Quantus Network Whitepaper

Penulis: Christopher Smith | **Terakhir diperbarui:** 14 Januari 2026

Pendahuluan

Ancaman Kuantum

Blockchain tradisional menghadapi ancaman eksistensial dari munculnya komputasi kuantum. Fondasi kriptografi blockchain bergantung pada tingkat kesulitan masalah logaritma diskrit (DLP), dan algoritma kuantum, terutama algoritma Shor, dapat menyelesaikan DLP secara eksponensial lebih cepat daripada komputer klasik. Kerentanan ini dapat memungkinkan musuh kuantum untuk menurunkan kunci privat dari kunci publik, yang memungkinkan mereka memalsukan transaksi dan mendekripsi data keuangan yang sensitif.

Hasilnya adalah kegagalan sistem yang katastrofik. Tanpa pemutakhiran tahan kuantum yang proaktif, ekonomi kripto bernilai triliunan dolar berisiko mengalami devaluasi mendadak akibat serangan semacam itu.

> 💡 **TIP**
>
> **Quantus memperbaiki hal ini.**

Proposisi Nilai Unik

Dinamakan berdasarkan kata Latin untuk “seberapa banyak”, Quantus Network menghadirkan pelestarian kekayaan yang skalabel dan aman secara kuantum. Quantus bukanlah platform smart contract. Sebaliknya, seperti restoran kelas atas tanpa menu, Quantus fokus melakukan sejumlah kecil hal dengan lebih baik daripada chain lainnya.

Secara khusus, Quantus menggunakan:

- signature pasca-kuantum untuk semua transaksi
- signature dan enkripsi pasca-kuantum (ML-DSA dan ML-KEM) untuk mengamankan koneksi peer

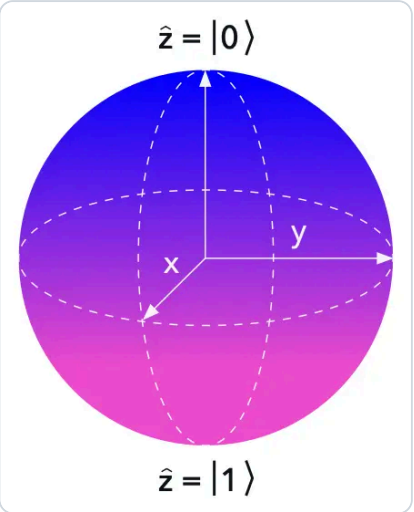
- Bridge pasca-kuantum ke blockchain lain dan membuat wrapped coin yang aman secara kuantum
- zero-knowledge-proofs pasca-kuantum untuk penskalaan
- Akun Keamanan Tinggi untuk mencegah pencurian dan memungkinkan pemulihan dari kesalahan
- check-phrase yang dapat dibaca manusia untuk verifikasi alamat yang mudah

Pendekatan terarah ini memberdayakan pengguna untuk melestarikan kekayaan dengan percaya diri, mengubah ancaman kuantum menjadi peluang.

> 💡 **TIP**
> Quantus adalah benteng tahan masa depan untuk kekayaan Anda.

Ancaman Kuantum terhadap Blockchain

Dasar-Dasar Komputasi Kuantum



Komputer kuantum memanfaatkan prinsip-prinsip seperti superposisi dan keterikatan (entanglement) untuk melakukan komputasi yang sulit diselesaikan oleh mesin klasik.

Berbeda dengan bit klasik yang bernilai 0 atau 1, bit kuantum (qubit) dapat berada dalam beberapa status secara bersamaan, memungkinkan paralelisme eksponensial untuk masalah tertentu. **Kemampuan ini menimbulkan risiko eksistensial terhadap sistem kriptografi yang mendasari keuangan blockchain, karena algoritma yang dikembangkan untuk perangkat keras kuantum merusak asumsi keamanan dari sebagian besar kriptografi kunci publik**.

Algoritma Shor

Diperkenalkan pada tahun 1994 oleh Peter Shor, menyediakan metode waktu polinomial untuk memfaktorkan bilangan bulat besar dan menyelesaikan masalah logaritma diskrit pada komputer kuantum. Intinya, algoritma ini mengeksploitasi Quantum Fourier Transforms (QFT) untuk menemukan periode suatu fungsi, memungkinkan pembalikan efisien dari fungsi trapdoor yang mendasari skema seperti RSA atau kriptografi kurva eliptik (ECC).

Untuk keuangan blockchain, ini berarti penyerang dengan komputer kuantum yang cukup kuat (diperkirakan sekitar 2.300 qubit logis) dapat menurunkan kunci privat dari kunci publik dalam waktu polinomial $O(n^3)$. Ini adalah percepatan yang ekstrem, membuat sistem yang rentan menjadi usang dalam semalam.

Algoritma Grover

Diusulkan oleh Lov Grover pada tahun 1996, menawarkan percepatan kuadratik untuk masalah pencarian tak terstruktur, mengurangi waktu untuk menemukan item tertentu dalam database yang tidak disortir dari $O(n)$ menjadi $O(\sqrt{n})$ operasi. Algoritma ini bekerja dengan secara iteratif memperkuat amplitudo status target melalui interferensi

kuantum. Meskipun tidak sedahsyat algoritma Shor untuk kriptografi asimetris, **algoritma Grover berdampak pada primitif simetris seperti fungsi hash dan enkripsi AES, yang secara efektif membagi dua tingkat keamanan** (misalnya, kunci 256-bit berperilaku seperti 128-bit terhadap serangan kuantum).

Meskipun berdampak, serangan ini dapat dimitigasi hanya dengan menggandakan bit keamanan, daripada mengubah skema kriptografi. Selain itu, percepatan kuadratik Grover tidak praktis karena persyaratan qubit dan gerbang yang tinggi, membutuhkan miliaran operasi secara berurutan, dengan paralelisme terbatas, membuatnya tidak layak untuk pembalikan dunia nyata bahkan pada perangkat keras masa depan.

Bahaya komputasi kuantum bagi keuangan blockchain dapat dikategorikan ke dalam empat area:

Memalsukan Digital signature

Algoritma Shor secara langsung mengancam signature berbasis ECC yang digunakan di sebagian besar blockchain (misalnya, kurva secp256k1 milik Bitcoin), memungkinkan musuh untuk meniru identitas pengguna dan mengotorisasi transaksi penipuan. Kemampuan seperti itu akan mewakili kegagalan kritis dari fitur paling dasar dari sebuah blockchain.

Memalsukan Bukti Palsu dalam Sistem Zero-Knowledge

Banyak zero-knowledge proof, seperti yang ada di zk-SNARKs untuk keuangan yang berfokus pada privasi, mengandalkan tingkat kesulitan logaritma diskrit melalui pasangan kurva eliptik untuk komitmen; algoritma Shor dapat memungkinkan pembuatan bukti tidak valid yang tampak valid, yang dapat memungkinkan penyerang untuk mencetak koin baru atau memalsukan status Layer-2 (L2).

Mendekripsi Informasi Rahasia

Serangan kuantum dapat mengekspos data terenkripsi yang dilindungi oleh skema kunci publik yang rentan dalam protokol privasi seperti Zcash atau Monero. Ini juga dapat mendekripsi komunikasi p2p dalam protokol keuangan, mengungkapkan detail kekayaan yang sensitif dan memungkinkan pencurian yang ditargetkan.

Membalikkan Fungsi Hash

Algoritma Grover dapat mempercepat serangan preimage pada hash seperti SHA-256, yang digunakan untuk proof-of-work dan pembuatan alamat, tetapi ini adalah ancaman yang paling tidak mengkhawatirkan. Banyak skema kriptografi pasca-kuantum

menggabungkan konstruksi berbasis hash karena hash dianggap cukup aman dengan digest yang cukup besar.

Tantangan Penskalaan dalam Kriptografi Pasca-Kuantum

Meskipun kriptografi pasca-kuantum (PQC) menawarkan perlindungan penting terhadap ancaman kuantum, ia memperkenalkan hambatan penskalaan yang signifikan karena desain inheren dari algoritma ini. Berbeda dengan skema kurva eliptik yang mengandalkan struktur matematika yang ringkas, primitif PQC membutuhkan parameter yang lebih besar untuk menjaga keamanan terhadap musuh klasik dan kuantum. Hal ini menghasilkan kunci publik, kunci privat, dan signature yang jauh lebih besar, seringkali dalam beberapa kali lipat.

Tabel berikut mengilustrasikan ukuran tipikal untuk ML-DSA pada tingkat keamanan pasca-kuantum 128-bit dibandingkan dengan rekan klasiknya seperti ECDSA 256-bit:

Algoritma	Ukuran Kunci Publik (Byte)	Ukuran Kunci Privat (Byte)	Ukuran Signature (Byte)
ML-DSA-87 (Dilithium)	2.592	4.896	4.627
ECDSA (256-bit)	32	32	65

Seperti yang ditunjukkan, signature ML-DSA bisa lebih dari 70 kali lebih besar dari padanan ECDSA, dan kunci publik lebih dari 80 kali lebih besar.

Keluarga PQC lainnya memperburuk hal ini: skema berbasis hash seperti SPHINCS+ dapat menghasilkan signature hingga 41 KB, sementara varian lattice yang dioptimalkan ukurannya seperti FALCON pun masih melebihi ukuran klasik dengan kelipatan yang signifikan.

Dalam konteks blockchain, ukuran yang membengkak ini menjadi masalah penskalaan sistemik. signature yang lebih besar membuat transaksi individu membengkak, mengurangi transaksi per detik (TPS) karena blok terisi lebih cepat dan membutuhkan lebih banyak waktu untuk validasi. Ini juga membebani komunikasi peer-to-peer (P2P), meningkatkan permintaan bandwidth dan penundaan propagasi, yang dapat meningkatkan risiko fork jaringan atau blok yatim (orphaned blocks) dalam mekanisme konsensus seperti proof-of-work. Persyaratan penyimpanan juga terpengaruh, yang menyebabkan biaya operasional node yang lebih tinggi dan hambatan untuk partisipasi, terutama bagi pengguna atau validator dengan sumber daya terbatas.

Tantangan penskalaan ini harus diatasi oleh semua blockchain di masa depan. Bitcoin, misalnya, akan memiliki jauh kurang dari 1 TPS jika ukuran blok maksimum tidak ditingkatkan.

Arsitektur Quantus Network

Primitif Kriptografi Pasca-Kuantum

Quantus Network menggunakan primitif **PQC standar NIST** untuk memastikan keamanan transaksi dan komunikasi jaringan terhadap ancaman kuantum. Inti dari integritas transaksi adalah **ML-DSA (Module-Lattice-based Digital Signature Algorithm**, sebelumnya dikenal sebagai CRYSTALS-Dilithium), sebuah skema signature berbasis lattice yang dipilih karena keseimbangan keamanan, efisiensi, dan kemudahan implementasi. **ML-DSA memanfaatkan tingkat kesulitan masalah** seperti Learning With Errors (LWE) dan Short Integer Solution (SIS) di atas module lattices, memberikan ketahanan yang kuat terhadap serangan klasik dan kuantum, termasuk dari algoritma Shor.

Untuk signature transaksi, **Quantus mengintegrasikan ML-DSA-87**, set parameter yang menawarkan tingkat keamanan tertinggi (NIST Security Level 5, setara dengan keamanan klasik 256-bit dan keamanan kuantum 128-bit) untuk **melindungi dari potensi terobosan kriptanalitik dalam masalah lattice**. Pilihan ini memprioritaskan kehati-hatian, karena kriptografi lattice relatif baru dan kurang teruji dibandingkan skema klasik. Parameter yang lebih besar memitigasi risiko dari potensi kemajuan dalam kriptanalisis lattice, yang masih akan menyisakan ukuran kunci yang lebih kecil sebagai target yang lebih empuk.

Alternatif

ML-DSA dipilih dibandingkan alternatif seperti FN-DSA (Falcon) karena:

- Kompleksitas implementasi FN-DSA yang lebih besar (misalnya, memerlukan operasi floating-point, yang tidak ramah blockchain)
- Kurangnya pembuatan kunci deterministik dalam spesifikasinya
- Statusnya yang belum difinalisasi pada saat pengembangan

Opsi berbasis hash seperti SLH-DSA ditolak karena ukuran signature-nya yang bahkan lebih besar (melebihi 17 KB). Crypto-agility (kemampuan untuk menukar skema signature yang berbeda) dibangun ke dalam Substrate, sehingga relatif mudah untuk menambahkan alternatif ini di masa mendatang jika keadaan menuntut.

Meskipun ML-DSA-87 menghasilkan kunci dan signature yang lebih besar, hal ini dapat dikelola dalam jaringan tahap awal Quantus, di mana penyimpanan belum menjadi hambatan, dan optimasi masa depan seperti wormhole address melalui zero-knowledge proof akan mengatasi penskalaan.

Untuk detail teknis tentang implementasi, lihat QIP-0006.

LibP2P

Quantus Network mengamankan komunikasi node peer-to-peer (P2P) menggunakan kombinasi ML-DSA untuk autentikasi dan ML-KEM (Module-Lattice-based Key Encapsulation Mechanism, sebelumnya CRYSTALS-Kyber) untuk enkripsi.

Integrasi ini memperluas PQC ke tumpukan jaringan libp2p, memodifikasi komponen inti untuk ketahanan kuantum: menggunakan signature ML-DSA-87 untuk identitas peer dan ML-KEM-768 untuk keamanan transport (memperluas handshake Noise dengan pesan KEM tambahan untuk rahasia bersama yang tahan kuantum).

Lapisan P2P sering diabaikan dalam analisis keamanan kuantum. Autentikasi peer itu penting, tetapi hal terburuk yang bisa dilakukan penyerang di tingkat peer adalah meniru identitas node dan mengirim pesan yang tidak valid, yang dapat mengakibatkan denial-of-service. Serangan ini sudah dimitigasi oleh fakta bahwa node umumnya tidak dipercaya dalam model blockchain dan node dapat dengan mudah mengganti kunci mereka jika serangan terdeteksi. Demikian pula, mendekripsi komunikasi P2P memberikan manfaat terbatas bagi penyerang (misalnya, melacak jalur transaksi, dimitigasi oleh proxy atau Tor), dan sebagian besar data menjadi publik secara on-chain.

Meskipun demikian, mengamankan lapisan P2P secara kuantum melindungi dari penyadapan, serangan man-in-the-middle, dan dekripsi kuantum, memastikan bahwa gossip node, propagasi blok, dan interaksi jaringan lainnya tetap rahasia dan tahan rusak untuk masa depan yang dapat diprediksi.

Untuk detail teknis tentang implementasi, lihat QIP-0004.

Penskalaan PQC

Untuk mengatasi tantangan penskalaan yang melekat dalam kriptografi pasca-kuantum, **Quantus Network memperkenalkan skema signature pasca-kuantum teragregasi yang inovatif yang disebut "Wormhole Addresses"**. Sistem ini memanfaatkan zero-knowledge proofs (ZKPs) yang dihasilkan melalui sistem pembuktian Plonky2 (pada dasarnya STARKs) untuk memindahkan verifikasi saldo ke luar rantai (off-chain), memungkinkan chain untuk memverifikasi satu bukti ringkas tanpa memproses signature individu.

Wormhole Addresses memungkinkan verifikasi sejumlah besar transaksi dengan satu bukti, dengan input publik (misalnya, nullifier, storage root, alamat keluar, dan jumlah) menjadi faktor pembatas utama. Ini mengurangi permintaan penyimpanan per transaksi yang diamortisasi menjadi **sekitar 256 byte tambahan per transaksi, jauh lebih kecil daripada skema signature PQC mana pun yang diketahui**.

Keamanan kuantum dari skema ini berasal dari penggunaan fungsi hash aman Poseidon2 untuk komitmen melalui FRI (Fast Reed-Solomon Interactive Oracle Proofs), alih-alih pasangan kurva eliptik yang rentan kuantum yang umum digunakan dalam SNARKs.

Selain itu, rahasia autentikasi disembunyikan di balik Poseidon2. Karena fungsi hash yang aman hanya diperlemah secara kuadratik oleh algoritma Grover, bukan rusak, bukti preimage hash dapat berfungsi sebagai signature pasca-kuantum yang ringan dalam konteks ZK, mirip dengan skema berbasis hash seperti SPHINCS+.

Alur Klien / Pembukti (Prover)

Pengguna menghasilkan alamat yang terbukti tidak dapat dibelanjakan dengan melakukan double-hashing pada salt yang digabungkan dengan rahasia:

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

Konstruksi ini mencegah positif palsu (misalnya, salah mengira kunci publik hash tunggal sebagai alamat yang tidak dapat dibelanjakan) karena dalam Substrate (dan umumnya) alamat blockchain adalah hash tunggal dari kunci publik, yang diturunkan dari kunci privat melalui beberapa operasi aljabar, bukan melalui hash yang aman. Oleh karena itu, keamanan konstruksi bermuara pada menemukan preimage-dari-preimage dari hash yang aman. Token yang dikirim ke alamat ini secara efektif dibakar. Mereka tidak dapat dibelanjakan karena tidak ada kunci privat untuk alamat yang menerimanya. Oleh karena itu, koin-koin ini dapat dicetak ulang tanpa menggembungkan pasokan.

Untuk setiap transfer, objek penyimpanan TransferProof dibuat, berisi detail seperti jumlah transfer global yang unik. Dompet pengguna menghasilkan bukti penyimpanan Merkle-Patricia-Trie (MPT) dari storage root header blok terbaru ke leaf untuk TransferProof ini.

Nullifier dihitung:

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

Untuk mencegah pengeluaran ganda (double-spend), dengan rahasia yang diturunkan secara deterministik dari seed dompet untuk retensi.

Alur Agregator

Pihak mana pun (klien, penambang, atau pihak ketiga) dapat mengagregasi beberapa bukti menggunakan rekursi Plonky2, membentuk pohon bukti di mana setiap bukti induk

adalah verifikasi dari bukti anak, dengan input publik bukti anak diagregasi:

- nullifier diteruskan tanpa perubahan
- alamat keluar dideduplikasi
- hash blok terbukti terkait dan kemudian semua kecuali yang terbaru dibuang
- jumlah untuk alamat keluar duplikat dijumlahkan Rekursi ini mendukung agregasi hierarkis, secara drastis mengurangi data on-chain.

Alur Chain / Verifikator

Jaringan memverifikasi bukti agregat dengan memeriksa:

- hash blok ada di chain dan terbaru
- keunikan nullifier (untuk mencegah pengeluaran ganda)
- validitas bukti

Sirkuit ZK menegakkan:

- kebenaran bukti penyimpanan
- akurasi perhitungan nullifier
- ketidakbelanjaan alamat
- kecocokan saldo antara input dan output
- keterkaitan header blok

Plonky2 dipilih karena alasan berikut:

- sudah diaudit
- pasca-kuantum
- tanpa trusted setup
- pembuktian/verifikasi yang efisien
- agregasi bukti yang mulus
- implementasi asli Rust
- kompatibel dengan lingkungan no-std Substrate

Sorotan kinerja meliputi:

Bukti rekursif dalam 170 milidetik dan ukuran ringkas (100 KB per bukti agregat), memungkinkan perolehan throughput yang masif.

Dalam kasus optimal dengan blok 5 MB dan semua transaksi menuju ke output yang sama, **Wormhole Addresses dapat mengemas sekitar 153.000 transaksi ke dalam satu blok** (4,9 MB / 32 byte per nullifier), peningkatan 223x dibandingkan sekitar 685 transaksi ML-DSA mentah (5 MB / 7,3 KB masing-masing).

Catatan Keamanan

Risiko potensial mencakup bug inflasi dari implementasi sirkuit/verifikasi yang salah, meskipun hal ini akan terdeteksi secara ekonomi jika koin yang dicetak ulang melebihi saldo alamat pengiriman nol. Pengguna secara opsional dapat membuktikan sebuah alamat adalah wormhole dengan mempublikasikan hash pertama tanpa mengungkapkan rahasianya. Transaksi verifikasi tidak ditandatangani, sehingga denial-of-service melalui transaksi yang gagal perlu dimitigasi secara non-finansial. Perhitungan pasokan token dipertahankan, karena pencetakan ulang muncul sebagai koin baru tetapi mempertahankan jaminan pasokan maksimum melalui pembakaran.

Untuk detail teknis lebih lanjut tentang implementasi, lihat QIP-0005.

Mekanisme Konsensus

Quantus Network menggunakan algoritma konsensus Proof-of-Work (PoW) yang mempertahankan properti yang diinginkan dari algoritma konsensus Bitcoin sambil meningkatkan kompatibilitas dengan sistem ZK-proof dengan mengganti SHA-256 dengan Poseidon2.

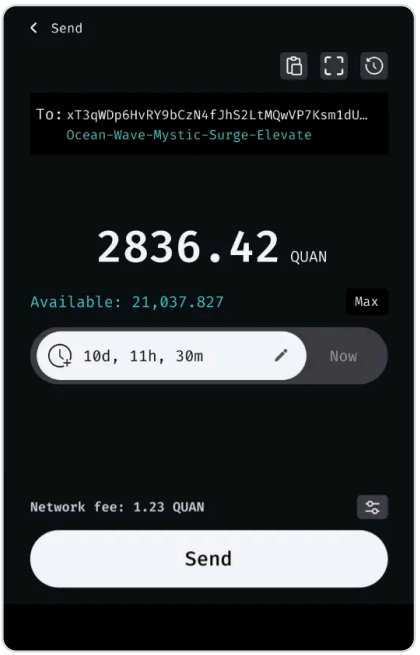
Penting untuk dicatat bahwa perubahan ini tidak dilakukan untuk keamanan kuantum. Fungsi hash kriptografi seperti SHA-256 diperlemah tetapi tidak dihancurkan oleh algoritma kuantum, terutama algoritma Grover. Beberapa skema signature pasca-kuantum menggunakan hash aman sebagai blok pembangun karena alasan ini.

Poseidon2 adalah penyempurnaan dari fungsi hash Poseidon. Membuat SNARK atau STARK untuk komputasi yang melibatkan fungsi hash tradisional seperti SHA-256 seringkali membutuhkan hampir 100x jumlah gerbang dibandingkan dengan menggunakan Poseidon, yang sepenuhnya bergantung pada fungsi aljabar di atas elemen field, alih-alih operasi tingkat bit. Kami menggunakan Goldilocks field untuk Poseidon2 dan Plonky2 untuk memaksimalkan efisiensi.

Pelestarian Kekayaan

Ada banyak risiko dalam mengelola kunci mata uang kripto. Kebanyakan dari mereka dapat dihindari. Quantus Network menanamkan kemudahan penggunaan ke dalam chain itu sendiri, memungkinkan non-ahli untuk bertransaksi dengan tenang.

Transaksi yang Dapat Dianulir (Reversible)

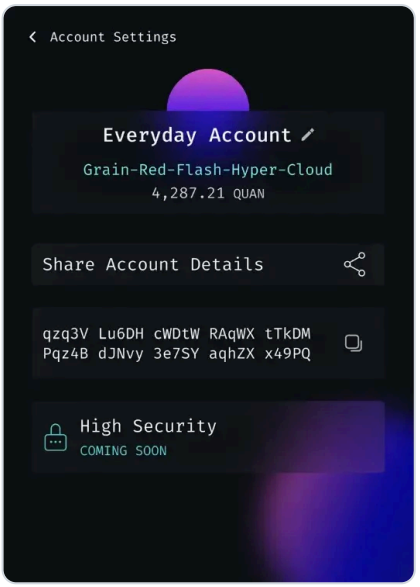


Quantus Network menawarkan transaksi yang dapat dibatalkan yang dapat dikonfigurasi pengguna, memungkinkan pengirim untuk menetapkan jendela waktu di mana mereka dapat membatalkan transfer keluar, meningkatkan pencegahan pencurian dan koreksi kesalahan tanpa mengorbankan ireversibilitas inti blockchain. Memanfaatkan "scheduler pallet" Substrate yang dimodifikasi yang menggunakan stempel waktu untuk penundaan intuitif, sistem ini memungkinkan klien untuk menjadwalkan transfer melalui antarmuka sederhana, menampilkan hitung mundur di dompet baik untuk pengirim (dengan tombol batal) maupun penerima (menunjukkan penyelesaian jika tidak dibatalkan). Ini menyeimbangkan finalitas cepat untuk perdagangan dengan fleksibilitas bagi pengguna yang khawatir membuat kesalahan atau ingin melakukan setoran dengan itikad baik tanpa layanan escrow.

Transaksi yang dapat dibatalkan membentuk blok pembangun yang kuat untuk protokol keamanan baru sambil mempertahankan desentralisasi melalui penegakan on-chain.

Untuk detail teknis lebih lanjut, lihat QIP-0009.

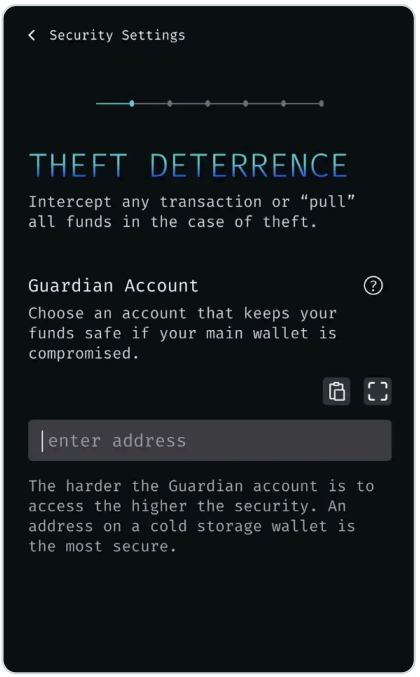
Check-Phrases



Quantus Network memperkenalkan “check-phrases,” checksum yang aman secara kriptografis dan dapat dibaca manusia untuk alamat blockchain dan data lain yang memerlukan verifikasi manusia. **Dengan melakukan hashing pada alamat untuk menghasilkan urutan kata pendek yang mudah diingat dari daftar mnemonik BIP-39, check-phrase memungkinkan pemeriksaan integritas yang cepat dan bebas kesalahan, melindungi dari salah ketik, perusakan, dan serangan seperti peracunan alamat (address poisoning)**. Alat ini memungkinkan pengguna untuk memverifikasi alamat dengan percaya diri selama transfer tanpa bergantung pada tampilan yang terpotong atau checksum yang lemah. Fungsi derivasi kunci 50.000 iterasi digunakan untuk memastikan bahwa pembuatan rainbow table untuk checksum tertentu sangat mahal. Tentu saja, untuk transaksi besar, pengguna harus tetap memeriksa setiap huruf alamat secara manual untuk kebenarannya.

Untuk detail teknis lebih lanjut, silakan lihat QIP-0008.

Akun Keamanan Tinggi



Quantus Network menawarkan kemampuan untuk meningkatkan akun apa pun menjadi "akun keamanan tinggi" yang memberlakukan periode pembatalan wajib pada semua transfer keluar, memungkinkan akun "wali" (guardian) yang ditunjuk seperti dompet perangkat keras, multisig, atau bahkan pihak ketiga tepercaya pilihan pengguna untuk secara eksklusif membatalkan transaksi mencurigakan selama periode pembatalan, mengirimkan dana ke wali alih-alih pengirim atau penerima. Fitur permanen yang bersifat opsional ini dibangun di atas transfer yang dapat dibatalkan, di mana pengguna menentukan penundaan dan pencegat saat aktivasi, mencegah pencuri menonaktifkannya.

Pencegat itu sendiri dapat berupa akun keamanan tinggi lainnya dengan walinya sendiri, memungkinkan hierarki yang dapat disusun di mana setiap wali memiliki izin yang lebih tinggi daripada akun yang dilindunginya. Desain ini meniru pembatalan yang diperintahkan pengadilan pada keuangan tradisional tetapi dengan kontrol pengguna. Ini menyeimbangkan keamanan dan kenyamanan untuk akun bernilai tinggi, memberikan waktu untuk mendeteksi dan menanggapi aktivitas yang tidak sah tanpa mengorbankan finalitas blockchain untuk aliran yang sah.

Untuk detail teknis lebih lanjut, lihat QIP-0011.

Pemulihan Kunci

Banyak kekayaan kripto telah terkubur bersama pemiliknya. Quantus Network menawarkan cara sederhana untuk menentukan alamat pemulihan yang dapat menarik dana Anda kapan saja, tergantung pada penundaan tetap. Selama waktu ini, pemilik dapat menolak pemulihan jika mereka memiliki akses ke kunci tersebut. Fitur ini memungkinkan kelangsungan hidup: pengguna memiliki wasiat on-chain tanpa memerlukan pengadilan atau harta warisan.

HD-Lattice

Dompet Hierarchical Deterministic (HD) adalah standar industri untuk blockchain, memungkinkan pengguna untuk mencadangkan satu seed phrase untuk semua kunci, meningkatkan keamanan dan kenyamanan dibandingkan pencadangan manual per tindakan.

Mengadaptasi ini ke skema lattice seperti Dilithium melibatkan dua tantangan:

- Output HMAC-SHA512 tidak dapat secara langsung membentuk kunci privat lattice, yang memerlukan polinomial "basis yang baik" melalui sampling penolakan (rejection sampling).
- Derivasi kunci non-hardened mengandalkan penambahan kurva eliptik, yang tidak ada dalam lattice (kunci publik tidak tertutup di bawah operasi aljabar apa pun).

Quantus Network mengatasi masalah pertama dengan menggunakan output HMAC sebagai entropi untuk membangun kunci privat secara deterministik, bukan sebagai kunci privat itu sendiri. Masalah kedua kurang kritis dan tetap menjadi pertanyaan penelitian terbuka apakah kriptografi lattice dapat diadaptasi untuk mengatasinya.

Untuk detail teknis lebih lanjut, lihat QIP-0002.

Tokenomics dan Tata Kelola

Quantus Network ada dalam lingkungan yang berubah, dan kami tidak dapat berasumsi bahwa kami akan melakukan segalanya dengan benar pada percobaan pertama. Untuk alasan ini, kami memilih titik awal yang sederhana dan membiarkan sistem tata kelola melakukan perubahan saat informasi baru diperoleh. Desain ini membuat blockchain menjadi entitas hidup yang dapat beradaptasi dengan lingkungannya sesuka hati. Secara khusus, proses tata kelola Substrate memungkinkan perubahan mendalam pada chain dengan koordinasi minimal di antara berbagai node-runner.

Hadiah Blok (Block Rewards)

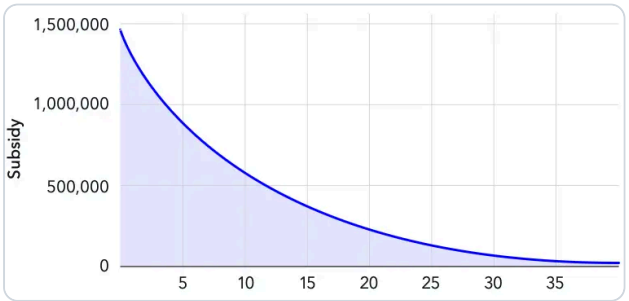
Quantus Network menggunakan model tokenomics langsung yang meniru Bitcoin. Ada pasokan maksimum 21.000.000 koin dan heuristik sederhana menentukan hadiah setiap blok.

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

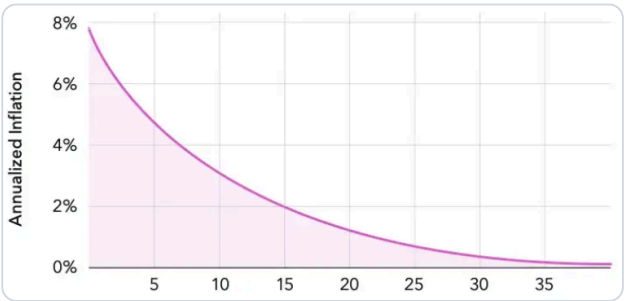
Heuristik ini membentuk kurva peluruhan eksponensial yang mulus karena block_reward berkontribusi pada current_supply yang mengurangi block_reward yang dihitung pada blok berikutnya.

Setiap pembakaran dari biaya atau lainnya mengurangi current_supply dan pada dasarnya menjadi bagian dari anggaran untuk hadiah blok. Konstanta dipilih sedemikian rupa sehingga, tanpa adanya pembakaran, 99% koin akan dipancarkan dalam waktu sekitar 40 tahun.

Hadiah Blok / Tahun



Inflasi / Tahun



Alokasi Investor

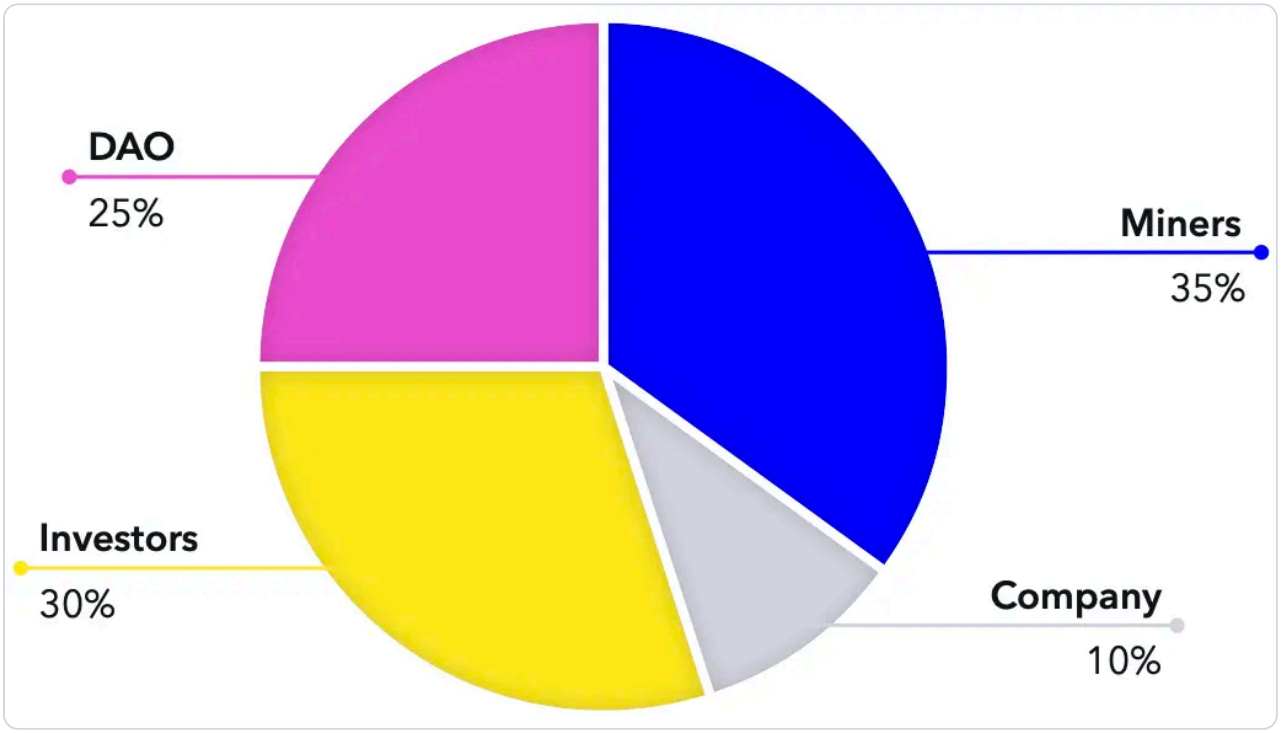
Quantus Network dibangun dengan bantuan investor malaikat (angel investors) yang mengambil risiko besar dalam mendanainya. Untuk menghindari kelebihan pasokan yang diciptakan oleh penguncian investor (investor-lockups), kami membuat semua investor, publik dan swasta, likuid pada hari pertama. Alokasi ini akan menjadi satu-satunya "pre-mine". Semua token lainnya harus ditambang untuk ada. Tergantung pada keberhasilan penjualan publik, bagian ini akan mewakili 20-30% dari total pasokan.

Alokasi Perusahaan

Untuk memberi kompensasi kepada tim karena mengambil risiko membangun teknologi baru tanpa janji keberhasilan, kami akan membagi hadiah blok menjadi dua bagian. Bagian pertama akan diberikan kepada penambang. Selama kurang lebih empat tahun, bagian kedua akan diberikan kepada perusahaan. Ini memberikan jadwal vesting de facto sekitar 10% dari total pasokan kepada perusahaan. Selama waktu ini, para penambang mendapatkan jumlah koin yang baru dicetak yang sama.

Setelah titik itu, bagian hadiah blok perusahaan akan dialihkan ke perbendaharaan yang dikelola oleh pemegang token, yang pada dasarnya membentuk DAO.

Perkiraan Alokasi Pasokan



Biaya Transaksi

Transaksi standar akan memiliki biaya yang diberikan kepada penambang, memberikan insentif untuk menyertakan transaksi. Transaksi yang dibatalkan dari akun keamanan tinggi akan dikenakan biaya berbasis volume sebesar 1% yang dibagi, dengan setengahnya diberikan kepada penambang dan setengahnya dibakar, masuk ke anggaran keamanan masa depan. Transaksi yang melalui sistem agregasi zk juga akan dikenakan biaya berbasis volume sebesar 0,1%, yang akan dibagi antara penambang, agregator bukti, dan pembakaran.

Pemutakhiran Tanpa Fork (Forkless Upgrades)

Quantus Network mendukung pemutakhiran "tanpa fork" melalui pemutakhiran runtime Substrate, memungkinkan logika inti blockchain ("runtime") untuk berkembang tanpa hard fork yang dapat mengganggu jaringan atau memecah komunitas. Hal ini dicapai melalui referendum tata kelola on-chain, di mana proposal yang disetujui memicu pertukaran runtime, yang pada dasarnya mengganti blob kode WASM yang ada dengan yang baru dalam satu blok, memastikan kelangsungan status dan operasi. Jalur pemutakhiran ini meminimalkan waktu henti dan risiko, memberdayakan komunitas untuk menyempurnakan protokol secara iteratif.

Sistem Tata Kelola

Quantus Network mewarisi kerangka tata kelolanya dari sistem OpenGov Polkadot melalui Substrate. Pemegang token berpartisipasi melalui conviction voting, di mana mereka setuju untuk mengunci aset mereka untuk periode yang bervariasi guna memperkuat bobot suara mereka. Penguatan ini dapat berkisar dari 1x (tanpa penguncian) hingga 6x (penguncian maksimum). Desain ini mendorong keselarasan jangka panjang dengan mengaitkan pengaruh dengan komitmen.

Proposal dikategorikan ke dalam beberapa jalur pemungutan suara yang disebut "origins". Setiap origin memiliki parameter yang disesuaikan seperti ambang persetujuan (misalnya, supermayoritas untuk perubahan berdampak tinggi), setoran minimum untuk mencegah spam, periode persiapan/pemberlakuan, dan garis waktu keputusan untuk mencegah kebuntuan. Desain multi-jalur ini memungkinkan pemrosesan paralel dari berbagai referendum, mulai dari pengeluaran perbendaharaan rutin hingga pemutakhiran runtime yang kritis.

Technical Collective adalah kelompok ahli teknis terpilih yang berfungsi sebagai badan khusus untuk mengusulkan, meninjau, atau memasukkan masalah teknis mendesak ke dalam daftar putih (whitelist), mempercepatnya melalui jalur khusus sambil tetap mempertahankan pengawasan komunitas.

Quantus mengadopsi sistem ini tanpa modifikasi tetapi dimulai dengan pengaturan minimalis untuk menghindari kompleksitas di tahap awal. Awalnya, hanya jalur Technical Collective yang aktif, yang akan digunakan untuk keputusan yang mengikat dan berhak istimewa tinggi seperti pemutakhiran protokol atau penyesuaian parameter.

Nantinya kami akan memperkenalkan jalur pemungutan suara komunitas yang tidak mengikat untuk mengukur sentimen pada topik yang tidak dapat ditegakkan, seperti saran fitur atau jajak pendapat ekosistem. Sistem ini akan menjadi mengikat ketika perusahaan menyerahkan jaringan ke DAO.

Pendekatan bertahap ini memungkinkan jaringan untuk berkembang secara organik melalui pemungutan suara tata kelola di masa depan tanpa membebani pengguna dengan kompleksitas yang tidak perlu di awal.

Roadmap

Heisenberg Inception

DESEMBER 2024

Pendanaan Diamankan, Substrate Dipilih

Resonance Alpha

JULI 2025

Testnet Publik, Signature Dilithium, Transaksi yang Dapat Dibatalkan

Schrödinger Beta

OKTOBER 2025

Fitur Lengkap, Siap untuk Audit

Dirac Beta

NOVEMBER 2025

PoW diubah ke Poseidon2, Audit Ditangani

Planck Beta

JANUARI 2026

Akun Keamanan Tinggi, Multisig, Dompet Perangkat Keras

Bell Mainnet

KUARTAL 1 2026

Peluncuran Mainnet

Fermi Upgrade

KUARTAL 2 2026

Agregasi ZK

Risiko

Membangun Quantus Network datang dengan risiko yang melekat.

- **Masalah Implementasi:** Cacat dalam logika perangkat lunak dapat menyebabkan kegagalan serius bahkan pada sistem yang dirancang paling baik sekalipun.
- **Masalah Pemilihan Algoritma NIST:** Potensi cacat atau pintu belakang (backdoor) dalam standar pasca-kuantum yang dipilih (misalnya, ML-DSA, ML-KEM) yang dapat muncul setelah standardisasi. Dalam kasus terburuk, cacat seperti itu akan memungkinkan penyerang untuk memalsukan signature dengan menurunkan kunci privat dari kunci publik, yang mewakili mode kegagalan katastrofik dari chain. Jika cacat seperti itu dipublikasikan, Quantus Network dapat ditingkatkan ke algoritma baru, tetapi jika cacat tersebut dieksploitasi secara hemat, mereka mungkin tidak akan pernah ditemukan.
- **Garis Waktu Komputasi Kuantum:** Terobosan kuantum mungkin tiba jauh lebih lambat dari yang diantisipasi, menunda kebutuhan akan PQC; sebaliknya, pengembangan rahasia (misalnya oleh pemerintah) dapat menyebabkan ancaman mendadak jika komunitas blockchain gagal memperbarui dengan cepat.
- **Pertimbangan Lain:** Hambatan adopsi umum, ketidakpastian peraturan dalam keuangan/blockchain, dan volatilitas inheren dari ekosistem kripto.

Penutup

QUANTUS

Kami percaya pada kekuatan protokol terbuka, proof-of-work, dan kepemilikan berdaulat. Aplikasi Quantus Network, tersedia di desktop dan seluler, memungkinkan pengguna menyimpan aset digital, menambang blok baru, dan berpartisipasi dalam masa depan keuangan yang lebih adil tanpa perantara.

Kami berkomitmen pada transparansi, privasi, dan pemberdayaan individu melalui alat penyimpanan mandiri (self-custodial) yang aman.