угроз

01 — подделка цифровых подписей

Алгоритм Шора напрямую угрожает подписям на основе ECC, используемым в большинстве блокчейнов (например, кривая

secp256k1 в Bitcoin), позволяя противникам выдавать себя за пользователей и авторизовать мошеннические транзакции. Такая возможность означала бы критический отказ самой базовой функции блокчейна.

02 — подделка ложных доказательств в системах с нулевым разглашением

Многие доказательства с нулевым разглашением, например в zk-SNARKs для финансов с упором на конфиденциальность, опираются на сложность дискретного логарифмирования через спаривание на эллиптических кривых для обязательств. Шор может позволить создавать недействительные доказательства, выглядящие действительными, что позволит атакующему чеканить новые монеты или фальсифицировать состояние L2.

03 — расшифровка секретной информации

Квантовые атаки могут раскрыть зашифрованные данные, защищённые уязвимыми схемами с открытым ключом в протоколах конфиденциальности вроде Zcash или Monero. Они также могут расшифровывать p2p-сообщения в финансовых протоколах, раскрывая чувствительные сведения о капитале и позволяя целевые кражи.

04 — обращение хеш-функций

Алгоритм Гровера может ускорить атаки на прообраз для хешей вроде SHA-256, используемых в proof-of-work и генерации адресов, но это наименее тревожная угроза. Многие

постквантовые схемы включают конструкции на основе хешей: хеши считаются достаточно безопасными при достаточно большом размере дайджеста.

проблемы масштабирования в постквантовой криптографии

Хотя постквантовая криптография (PQC) даёт необходимую защиту от квантовых угроз, она вносит серьёзные препятствия для масштабирования из-за самой природы этих алгоритмов. В отличие от схем на эллиптических кривых, опирающихся на компактные математические структуры, примитивы PQC требуют больших параметров, чтобы сохранять стойкость против классических и квантовых противников. Отсюда заметно большие открытые и закрытые ключи и подписи, часто на порядки величины. Следующая таблица иллюстрирует типичные размеры ML-DSA при уровне постквантовой безопасности 128 бит в сравнении с классическими аналогами вроде 256-битного ECDSA: [10]

АЛГОРИТМ	ОТКРЫТЫЙ КЛЮЧ	ЗАКРЫТЫЙ КЛЮЧ	ПОДПИСЬ
ML-DSA-87 (Dilithium)	2 592 байта	4 896 байт	4 627 байт
ECDSA (256 бит)	32 байта	32 байта	65 байт

Размеры при уровне постквантовой безопасности 128 бит. Источник: Open Quantum Safe Project [10]

Как видно, подписи ML-DSA могут быть более чем в 70 раз больше эквивалентов ECDSA, а открытые ключи — более чем в 80 раз. Другие семьи PQC усугубляют ситуацию: хешевые схемы вроде SPHINCS+ могут давать подписи до 41 КБ, тогда как решёточные варианты, оптимизированные по размеру, вроде FALCON, всё равно превосходят классические размеры в несколько раз.

В контексте блокчейна раздутые размеры складываются в системные проблемы масштабирования. Более крупные подписи раздувают отдельные транзакции, снижая TPS, так как блоки заполняются быстрее и требуют больше времени на проверку. Также нагружается P2P-связь, растут пропускная способность и задержки распространения, что может повышать риск форков или осиротевших блоков в механизмах консенсуса вроде proof-of-work. Требования к хранению тоже растут: выше операционные расходы узлов и барьеры к участию, особенно для пользователей или валидаторов с ограниченными ресурсами.

> **ПРИМЕЧАНИЕ**
>
> Эти проблемы масштабирования в будущем придётся решать всем блокчейнам. У Bitcoin, например,

> будет гораздо меньше 1 TPS, если не увеличивать максимальный размер блока.

03

кризис миграции

проблема координации

Консервативная культура Bitcoin сопротивляется изменениям протокола. Любое улучшение PQC потребовало бы консенсуса по спорным вопросам: сроки миграции, возможная конфискация монет и увеличение размера блока. Даже если сообщество согласится, каждому пользователю пришлось бы переносить монеты на новые квантово-безопасные адреса. Миграция требует действий всех держателей криптовалют, многие из которых потеряли доступ к кошелькам или не осознают угрозу.

Эти проблемы есть у любой публичной блокчейн-сети, но для Bitcoin они особенно сложны из-за отсутствия ясного лидерства и философии технического «окаменения».

проблема потерянных монет

Оценивается, что от 250 до 500 миллиардов долларов в Bitcoin навсегда недоступны из-за потерянных ключей, умерших владельцев или забытых кошельков. [3] Эти монеты нельзя мигрировать: они действуют как публичная награда за создание CRQC. Квантовые атакующие выведут закрытые

ключи из немигрированных открытых ключей и, вероятно, обрушат на рынок миллиарды долларов в BTC.

> единственное техническое решение — жёсткий срок, который замораживает немигрированные монеты: это политически невозможно.

Без такого срока немигрированные монеты будут украдены и проданы, обрушив рынок и разрушив доверие к сети.

проблема календаря миграции

Постквантовые подписи в 20–80 раз больше текущих подписей Bitcoin. Без фундаментальных архитектурных изменений производительность Bitcoin рухнет до доли уже и так ограниченной пропускной способности.

Даже если Bitcoin преодолеет политические и технические трудности, сама миграция займёт месяцы или годы. Каждый владелец должен отправить хотя бы одну транзакцию, чтобы перевести средства на квантово-безопасный адрес. Многие сначала отправят пробные транзакции. Когда раздутые PQC-подписи душат пропускную способность, сеть сталкивается с очередью на месяцы или годы, пока уязвимые к кванту монеты остаются под угрозой.

> **ОТВЕТ QUANTUS**

> Эти накопленные вызовы делают чрезвычайно трудным добавление квантовой безопасности к существующим цепям. Quantus Network избегает этого, встраивая квантовую безопасность в цепь с первого дня.

04

архитектура quantus network

основы

Quantus Network построена на Substrate — SDK блокчейна, разработанном Parity Technologies, командой за Ethereum и Polkadot. Substrate высокомодулен: компоненты легко заменять, чтобы сфокусироваться на том, что делает Quantus уникальной.

Quantus расширяет Substrate:

— Добавляя поддержку постквантовых схем подписи

— Обновляя безопасность P2P-сети до постквантовой

— Добавляя управляемую пользователем обратимость транзакций

— Делая базу данных совместимой с zk, выравнивая все типы данных с границами элементов поля

постквантовые криптографические примитивы

Quantus Network использует PQC, стандартизированную NIST, чтобы обеспечить безопасность транзакций и сетевого взаимодействия против квантовых угроз. В основе целостности транзакций — **ML-DSA** (алгоритм цифровой подписи на

модульных решётках, ранее CRYSTALS-Dilithium) — схема подписи на решётках, выбранная за баланс безопасности, эффективности и простоты реализации. ML-DSA опирается на сложность задач вроде Learning With Errors (LWE) и Short Integer Solution (SIS) на модульных решётках, обеспечивая устойчивость к классическим и квантовым атакам, включая алгоритм Шора. [4]

Для подписей транзакций Quantus внедряет **ML-DSA-87** — набор параметров с наивысшим уровнем безопасности (уровень 5 NIST, эквивалент 256 битам классической и 128 битам квантовой стойкости), чтобы защититься от возможных прорывов в криптоанализе решёток. Этот выбор отдаёт приоритет осторожности: криптография на решётках относительно нова и менее проверена в бою, чем классические схемы. Более крупные параметры снижают риски потенциальных успехов в криптоанализе решёток, при которых меньшие ключи остались бы более слабой мишенью.

рассмотренные альтернативы

ML-DSA выбран вместо альтернатив вроде FN-DSA (Falcon) из-за большей сложности реализации FN-DSA (например, требуются операции с плавающей запятой, неудобные для блокчейна), отсутствия детерминированной генерации ключей в спецификации и незавершённого статуса на момент разработки.

Хешевые варианты вроде SLH-DSA не выбраны из-за ещё больших подписей (свыше 17 КБ). Крипто-гибкость (возможность менять схему подписи) встроена в Substrate, поэтому добавить эти альтернативы в будущем относительно просто, если потребуется.

Хотя ML-DSA-87 даёт более крупные ключи и подписи, они управляемы на ранней стадии сети Quantus, где хранение ещё не узкое место, а оптимизации вроде wormhole-адресов через доказательства с нулевым разглашением решат проблему масштабирования.

Технические детали реализации см. в QIP-0006.

libp2p — квантово-безопасная сеть

Quantus Network защищает обмен между узлами peer-to-peer (P2P), сочетая ML-DSA для аутентификации и **ML-KEM** (механизм инкапсуляции ключей на модульных решётках, ранее CRYSTALS-Kyber) для шифрования. Эта интеграция распространяет PQC на стек libp2p, изменяя ключевые компоненты для квантовой стойкости: подписи ML-DSA-87 для идентичности пиров и ML-KEM-768 для безопасности транспорта (расширение рукопожатия Noise дополнительным KEM-сообщением для общих секретов, устойчивых к кванту). [5]

P2P-уровень часто упускают в анализе квантовой безопасности. Аутентификация пиров важна, но худшее, что может сделать атакующий на уровне пиров, — выдать себя за узел и слать недействительные сообщения, что может вызвать отказ в обслуживании. Это уже смягчается тем, что узлы в модели блокчейна обычно не доверяют и могут легко сменить ключ при обнаружении атаки. Расшифровка P2P даёт атакующему ограниченную пользу (например, отслеживание путей транзакций, смягчается прокси или Tor), а большая часть данных всё равно становится публичной в цепи.

Тем не менее квантово-безопасный P2P защищает от прослушки, атак «человек посередине» и квантового расшифрования, гарантируя, что gossip узлов, распространение блоков и другие сетевые взаимодействия остаются конфиденциальными и целостными в обозримом будущем.

Технические детали см. в QIP-0004.

масштабирование pqc — wormhole-адреса

Чтобы справиться с проблемами масштабирования постквантовой криптографии, Quantus Network вводит инновационную агрегированную постквантовую схему подписи под названием **«Wormhole Addresses»**. Она использует доказательства с нулевым разглашением (ZKP), генерируемые системой доказательств Plonky2 (по сути STARK), чтобы

вынести проверку балансов за пределы цепи, позволяя цепи проверять одно компактное доказательство без обработки отдельных подписей. Wormhole Addresses позволяют верифицировать большое число транзакций одним доказательством; публичные входы (например, nullifier, корень хранилища, выходные адреса и суммы) — главный ограничивающий фактор. Это снижает амортизированные потребности в хранении на транзакцию до примерно 256 дополнительных байт на транзакцию — намного меньше, чем у любой известной схемы PQC-подписи.

Квантовая безопасность схемы обеспечивается использованием стойкой хеш-функции **Poseidon2** для обязательств через FRI (Fast Reed-Solomon Interactive Oracle Proofs) вместо привычных для SNARK уязвимых к кванту спариваний на эллиптических кривых.

Кроме того, секреты аутентификации скрыты за Poseidon2. Поскольку стойкие хеш-функции ослабляются только квадратично алгоритмом Гровера, они не «ломаются»; доказательства прообраза для хеша могут служить лёгкими постквантовыми подписями в ZK-контекстах, аналогично хешевым схемам вроде SPHINCS+.

поток клиент / доказывающая сторона

Пользователи генерируют доказуемо нерасходуемый адрес двойным хешированием соли, сконкатенированной с секретом:

```
H(H(salt|secret))
```

Эта конструкция исключает ложные срабатывания (например, путаница простого хеш-ключа с нерасходуемым адресом): в Substrate (и вообще) блокчейн-адреса — это простой хеш открытого ключа, полученного из закрытого через алгебраическую операцию, а не стойкий хеш. Безопасность конструкции сводится к поиску прообраза-прообраза стойкого хеша. Токены, отправленные на этот адрес, фактически сжигаются. Их нельзя потратить: для адреса-получателя нет закрытого ключа. Эти монеты можно снова отчеканить без инфляции предложения.

Для каждого перевода создаётся объект хранилища TransferProof с деталями вроде глобального счётчика переводов. Кошелёк пользователя генерирует доказательство Merkle-Patricia-Trie (MPT) от корня хранилища недавнего заголовка блока до листа этого TransferProof. Вычисляется nullifier, чтобы предотвратить двойной расход:

```
H(H(salt | secret | global_transfer_count))
```

поток агрегатора

Любая сторона (клиент, майнер или третье лицо) может агрегировать несколько доказательств через рекурсию Plonky2, формируя дерево доказательств, где каждое

родительское доказывает дочерние, агрегируя публичные входы детей:

— Nullifier проходят без изменений

— Выходные адреса дедуплицируются

— Хеши блоков доказываются связанными, затем отбрасываются кроме последнего

— Суммы для дублирующихся выходных адресов суммируются

поток цепь / верификатор

Сеть проверяет агрегированное доказательство: хеш блока в цепи и недавний, уникальность nullifier (против двойного расхода) и валидность доказательства. ZK-схема обеспечивает корректность доказательства хранилища, точность nullifier, нерасходуемость адреса, согласованность балансов входов и выходов и связь заголовков блоков.

почему plonky2

— Уже проходил аудит

— Постквантовый

— Без trusted setup

— Эффективное доказательство/верификация

— Плавная агрегация доказательств

— Нативная реализация на Rust

— Совместим с no-std окружением Substrate

> **ПРОИЗВОДИТЕЛЬНОСТЬ**
>
> Рекурсивные доказательства завершаются за 170 миллисекунд при компактных размерах (100 КБ на агрегированное доказательство). В оптимальном случае с блоками 5 МБ и всеми транзакциями на один выход wormhole-адреса могли бы упаковать ~153 000 транзакций в один блок (4,9 МБ / 32 байта на nullifier): улучшение в 223 раза по сравнению с ~685 «сырыми» транзакциями ML-DSA (5 МБ / 7,3 КБ каждая).

замечания по безопасности

Потенциальные риски включают ошибки инфляции из-за дефектов схемы/верификатора, хотя они будут экономически заметны, если перечеканенные монеты превысят балансы с нулевых адресов отправки. Пользователи могут по желанию доказать, что адрес — wormhole, опубликовав первый хеш без раскрытия секрода. Проверочные транзакции не подписаны, поэтому DoS из-за неудачных транзакций нужно смягчать без финансовых рычагов. Расчёты предложения токенов сохраняются: перечеканка выглядит как новые монеты, но сохраняет гарантии максимального предложения за счёт сжиганий.

Подробнее см. QIP-0005.

механизм консенсуса

Quantus Network использует алгоритм консенсуса Proof-of-Work (PoW), сохраняющий желаемые свойства консенсуса Bitcoin и улучшающий совместимость с ZK-доказательствами, заменяя SHA-256 на **Poseidon2**.

Важно: это изменение сделано не ради квантовой безопасности. Криптографические хеш-функции вроде SHA-256 ослабляются, но не уничтожаются квантовыми алгоритмами, в частности Гровером. Некоторые постквантовые схемы подписи используют стойкие хеши как строительный блок по этой причине.

Poseidon2 — усовершенствование хеш-функции Poseidon. Создание SNARK или STARK для вычислений с традиционными хешами вроде SHA-256 обычно требует почти в 100 раз больше гейтов, чем с Poseidon, который целиком опирается на алгебраические операции над элементами поля, а не на побитовые операции.

Для Poseidon2 и Plonky2 используется **поле Goldilocks**. Порядок поля Goldilocks помещается в 64-битное беззнаковое целое, что повышает эффективность без ущерба для стойкости.

05

сохранение капитала

При управлении ключами криптовалют существует много рисков. Большинство из них можно избежать.

обратимые транзакции

Quantus Network предлагает настраиваемые пользователем обратимые транзакции. Отправители задают временное окно, в котором могут отменить исходящие переводы. Это сдерживает кражи и исправляет ошибки без потери финальности. Система использует модифицированный pallet Substrate «scheduler» с метками времени. Кошельки показывают обратный отсчёт отправителю (с кнопкой отмены) и получателю.

Обратимые транзакции позволяют новые протоколы безопасности, сохраняя децентрализацию через исполнение в цепи.

Подробнее см. QIP-0009.

контрольные фразы

Quantus Network вводит «check-phrases» — читаемую человеком криптографически стойкую контрольную сумму для блокчейн-адреса. Адрес хешируется, чтобы получить короткую последовательность запоминающихся слов из списка BIP-39.

Контрольные фразы защищают от опечаток, подмены и атак отравления адресов. Функция вывода ключа с 50 000 итераций делает атаки радужных таблиц дорогими. Для крупных транзакций пользователи всё равно должны проверять каждый символ адреса.

Технические детали см. в QIP-0008.

счета повышенной безопасности

Любой счёт можно улучшить до «счёта повышенной безопасности» с обязательными периодами обратимости для всех исходящих переводов. Назначенный **опекун** (аппаратный кошелёк, мультисиг или доверенное третье лицо) может отменять подозрительные транзакции в период обратимости, переводя средства опекуну вместо отправителя или получателя. Эта опция необратима после включения: воры не смогут её отключить.

Опекуны можно выстраивать в цепочку: опекун счёта повышенной безопасности может сам быть счётом повышенной безопасности со своим опекуном. Так возникают композитные иерархии, где у каждого опекуна есть более высокие полномочия над защищаемым счётом. Дизайн даёт время обнаружить и отреагировать на несанкционированную активность без компромисса финальности легитимных переводов.

Подробнее см. QIP-0011.

восстановление ключей

Многие крипто-состояния ушли в могилу вместе с владельцами. Quantus Network даёт простой способ указать адрес восстановления, который может вывести средства в любой момент после фиксированной задержки. В течение этого времени владелец может отклонить восстановление, если имеет доступ к ключу. Эта функция обеспечивает «выживание»: у пользователей есть завещание в цепи без судов и формального наследования.

hd-lattice

Иерархические детерминированные (HD) кошельки — отраслевой стандарт для блокчейнов: одна seed-фраза для всех ключей, выше безопасность и удобство по сравнению с ручным копированием на каждое действие. Адаптация к решёточным схемам вроде Dilithium ставит две задачи:

— Выходы HMAC-SHA512 не могут напрямую формировать решёточные закрытые ключи, которые представляют собой полиномы, выбранные из кольца с определёнными свойствами.

— Неусиленная деривация ключей опирается на сложение на эллиптических кривых, отсутствующее на решётках (открытые ключи не замкнуты ни под какой алгебраической операцией).

Quantus Network решает первый пункт, используя выход HMAC как энтропию для детерминированного построения закрытого ключа, а не как сам ключ. Второй пункт менее критичен и остаётся открытым вопросом исследований — можно ли адаптировать решёточную криптографию для его решения.

Подробнее см. QIP-0002.

06

токеномика и управление

Quantus Network существует в меняющейся среде, и мы не можем предполагать, что всё сделаем с первого раза. Поэтому выбрана простая отправная точка, а система управления может вносить изменения по мере поступления новой информации. Такой дизайн превращает блокчейн в живую сущность, способную подстраиваться к окружению. В частности, процесс управления Substrate позволяет глубокие изменения цепи при минимальной координации между операторами узлов.

награды за блок

Quantus Network использует простую токеномику по образцу Bitcoin. Максимальное предложение — **21 000 000 монет**, а простая эвристика определяет награду за блок:

```
block_reward = (max_supply - current_supply) / co
```

Эта эвристика образует плавно убывающую экспоненциальную кривую: по мере того как block_reward увеличивает current_supply, уменьшается рассчитанная block_reward в следующем блоке. Сжигания комиссий и другие уменьшения current_supply снова входят в бюджет наград за блок. Константа подобрана так, что без сжиганий 99% монет выпускается примерно за 30 лет.

распределение инвесторам

Quantus Network создавалась с помощью инвесторов, взявших на себя большой риск финансирования. Частные инвесторы подлежат графику вестинга 4 года, как и команда. Инвесторы публичной продажи получат полную ликвидность в первый день. Средства публичной продажи будут сопоставлены с токенами и направлены на ликвидность (DEX, CEX и маркет-мейкеры). Эти распределения инвесторам вместе с ликвидностью составят единственный «премайн». Остальные токены должны быть добыты майнингом до исчерпания предложения.

Если в ходе публичной продажи будет продано меньше максимальных 10%, токены ликвидности будут пропорционально уменьшены, а остаток будет выпущен майнерам через награды за блок.

распределение компании

Чтобы вознаградить команду за риск создания новой технологии без гарантии успеха, часть награды за блок направляется компании около четырёх лет. Это фактически график вестинга примерно **15% от общего предложения** для компании.

После этого долю компании в наградах за блок можно отключить, скорректировать или перенаправить по

голосованию держателей токенов.

комиссии транзакций

ТИП ТРАНЗАКЦИИ	СТРУКТУРА КОМИССИИ	НАЗНАЧЕНИЕ
Стандартная	Фиксированная комиссия	Майнеры
Обратимая (повышенная безопасность)	1% от объёма	Сжигание
Агрегированная ZK	0,1% от объёма	50% майнер / 50% сжигание

обновления без форка

Quantus Network поддерживает обновления «без форка» через обновления runtime в Substrate: основная логика блокчейна («runtime») может эволюционировать без хард-форков, нарушающих сеть или разделяющих сообщество. Это достигается референдумами управления в цепи: одобренные предложения активируют смену runtime — по сути замену существующего WASM-блоба новым в одном блоке с сохранением состояния и операций. Такой путь минимизирует простои и риски, давая сообществу итеративно улучшать протокол по мере того, как реальное использование выявляет улучшения.

По мере роста доверия к системе возможность менять runtime будет существенно ограничена, чтобы снизить поверхность атаки, если злоумышленник получит контроль над процессом обновления.

система управления

Quantus Network наследует рамку управления из системы OpenGov Polkadot через Substrate. Держатели токенов участвуют через **голосование с убеждением (conviction voting)**, блокируя активы на разные сроки, чтобы усилить вес голоса. Усиление может быть от 1× (без блокировки) до 6× (максимальная блокировка). Такой дизайн поощряет долгосрочное выравнивание интересов, связывая влияние с обязательством.

Предложения распределяются по нескольким трекам голосования — «origins». У каждого origin свои параметры: пороги одобрения (например, квалифицированное большинство для высокоинвазивных изменений), минимальные депозиты против спама, периоды подготовки/исполнения и сроки решения, чтобы избежать тупиков. Многотрековый дизайн позволяет параллельно обрабатывать разные референдумы — от рутинных трат казны до критических обновлений runtime.

Technical Collective — курируемая группа технических экспертов, выступающая специализированным органом для

предложения, ревью или внесения в белый список срочных технических вопросов, ускоряя их по выделенному треку при сохранении надзора сообщества.

Quantus принимает эту систему без изменений, но начинает с минималистичной конфигурации, чтобы избежать сложности на ранних этапах. Изначально активен только трек Technical Collective для обязательных решений высокого уровня вроде обновлений протокола или корректировки параметров.

Позже Quantus может добавить трек некоммьюнити-голосования без обязательной силы для опроса настроений по необязательным темам — предложения функций или опросы экосистемы. Эта система станет обязательной, когда компания передаст сеть DAO. Поэтапный подход позволяет сети органично развиваться будущими голосованиями управления без перегрузки пользователей сложностью в начале.

07

дорожная карта

Текущая дорожная карта до 2026 года, может меняться.

heisenberg inception Декабрь 2024	Финансирование обеспечено, выбран Substrate.
resonance alpha Июль 2025	Публичная тестовая сеть, подписи Dilithium, обратимые транзакции.
schrödinger beta Октябрь 2025	Полный функционал, готовность к аудиту.
dirac beta Ноябрь 2025	PoW переведён на Poseidon2, аудиты учтены.
planck beta Январь 2026	Счета повышенной безопасности, мультисиг, аппаратный кошелёк, интеграция ZK.
bell mainnet 2 кв. 2026	Запуск mainnet.
fermi upgrade 4 кв. 2026	Инфраструктура агрегации ZK-доказательств.

08

риски

Создание Quantus Network сопряжено с присущими рисками.

ошибки реализации

Дефекты в логике ПО могут вызывать серьёзные сбои даже в лучше всего спроектированных системах.

риски выбора алгоритмов nist

Дефекты или потенциальные бэкдоры в выбранных постквантовых стандартах (например, ML-DSA, ML-KEM), которые могут проявиться после стандартизации. В худшем случае такие дефекты позволят атакующему подделывать подписи, выводя закрытый ключ из открытого — это катастрофический режим отказа цепи. Если такие дефекты станут публичными, Quantus Network сможет обновиться на новый алгоритм, но при редкой эксплуатации они могут так и не быть обнаружены.

сроки квантовых вычислений

Квантовый прогресс может наступить гораздо позже прогнозов, откладывая необходимость PQC; наоборот, секретная разработка (например государствами) может

создать внезапные угрозы, если блокчейн-сообщество не обновится быстро.

прочие соображения

Общие барьеры внедрения, регуляторная неопределённость в финансах/блокчейне и присущая криптоэкосистемам волатильность.

09

ссылки и дополнительные материалы

[1] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[2] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eight Annual ACM Symposium on Theory of Computing*, 212-219. https://doi.org/10.1145/237814.237866

[3] Chainalysis. (2024). *The Chainalysis 2024 Crypto Crime Report*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

[4] National Institute of Standards and Technology. (2024). *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML- DSA)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[5] National Institute of Standards and Technology. (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. U.S. Department of

Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[6] Häner, T., Jaques, S., Naehrig, M., Roetteler, M., & Soeken, M. (2020). Improved quantum circuits for elliptic curve discrete logarithms. *arXiv:2002.12480*. https://arxiv.org/abs/2002.12480

[7] Gidney, C., & Ekerå, M. (2021). *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. *arXiv:1905.09749*. https://arxiv.org/abs/1905.09749

[8] Aggarwal, D., et al. (2021). Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies. *ePrint IACR*. https://eprint.iacr.org/2021/967.pdf

[9] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. *arXiv:1706.06752*. https://arxiv.org/abs/1706.06752

[10] Open Quantum Safe Project. (n.d.). ML-DSA | Open Quantum Safe. Retrieved January 29, 2026, from https://openquantumsafe.org/liboqs/algorithms/sig/ml-dsa.html