Quantus Network Whitepaper

Авторы: Christopher Smith | **Последнее обновление:** 14 января 2026 г.

Введение

Квантовая угроза

Традиционные блокчейны сталкиваются с экзистенциальной угрозой в связи с появлением квантовых вычислений. 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 злоумышленникам вычислять закрытые ключи на основе открытых ключей, что позволит им подделывать транзакции и расшифровывать конфиденциальные финансовые данные.

Результатом является катастрофический сбой системы. Без упреждающих обновлений, устойчивых к квантовым вычислениям, криптоэкономика стоимостью в триллионы долларов рискует внезапно обесцениться в результате таких атак.

> 💡 **TIP**
>
> **Quantus исправляет это.**

Уникальное ценностное предложение

Названная в честь латинского слова, означающего «сколько», Quantus Network обеспечивает масштабируемое и квантово-безопасное сохранение капитала. Quantus не является платформой для смарт-контрактов. Вместо этого, подобно высококлассному ресторану без меню, Quantus сосредоточена на том, чтобы делать небольшое количество вещей лучше, чем любая другая chain.

В частности, Quantus использует:

- Постквантовые signature для всех транзакций
- Постквантовые signature и шифрование (ML-DSA и ML-KEM) для защиты пиринговых соединений

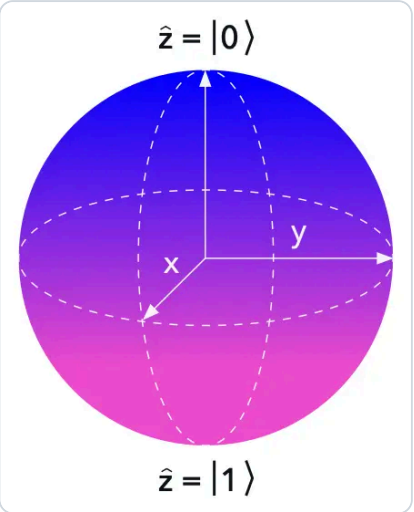
- Постквантовый Bridge к другим блокчейнам и создание квантово-безопасных «обернутых» монет (wrapped coins)
- Постквантовые zero-knowledge-proofs для масштабирования
- Счета повышенной безопасности для предотвращения краж и возможности восстановления после ошибок
- Читаемые человеком check-phrases для простой проверки адресов

Этот целенаправленный подход позволяет пользователям уверенно сохранять капитал, превращая квантовые угрозы в возможности.

> 💡 **TIP**
>
> Quantus — это защищенная от вызовов будущего крепость для вашего состояния.

Квантовая угроза для блокчейна

Основы квантовых вычислений



Квантовые компьютеры используют такие принципы, как суперпозиция и запутанность (entanglement), для выполнения вычислений, которые невыполнимы для классических машин.

В отличие от классических битов, которые принимают значение либо 0, либо 1, квантовые биты (кубиты) могут существовать в нескольких состояниях одновременно, обеспечивая экспоненциальный параллелизм для определенных задач. **Эта способность создает экзистенциальные риски для криптографических систем, лежащих в основе блокчейн-финансов, поскольку алгоритмы, разработанные для квантового оборудования, подрывают предположения о безопасности большинства методов криптографии с открытым ключом.**

Алгоритм Шора

Представленный в 1994 году Питером Шором, он обеспечивает метод с полиномиальным временем работы для факторизации больших целых чисел и решения задачи дискретного логарифмирования на квантовом компьютере. По сути, он использует квантовое преобразование Фурье (QFT) для поиска периода функции, что позволяет эффективно обращать односторонние функции с секретом (trapdoor functions), лежащие в основе таких схем, как RSA или криптография на эллиптических кривых (ECC).

Для блокчейн-финансов это означает, что злоумышленник с достаточно мощным квантовым компьютером (оценивается примерно в 2300 логических кубитов) сможет вычислить закрытые ключи на основе открытых ключей за полиномиальное время $O(n^3)$. Это колоссальное ускорение, которое в одночасье сделает уязвимые системы устаревшими.

Алгоритм Гровера

Предложенный Ловом Гровером в 1996 году, он предлагает квадратичное ускорение для задач неструктурированного поиска, сокращая время поиска конкретного элемента в несортированной базе данных с $O(n)$ до $O(\sqrt{n})$ операций. Он работает путем итеративного усиления амплитуды целевого состояния посредством квантовой интерференции. Хотя он не так разрушителен, как

алгоритм Шора для асимметричной криптографии, **алгоритм Гровера влияет на симметричные примитивы, такие как хеш-функции и шифрование AES, фактически сокращая уровень безопасности вдвое** (например, 256-битный ключ ведет себя как 128-битный против квантовых атак).

Несмотря на значимость, эта атака нивелируется простым удвоением количества бит безопасности, а не сменой криптографической схемы. Кроме того, квадратичное ускорение Гровера непрактично из-за высоких требований к количеству кубитов и гейтов, требуя миллиардов последовательных операций с ограниченным параллелизмом, что делает его невыполнимым для реального взлома даже на оборудовании будущего.

Опасности квантовых вычислений для блокчейн-финансов можно разделить на четыре области:

Подделка цифровых signature

Алгоритм Шора напрямую угрожает signature на основе ECC, используемым в большинстве блокчейнов (например, кривая secp256k1 в Bitcoin), позволяя злоумышленникам выдавать себя за пользователей и авторизовать мошеннические транзакции. Такая возможность означала бы критический отказ самой базовой функции блокчейна.

Подделка ложных доказательств в системах с нулевым разглашением

Многие доказательства с нулевым разглашением, такие как в zk-SNARKs для финансов с упором на конфиденциальность, полагаются на сложность дискретного логарифмирования через спаривание на эллиптических кривых для обязательств; алгоритм Шора может позволить создавать недействительные доказательства, которые выглядят как действительные, что может позволить злоумышленнику выпускать новые монеты или фальсифицировать состояние уровней Layer-2 (L2).

Расшифровка секретной информации

Квантовые атаки могут раскрыть зашифрованные данные, защищенные уязвимыми схемами с открытым ключом в протоколах конфиденциальности, таких как Zcash или Monero. Они также могут расшифровать p2p-коммуникации в финансовых протоколах, раскрывая конфиденциальные детали состояния и обеспечивая возможность адресных краж.

Обращение хеш-функций

Алгоритм Гровера может ускорить атаки по поиску прообраза на хеши, такие как SHA-256, используемые для proof-of-work и генерации адресов, но это наименее вызывающая беспокойство угроза. Многие постквантовые криптографические схемы включают конструкции на

основе хешей, так как хеши считаются достаточно безопасными при достаточно большом размере дайджеста.

Проблемы масштабирования в постквантовой криптографии

Хотя постквантовая криптография (PQC) обеспечивает необходимую защиту от квантовых угроз, она создает значительные препятствия для масштабирования из-за особенностей архитектуры этих алгоритмов. В отличие от схем на эллиптических кривых, которые полагаются на компактные математические структуры, примитивы PQC требуют больших параметров для поддержания безопасности как против классических, так и против квантовых злоумышленников. Это приводит к существенно большему размеру открытых ключей, закрытых ключей и signature, часто на несколько порядков.

В следующей таблице показаны типичные размеры для ML-DSA при 128-битном уровне постквантовой безопасности в сравнении с классическими аналогами, такими как 256-битный ECDSA:

Алгоритм	Размер открытого ключа (байты)	Размер закрытого ключа (байты)	Размер signature (байты)
ML-DSA-87 (Dilithium)	2 592	4 896	4 627
ECDSA (256-бит)	32	32	65

Как видно, signature ML-DSA могут быть более чем в 70 раз больше аналогов ECDSA, а открытые ключи — более чем в 80 раз больше.

Другие семейства PQC усугубляют ситуацию: схемы на основе хешей, такие как SPHINCS+, могут создавать signature размером до 41 КБ, в то время как даже оптимизированные по размеру варианты на решетках, такие как FALCON, все равно в разы превышают классические размеры.

В контексте блокчейна эти раздутые размеры превращаются в системные проблемы масштабирования. Более крупные signature увеличивают размер отдельных транзакций, снижая количество транзакций в секунду (TPS), так как блоки заполняются быстрее и требуют больше времени на проверку. Это также создает нагрузку на пиринговую (P2P) связь, увеличивая требования к пропускной способности и задержки распространения, что может повысить риск форков сети или «осиротевших» блоков (orphaned blocks) в механизмах консенсуса, таких как proof-of-work. Также затрагиваются требования к хранению данных, что ведет к росту эксплуатационных расходов узлов и барьеров для участия, особенно для пользователей или валидаторов с ограниченными ресурсами.

Эти проблемы масштабирования в будущем придется решать всем блокчейнам. Например, у Bitcoin будет гораздо меньше 1 TPS, если максимальный размер блока не будет увеличен.

Архитектура Quantus Network

Постквантовые криптографические примитивы

Quantus Network использует примитивы **PQC, стандартизированные NIST**, для обеспечения безопасности транзакций и сетевых коммуникаций против квантовых угроз. В основе целостности транзакций лежит **ML-DSA (Module-Lattice-based Digital Signature Algorithm**, ранее известный как CRYSTALS-Dilithium) — схема подписи на основе решеток, выбранная за баланс безопасности, эффективности и простоты реализации. **ML-DSA использует сложность таких задач**, как обучение с ошибками (LWE) и поиск кратчайшего вектора (SIS) на модульных решетках, обеспечивая надежную устойчивость как к классическим, так и к квантовым атакам, включая атаки с использованием алгоритма Шора.

Для подписей транзакций **Quantus интегрирует ML-DSA-87** — набор параметров, обеспечивающий высочайший уровень безопасности (NIST Security Level 5, эквивалентный 256-битной классической и 128-битной квантовой безопасности) для **защиты от потенциальных криптоаналитических прорывов в задачах на решетках**. Этот выбор отдает приоритет осторожности, так как криптография на решетках относительно нова и менее проверена временем, чем классические схемы. Большие параметры смягчают риски от потенциальных успехов в криптоанализе решеток, при которых ключи меньшего размера стали бы легкой мишенью.

Альтернативы

ML-DSA был выбран вместо альтернатив, таких как FN-DSA (Falcon), по следующим причинам:

- Большая сложность реализации FN-DSA (например, требование операций с плавающей запятой, которые неудобны для блокчейна)
- Отсутствие детерминированной генерации ключей в спецификации
- Его незавершенный статус на момент разработки

Варианты на основе хешей, такие как SLH-DSA, были отклонены из-за еще больших размеров подписи (превышающих 17 КБ). Крипто-гибкость (возможность замены схем подписи) заложена в Substrate, поэтому добавить эти альтернативы в будущем будет относительно легко, если того потребуют обстоятельства.

Хотя использование ML-DSA-87 приводит к увеличению размера ключей и signature, они вполне допустимы на ранней стадии развития сети Quantus, где хранение данных еще не

является узким местом, а будущие оптимизации, такие как «червоточины» (wormhole addresses) через доказательства с нулевым разглашением, решат проблему масштабирования.

Технические подробности реализации см. в QIP-0006.

LibP2P

Quantus Network защищает пиринговые (P2P) коммуникации узлов, используя комбинацию ML-DSA для аутентификации и ML-KEM (Module-Lattice-based Key Encapsulation Mechanism, ранее CRYSTALS-Kyber) для шифрования.

Эта интеграция распространяет PQC на сетевой стек libp2p, модифицируя основные компоненты для обеспечения квантовой устойчивости: использование signature ML-DSA-87 для идентификации узлов и ML-KEM-768 для безопасности транспорта (расширение рукопожатия Noise дополнительным сообщением KEM для создания квантово-устойчивых общих секретов).

P2P-уровню часто не уделяют должного внимания в анализе квантовой безопасности. Аутентификация узлов важна, но худшее, что может сделать злоумышленник на уровне пиров — это выдать себя за узел и отправить недействительные сообщения, что может привести к отказу в обслуживании. Эта атака уже нивелируется тем фактом, что узлы в модели блокчейна обычно не считаются доверенными, и узлы могут легко сменить свои ключи при обнаружении атаки. Аналогично, расшифровка P2P-коммуникаций дает злоумышленнику ограниченные преимущества (например, отслеживание путей транзакций, что нивелируется прокси-серверами или Tor), а большинство данных в любом случае становится публичным в блокчейне.

Тем не менее, квантовая защита P2P-уровня предохраняет от прослушивания, атак типа «человек посередине» и квантовой расшифровки, гарантируя, что обмен данными между узлами, распространение блоков и другие сетевые взаимодействия останутся конфиденциальными и защищенными от несанкционированного доступа в обозримом будущем.

Технические подробности реализации см. в QIP-0004.

Масштабирование PQC

Чтобы решить проблемы масштабирования, присущие постквантовой криптографии, **Quantus Network внедряет инновационную схему агрегированной постквантовой подписи под названием «Wormhole Addresses»**. Эта система использует доказательства с нулевым разглашением (ZKP), генерируемые через систему Plonky2 (по сути, STARKs), для выноса проверки баланса за пределы блокчейна, что позволяет сети проверять одно компактное доказательство без обработки отдельных signature.

Wormhole Addresses позволяют проверять большое количество транзакций с помощью одного доказательства, при этом основным ограничивающим фактором становятся публичные входные данные (например, нуллификаторы, корень хранилища, адреса выхода и суммы). Это снижает амортизированные требования к хранению одной транзакции до **примерно 256 дополнительных байт на транзакцию, что намного меньше любой известной схемы подписи PQC**.

Квантовая безопасность схемы обеспечивается использованием безопасной хеш-функции Poseidon2 для обязательств через FRI (Fast Reed-Solomon Interactive Oracle Proofs) вместо уязвимых для квантовых атак спариваний на эллиптических кривых, обычно используемых в SNARKs.

Кроме того, секреты аутентификации скрыты за Poseidon2. Поскольку безопасные хеш-функции лишь квадратично ослабляются алгоритмом Гровера, а не взламываются, доказательства прообраза хеша могут служить в качестве легковесных постквантовых signature в контекстах ZK, подобно схемам на основе хешей, таким как SPHINCS+.

Поток Клиент / Доказывающий (Prover)

Пользователи генерируют доказуемо не расходуемый адрес путем двойного хеширования «соли» (salt), объединенной с секретом:

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

Эта конструкция предотвращает ложноположительные результаты (например, ошибочное принятие открытого ключа с одинарным хешированием за нерасходуемый адрес), потому что в Substrate (и в целом) адреса блокчейна представляют собой одинарный хеш открытого ключа, который выводится из закрытого ключа через некоторую алгебраическую операцию, а не через безопасный хеш. Таким образом, безопасность конструкции сводится к поиску прообраза прообраза безопасного хеша. Токены, отправленные на этот адрес, фактически сжигаются. Их нельзя потратить, так как для адреса, который их получил, не существует закрытого ключа. Следовательно, эти монеты могут быть выпущены заново (re-minted) без раздувания предложения.

Для каждого перевода создается объект хранения TransferProof, содержащий такие детали, как уникальный глобальный счетчик переводов. Кошелек пользователя генерирует доказательство хранения Merkle-Patricia-Trie (MPT) от корня хранилища заголовка недавнего блока до «листа» для этого TransferProof.

Вычисляется нуллификатор (nullifier):

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

Для предотвращения двойного расходования, при этом секрет выводится детерминировано из сид-фразы кошелька для обеспечения сохранности.

Поток Агрегатор

Любая сторона (клиент, майнер или третья сторона) может агрегировать несколько доказательств, используя рекурсию Plonky2, формируя дерево доказательств, где каждое родительское доказательство является проверкой дочерних доказательств, при этом публичные входные данные дочерних доказательств агрегируются:

- нуллификаторы передаются без изменений
- адреса выхода дедуплицируются
- хеши блоков доказываются как связанные, после чего все, кроме самого последнего, отбрасываются
- суммы для дублирующихся адресов выхода суммируются Эта рекурсия поддерживает иерархическую агрегацию, радикально сокращая объем данных в блокчейне.

Поток Сеть / Проверяющий (Verifier)

Сеть проверяет агрегированное доказательство, контролируя:

- хеш блока присутствует в блокчейне и является недавним
- уникальность нуллификатора (для предотвращения двойного расходования)
- валидность доказательства

ZK-схема обеспечивает:

- корректность доказательства хранения
- точность вычисления нуллификатора
- невозможность расходования с адреса
- соответствие баланса между входами и выходами
- связность заголовков блоков

Plonky2 была выбрана по следующим причинам:

- уже прошла аудит

- постквантовая устойчивость
- отсутствие доверенной настройки (no trusted setup)
- эффективное доказывание/проверка
- бесшовная агрегация доказательств
- нативная реализация на Rust
- совместимость со средой no-std в Substrate

Основные показатели производительности:

Рекурсивные доказательства за 170 миллисекунд и компактные размеры (100 КБ на агрегированное доказательство), что обеспечивает колоссальный прирост пропускной способности.

В оптимальном случае с блоками по 5 МБ и всеми транзакциями, идущими на один и тот же выход, **Wormhole Addresses могут упаковать ~153 000 транзакций в один блок** (4,9 МБ / 32 байта на нуллификатор), что в 223 раза лучше, чем ~685 «сырых» транзакций ML-DSA (5 МБ / 7,3 КБ каждая).

Примечания по безопасности

Потенциальные риски включают ошибки инфляции из-за неверной реализации схемы/проверки, хотя это было бы экономически заметно, если количество заново выпущенных монет превысит балансы адресов с нулевой отправкой. Пользователи могут по желанию доказать, что адрес является «червоточиной», опубликовав первый хеш без раскрытия секрета. Транзакции проверки не подписываются, поэтому отказ в обслуживании через неудачные транзакции должен нивелироваться нефинансовыми методами. Расчеты предложения токенов сохраняются, так как повторные выпуски выглядят как новые монеты, но гарантии максимального предложения поддерживаются через сжигание.

Дополнительные технические подробности реализации см. в QIP-0005.

Механизм консенсуса

Quantus Network использует алгоритм консенсуса Proof-of-Work (PoW), который сохраняет желаемые свойства алгоритма консенсуса Bitcoin, улучшая при этом совместимость с системами ZK-доказательств путем замены SHA-256 на Poseidon2.

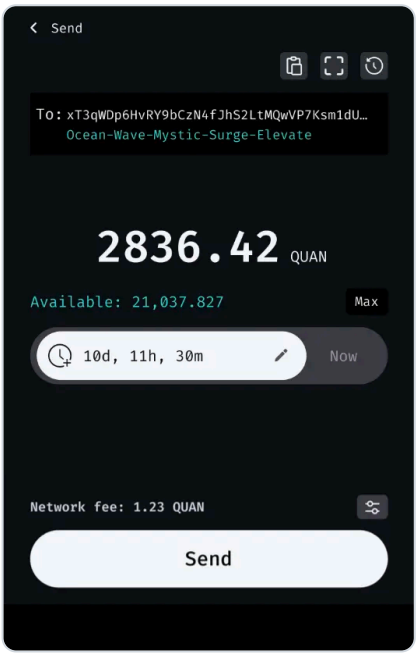
Важно отметить, что это изменение вносится не ради квантовой безопасности. Криптографические хеш-функции, такие как SHA-256, ослабляются, но не уничтожаются квантовыми алгоритмами, в частности алгоритмом Гровера. Некоторые схемы постквантовой подписи используют безопасные хеши в качестве строительного блока именно по этой причине.

Poseidon2 является усовершенствованием хеш-функции Poseidon. Создание SNARK или STARK для вычислений с использованием традиционных хеш-функций, таких как SHA-256, часто требует почти в 100 раз больше гейтов по сравнению с использованием Poseidon, который полностью полагается на алгебраические функции над элементами поля вместо побитовых операций. Мы используем поле Goldilocks как для Poseidon2, так и для Plonky2, чтобы максимизировать эффективность.

Сохранение капитала

Существует много рисков при управлении ключами криптовалют. Большинства из них можно избежать. Quantus Network встраивает простоту использования в саму сеть, позволяя непрофессионалам совершать транзакции со спокойной душой.

Отменяемые транзакции (Reversible Transactions)

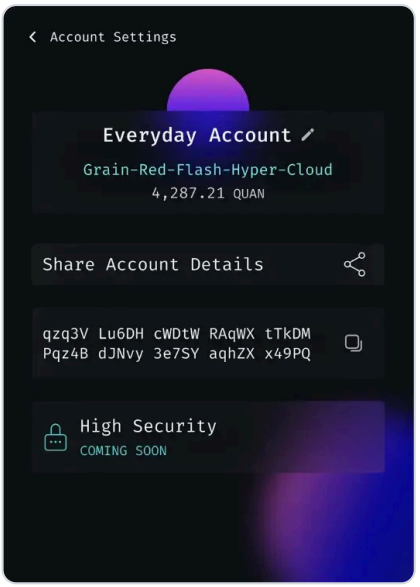


Quantus Network предлагает настраиваемые пользователем отменяемые транзакции, позволяя отправителям устанавливать временное окно, в течение которого они могут отменить исходящие переводы. Это повышает эффективность сдерживания краж и исправления ошибок без ущерба для основной необратимости блокчейна. Используя модифицированный модуль Substrate «scheduler pallet», который применяет временные метки для интуитивно понятных задержек, система позволяет клиентам планировать переводы через простой интерфейс, отображая обратный отсчет в кошельках как для отправителя (с кнопкой отмены), так и для получателя (указывая на завершение, если транзакция не отменена). Это балансирует быструю окончательность для коммерции с гибкостью для пользователей, которые боятся совершить ошибку или хотят внести добросовестный депозит без услуг эскроу.

Отменяемые транзакции формируют мощный строительный блок для новых протоколов безопасности, сохраняя при этом децентрализацию за счет исполнения на уровне сети.

Дополнительные технические подробности см. в QIP-0009.

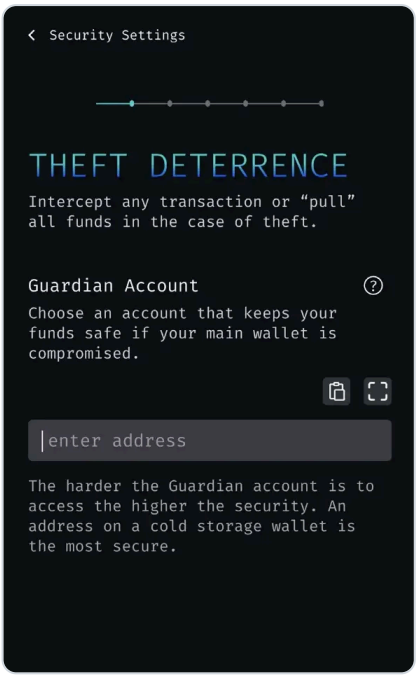
Check-Phrases



Quantus Network внедряет «check-phrases» — криптографически безопасную, читаемую человеком контрольную сумму для адресов блокчейна и других данных, требующих проверки человеком. **Путем хеширования адреса для генерации короткой последовательности запоминающихся слов из мнемонического списка BIP-39, check-phrases обеспечивают быструю и безошибочную проверку целостности, защищая от опечаток, подмены и таких атак, как «отравление адреса» (address poisoning)**. Этот инструмент позволяет пользователям уверенно проверять адреса во время переводов, не полагаясь на обрезанные отображения или слабые контрольные суммы. Используется функция вывода ключа с 50 000 итераций, чтобы гарантировать, что создание радужной таблицы для данных контрольных сумм будет очень дорогостоящим. Разумеется, для крупных транзакций пользователи все равно должны вручную проверять каждую букву адреса на правильность.

Дополнительные технические подробности см. в QIP-0008.

Счета повышенной безопасности



Quantus Network предлагает возможность повысить статус любого счета до «счета повышенной безопасности», который вводит обязательные периоды отмены для всех исходящих переводов. Это позволяет назначенному счету-«опекуну» (guardian), такому как аппаратный кошелек, мультисиг или даже выбранная пользователем доверенная третья сторона, эксклюзивно отменять подозрительные транзакции в течение периода отмены, отправляя средства опекуну вместо отправителя или получателя. Эта добровольная постоянная функция основана на отменяемых переводах, где пользователи указывают задержку и перехватчика при активации, что не позволяет ворам отключить ее.

Перехватчик сам может быть другим счетом повышенной безопасности со своим опекуном, что позволяет создавать компонуемые иерархии, где каждый опекун имеет более высокие полномочия по сравнению со счетом, который он защищает. Эта конструкция имитирует судебные отмены транзакций в традиционных финансах, но под контролем пользователя. Она балансирует безопасность и удобство для счетов с крупными суммами, давая время на обнаружение и реагирование на несанкционированную активность без ущерба для окончательности блокчейна для легитимных потоков.

Дополнительные технические подробности см. в QIP-0011.

Восстановление ключей

Многие криптосостояния ушли в могилу вместе со своими владельцами. Quantus Network предлагает простой способ указать адрес восстановления, который может забрать ваши средства в любое время при условии фиксированной задержки. В течение этого времени владелец может отклонить восстановление, если у него есть доступ к ключу. Эта функция обеспечивает преемственность: у пользователей есть завещание в блокчейне без необходимости обращения в суды или оформления наследства.

HD-Lattice

Иерархически детерминированные (HD) кошельки являются отраслевым стандартом для блокчейнов, позволяя пользователям создавать резервную копию одной сид-фразы для всех

ключей, что повышает безопасность и удобство по сравнению с ручным резервным копированием для каждого действия.

Адаптация этого подхода к схемам на решетках, таким как Dilithium, сопряжена с двумя проблемами:

- Результаты HMAC-SHA512 не могут напрямую формировать закрытые ключи на решетках, для которых требуются полиномы с «хорошим базисом» через выборку с отклонением (rejection sampling).
- Неукрепленный (non-hardened) вывод ключей опирается на сложение на эллиптических кривых, которое отсутствует в решетках (открытые ключи не замкнуты относительно какой-либо алгебраической операции).

Quantus Network решает первую проблему, используя результат HMAC как энтропию для детерминированного построения закрытого ключа, а не как сам закрытый ключ. Вторая проблема менее критична и остается открытым вопросом исследований — можно ли адаптировать криптографию на решетках для ее решения.

Дополнительные технические подробности см. в QIP-0002.

Токеномика и управление

Quantus Network существует в меняющейся среде, и мы не можем предполагать, что сделаем все правильно с первой попытки. По этой причине мы выбираем простую отправную точку и позволяем системе управления вносить изменения по мере получения новой информации. Такая конструкция делает блокчейн живым организмом, который может адаптироваться к своей среде по желанию. В частности, процесс управления Substrate позволяет вносить глубокие изменения в сеть при минимальной координации между различными операторами узлов.

Награды за блок

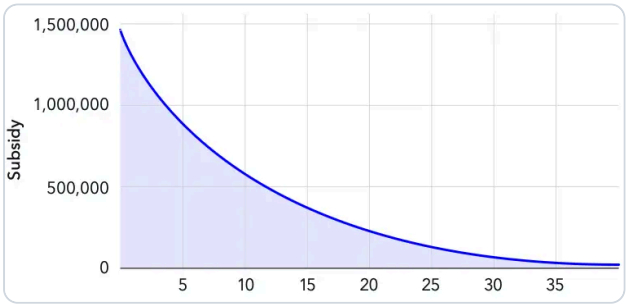
Quantus Network использует прямолинейную модель токеномики, имитирующую модель Bitcoin. Максимальное предложение составляет 21 000 000 монет, а награда за каждый блок определяется простой эвристикой.

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

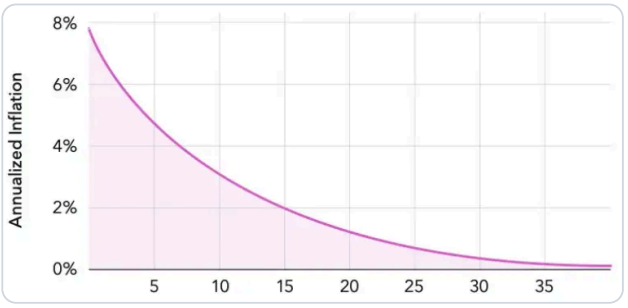
Эта эвристика формирует плавную кривую экспоненциального затухания, так как block_reward пополняет current_supply, что уменьшает block_reward, вычисляемую для следующего блока.

Любые сжигания комиссий или иные сокращения current_supply фактически становятся частью бюджета для наград за блок. Константа выбрана так, чтобы при отсутствии сжиганий 99% монет были эмитированы примерно за 40 лет.

Награды за блок / Год



Инфляция / Год



Распределение для инвесторов

Quantus Network была построена с помощью бизнес-ангелов, которые пошли на большой риск, финансируя ее. Чтобы избежать избыточного предложения, которое создают периоды блокировки инвесторов (investor-lockups), мы делаем всех инвесторов, как государственных, так и частных,

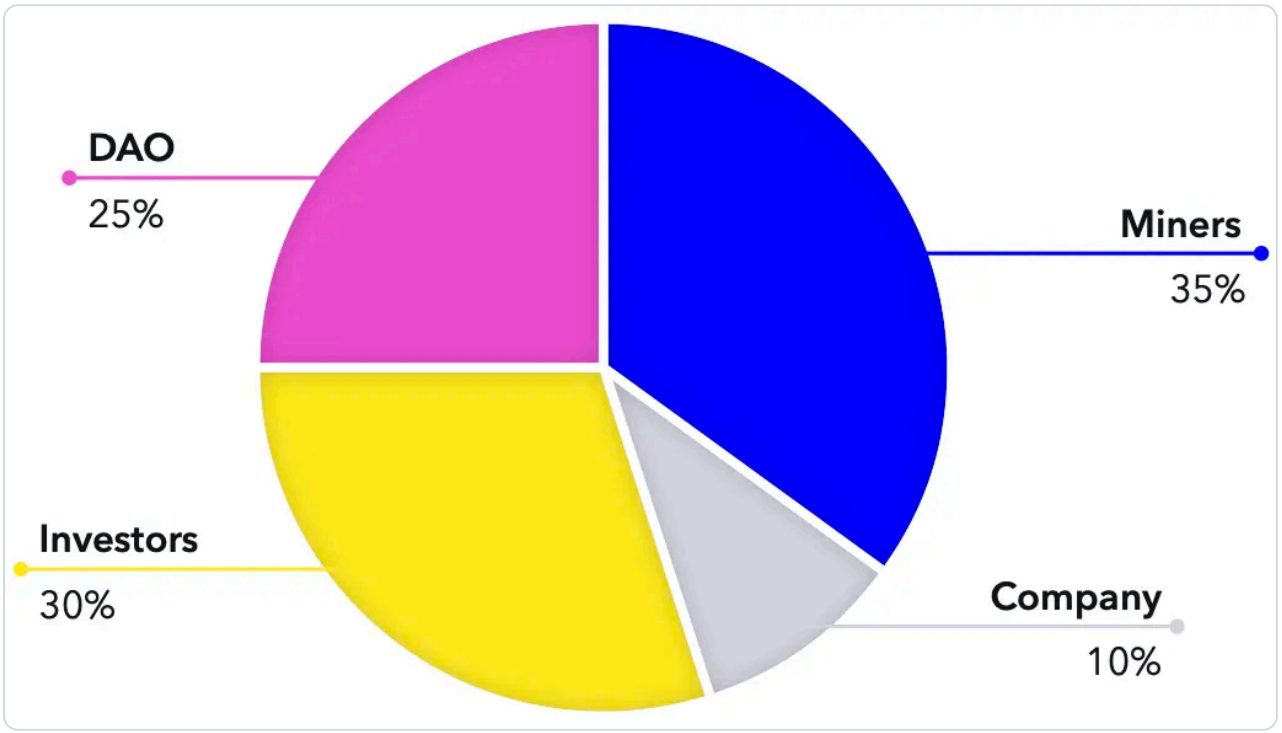
ликвидными с первого дня. Это распределение будет единственным «пре-майном». Все остальные токены должны быть добыты в процессе майнинга. В зависимости от успеха публичных продаж эта часть составит 20–30% от общего предложения.

Распределение компании

Чтобы компенсировать команде риск создания новой технологии без гарантии успеха, мы разделим награды за блок на две половины. Первая половина пойдет майнеру. Примерно в течение четырех лет вторая половина будет идти компании. Это дает фактический график вестинга (vesting) около 10% от общего предложения компании. В течение этого времени майнеры получают такое же количество вновь отчеканенных монет.

После этого момента доля наград за блок, причитающаяся компании, будет перенаправлена в казначейство, управляемое держателями токенов, фактически формируя DAO.

Приблизительное распределение предложения



Комиссии за транзакции

Стандартные транзакции будут иметь комиссию, которая идет майнерам, обеспечивая стимул для включения транзакций в блок. С отмененных транзакций со счетов повышенной безопасности будет взиматься комиссия в размере 1% от объема, которая делится пополам: половина идет майнеру, а половина сжигается, пополняя будущий бюджет безопасности. Транзакции, проходящие через систему агрегации zk, также будут облагаться комиссией в размере 0,1% от объема, которая будет распределяться между майнером, агрегатором доказательств и сжиганием.

Обновления без форков (Forkless Upgrades)

Quantus Network поддерживает обновления «без форков» через обновление рантайма (runtime) Substrate, позволяя основной логике блокчейна («рантайму») развиваться без хардфорков, которые могли бы нарушить работу сети или расколоть сообщество. Это достигается через ончейн-референдумы по управлению, где одобренные предложения инициируют замену рантайма, фактически заменяя существующий блок кода WASM на новый в рамках одного блока, обеспечивая непрерывность состояния и операций. Такой путь обновления сводит к минимуму время простоя и риски, позволяя сообществу итеративно совершенствовать протокол.

Система управления

Quantus Network наследует структуру управления от системы OpenGov сети Polkadot через Substrate. Держатели токенов участвуют через голосование убежденностью (conviction voting), при котором они соглашаются заблокировать свои активы на различные периоды, чтобы усилить вес своего голоса. Это усиление может варьироваться от 1x (без блокировки) до 6x (максимальная блокировка). Такая конструкция поощряет долгосрочную приверженность, связывая влияние с обязательствами.

Предложения распределяются по нескольким направлениям голосования, называемым «origins». Каждое направление имеет индивидуальные параметры, такие как пороги одобрения (например, квалифицированное большинство для важных изменений), минимальные депозиты для предотвращения спама, периоды подготовки/вступления в силу и сроки принятия решений для предотвращения тупиковых ситуаций. Такая многоканальная структура позволяет параллельно обрабатывать различные референдумы — от рутинных расходов казначейства до критических обновлений рантайма.

Технический коллектив (Technical Collective) — это кураторская группа технических экспертов, выступающая в качестве специализированного органа для предложения, рассмотрения или внесения в «белый список» срочных технических вопросов, ускоряя их решение через выделенный канал при сохранении надзора со стороны сообщества.

Quantus принимает эту систему без изменений, но начинает с минималистичной настройки, чтобы избежать сложности на ранних этапах. Первоначально активен только канал Технического коллектива, который будет использоваться для обязательных, высокопривилегированных решений, таких как обновления протокола или настройка параметров.

Позже мы введем канал необязательного голосования сообщества для оценки настроений по неисполняемым темам, таким как предложения по функциям или опросы экосистемы. Эта система станет обязательной, когда компания передаст сеть в управление DAO.

Такой поэтапный подход позволяет сети развиваться органично через будущие голосования по управлению, не обременяя пользователей ненужной сложностью в самом начале.

Дорожная карта

Heisenberg Inception

ДЕКАБРЬ 2024

Финансирование обеспечено, выбран Substrate

Resonance Alpha

ИЮЛЬ 2025

Публичная тестовая сеть, подписи Dilithium, отменяемые транзакции

Schrödinger Beta

ОКТЯБРЬ 2025

Функционал готов, подготовка к аудиту

Dirac Beta

НОЯБРЬ 2025

PoW изменен на Poseidon2, учтены результаты аудитов

Planck Beta

ЯНВАРЬ 2026

Счета повышенной безопасности, мультисиги, аппаратный кошелек

Bell Mainnet

1 КВ. 2026

Запуск основной сети

Fermi Upgrade

2 КВ. 2026

ZK-агрегация

Риски

Создание Quantus Network сопряжено с неизбежными рисками.

- **Проблемы реализации:** Ошибки в логике программного обеспечения могут привести к серьезным сбоям даже в самых продуманных системах.
- **Проблемы выбора алгоритмов NIST:** Потенциальные недостатки или «бэкдоры» в выбранных постквантовых стандартах (например, ML-DSA, ML-KEM), которые могут проявиться после стандартизации. В худшем случае такие недостатки позволят злоумышленнику подделывать signature, вычисляя закрытый ключ на основе открытого, что станет катастрофическим сценарием для сети. Если такие недостатки станут достоянием общественности, Quantus Network можно будет перевести на новый алгоритм, но если такие уязвимости будут использоваться скрытно и редко, они могут никогда не быть обнаружены.
- **Сроки появления квантовых компьютеров:** Квантовые прорывы могут произойти гораздо позже, чем ожидается, что отсрочит необходимость в PQC; и наоборот, секретные разработки (например, со стороны правительств) могут привести к внезапным угрозам, если блокчейн-сообщество не успеет быстро обновиться.
- **Другие соображения:** Общие барьеры для внедрения, неопределенность регулирования в сфере финансов/блокчейна и присущая криптоэкосистемам волатильность.

Заключение

QUANTUS

Мы верим в силу открытых протоколов, proof-of-work и суверенного владения. Приложение Quantus Network, доступное для компьютеров и мобильных устройств, позволяет пользователям хранить цифровые активы, майнить новые блоки и участвовать в более справедливом финансовом будущем без посредников.

Мы привержены принципам прозрачности, конфиденциальности и расширения возможностей людей с помощью безопасных инструментов для самостоятельного хранения активов.