quantus

uang aman kuantum, terenkripsi

DITERBITKAN
21 maret 2026

VERSI
0.3.3

KLASIFIKASI
public

Whitepaper ini disediakan hanya untuk tujuan informasi dan bukan merupakan penawaran untuk menjual, ajakan untuk membeli, atau rekomendasi untuk sekuritas, investasi, atau produk keuangan apa pun. Pembaca harus melakukan uji tuntas sendiri dan berkonsultasi dengan profesional yang berkualifikasi sebelum membuat keputusan investasi apa pun. Quantus Network tidak memberikan pernyataan atau jaminan mengenai keakuratan atau kelengkapan informasi di sini.

DAFTAR ISI

01

pendahuluan

ancaman kuantum

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

> tanpa peningkatan tahan kuantum yang proaktif, ekonomi kripto bernilai triliunan dolar berisiko devaluasi mendadak akibat serangan semacam itu.

proposisi nilai unik

Dinamai dari kata Latin untuk “berapa banyak”, Quantus Network menghadirkan uang privat yang skalabel dan aman secara kuantum. Quantus bukan platform smart contract serba guna. Seperti restoran dengan beberapa menu yang sangat disempurnakan, Quantus menyediakan:

— Tanda tangan pasca-kuantum untuk semua transaksi

— Tanda tangan dan enkripsi Pasca-Kuantum (ML-DSA dan ML-KEM) untuk mengamankan koneksi peer

— Bukti tanpa pengetahuan (zero-knowledge) pasca-kuantum untuk penskalaan

— Akun Keamanan Tinggi untuk mencegah pencurian dan memungkinkan pemulihan dari kesalahan

— Frasa pemeriksaan yang mudah dibaca manusia untuk verifikasi alamat yang mudah

Keputusan untuk fokus pada uang privat yang skalabel dan aman secara kuantum berasal dari ancaman yang ditimbulkan CRQC terhadap industri dan ketidakmampuan Bitcoin untuk mengatasi tantangan ini.

02

ancaman kuantum terhadap blockchain

dasar-dasar komputasi kuantum

Komputer kuantum memanfaatkan prinsip seperti superposisi dan keterikatan untuk melakukan komputasi yang sulit bagi mesin klasik. Berbeda dengan bit klasik, yang bernilai 0 atau 1, bit kuantum (qubit) dapat berada dalam banyak keadaan 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 1994 oleh Peter Shor, memberikan metode waktu polinomial untuk memfaktorkan bilangan bulat besar dan menyelesaikan masalah logaritma diskrit pada komputer kuantum. Algoritma ini mengeksploitasi Quantum Fourier Transform (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 ~2.000 qubit logis [6][7]

[8][9]) dapat menurunkan kunci privat dari kunci publik dalam waktu polinomial $O(n^3)$ — percepatan ekstrem yang membuat sistem rentan usang dalam semalam. [1]

Algoritma Grover, diusulkan oleh Lov Grover pada 1996, menawarkan percepatan kuadratik untuk masalah pencarian tak terstruktur, mengurangi waktu pencarian dari $O(n)$ menjadi $O(\sqrt{n})$ operasi. Meskipun tidak se dahsyat Shor untuk kriptografi asimetris, Grover mempengaruhi primitif simetris seperti fungsi hash dan enkripsi AES, secara efektif membagi dua tingkat keamanan (misalnya kunci 256-bit berperilaku seperti 128 bit terhadap serangan kuantum). Serangan ini dimitigasi dengan menggandakan bit keamanan, bukan mengubah skema kriptografi. Selain itu, percepatan kuadratik Grover tidak praktis karena persyaratan qubit dan gerbang yang tinggi, membutuhkan miliaran operasi berurutan dengan paralelisasi terbatas, sehingga tidak layak untuk pembalikan dunia nyata bahkan pada perangkat keras masa depan. [2]

empat kategori ancaman

01 - memalsukan tanda tangan digital

Algoritma Shor secara langsung mengancam tanda tangan berbasis ECC yang digunakan di sebagian besar blockchain (misalnya kurva secp256k1 Bitcoin), memungkinkan penyerang menyamar sebagai pengguna dan mengotorisasi transaksi palsu. Kemampuan seperti

itu akan merupakan kegagalan kritis dari fitur paling dasar sebuah blockchain.

02 - memalsukan bukti palsu dalam sistem zero-knowledge

Banyak bukti zero-knowledge, seperti dalam zk-SNARKs untuk keuangan berfokus privasi, bergantung pada kesulitan logaritma diskrit melalui pasangan kurva eliptik untuk komitmen. Shor dapat memungkinkan pembuatan bukti tidak valid yang tampak valid, yang dapat memungkinkan penyerang mencetak koin baru atau memalsukan keadaan Layer-2 (L2).

03 - mendekripsi informasi rahasia

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

04 - membalikkan fungsi hash

Algoritma Grover dapat mempercepat serangan preimage pada hash seperti SHA-256, 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, PQC memperkenalkan hambatan penskalaan signifikan karena desain inheren algoritma ini. Berbeda dengan skema kurva eliptik, yang mengandalkan struktur matematika ringkas, primitif PQC memerlukan parameter lebih besar untuk mempertahankan keamanan terhadap penyerang klasik dan kuantum. Hal ini menghasilkan kunci publik, kunci privat, dan tanda tangan yang jauh lebih besar, sering berorde magnitudo. Tabel berikut mengilustrasikan ukuran tipikal untuk ML-DSA pada tingkat keamanan pasca-kuantum 128-bit dibandingkan rekan klasik seperti ECDSA 256-bit: [10]

ALGORITMA	KUNCI PUBLIK	KUNCI PRIVAT	TANDA TANGAN
ML-DSA-87 (Dilithium)	2,592 bytes	4,896 bytes	4,627 bytes
ECDSA (256-bit)	32 bytes	32 bytes	65 bytes

Ukuran pada tingkat keamanan pasca-kuantum 128-bit. Sumber: Open Quantum Safe Project [10]

Seperti ditunjukkan, tanda tangan ML-DSA dapat lebih dari 70 kali lebih besar daripada setara ECDSA, dan kunci publik lebih dari 80

kali lebih besar. Keluarga PQC lain memperparah hal ini: skema berbasis hash seperti SPHINCS+ dapat menghasilkan tanda tangan hingga 41 KB, sementara varian lattice yang dioptimalkan ukuran seperti FALCON masih melebihi ukuran klasik dengan kelipatan signifikan.

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

> **CATATAN**
>
> 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.

03

krisis migrasi

masalah koordinasi

Budaya konservatif Bitcoin menolak perubahan protokol. Peningkatan PQC mana pun akan memerlukan konsensus tentang isu kontroversial seperti timeline migrasi, potensi penyitaan koin, dan peningkatan ukuran blok. Bahkan jika komunitas setuju, setiap pengguna harus memigrasikan koin mereka ke alamat aman kuantum baru. Migrasi memerlukan tindakan dari setiap pemegang kripto, banyak di antaranya kehilangan akses ke dompet atau tidak menyadari ancaman.

Isu ini ada di setiap blockchain publik, tetapi sangat menantang bagi Bitcoin karena kurangnya kepemimpinan yang jelas dan filsafat pengerasan teknis.

masalah koin yang hilang

Perkiraan $250 miliar hingga $500 miliar nilai Bitcoin tidak dapat diakses secara permanen karena kunci yang hilang, pemegang yang meninggal, atau dompet yang terlupakan. [3] Koin ini tidak dapat dimigrasikan dan berfungsi sebagai hadiah publik untuk membuat komputer kuantum yang relevan secara kriptografis (CRQC). Penyerang kuantum akan menurunkan kunci privat dari kunci publik

yang tidak dimigrasikan dan kemungkinan membanjiri miliaran dolar BTC ke pasar.

> satu-satunya solusi teknis memerlukan tenggat keras yang membekukan koin yang tidak dimigrasikan — sebuah kemustahilan politik.

Tanpa tenggat seperti itu, hasilnya adalah koin yang tidak dimigrasikan dicuri dan dijual, menghancurkan pasar dan merusak kepercayaan pada jaringan.

masalah timeline migrasi

Tanda tangan pasca-kuantum 20x–80x lebih besar daripada tanda tangan Bitcoin saat ini. Tanpa perubahan arsitektur mendasar, throughput Bitcoin akan runtuh menjadi sebagian kecil dari kapasitas terbatasnya.

Dengan asumsi Bitcoin mengatasi tantangan politik dan teknis, migrasi itu sendiri akan memakan waktu berbulan-bulan atau bertahun-tahun. Setiap pemegang harus mengirim setidaknya satu transaksi untuk memindahkan dana ke alamat aman kuantum. Banyak yang akan mengirim transaksi uji terlebih dahulu. Dengan tanda tangan PQC yang membengkak yang mencekik throughput, jaringan menghadapi antrian yang berlangsung berbulan-bulan atau bertahun-tahun sementara koin rentan kuantum tetap terpapar.

JAWABAN QUANTUS

Tantangan yang bertumpuk ini membuat retrofit keamanan kuantum ke chain yang ada sangat sulit. Quantus Network menghindari ini dengan membangun keamanan kuantum ke dalam chain sejak hari pertama.

04

arsitektur quantus network

fondasi

Quantus Network dibangun di atas Substrate, SDK blockchain yang dikembangkan oleh Parity Technologies, tim di balik Ethereum dan Polkadot. Substrate sangat modular, memungkinkan penggantian komponen dengan mudah sehingga kami dapat fokus pada apa yang membuat Quantus unik.

Quantus meningkatkan Substrate dengan:

— Menambahkan dukungan untuk skema tanda tangan pasca-kuantum

— Meningkatkan keamanan jaringan p2p menjadi pasca-kuantum

— Menambahkan reversibilitas transaksi yang dikontrol pengguna

— Membuat database ramah zk dengan menyelaraskan semua tipe data ke batas elemen lapangan

primitif kriptografi pasca-kuantum

Quantus Network menggunakan PQC yang distandarisasi NIST untuk memastikan keamanan transaksi dan komunikasi jaringan terhadap ancaman kuantum. Inti integritas transaksi adalah **ML-DSA** (Module-Lattice-based Digital Signature Algorithm,

sebelumnya dikenal sebagai CRYSTALS-Dilithium), skema tanda tangan berbasis lattice yang dipilih karena keseimbangan keamanan, efisiensi, dan kemudahan implementasi. ML-DSA memanfaatkan kesulitan masalah seperti Learning With Errors (LWE) dan Short Integer Solution (SIS) pada module lattice, memberikan resistensi kuat terhadap serangan klasik dan kuantum, termasuk dari algoritma Shor. [4]

Untuk tanda tangan transaksi, Quantus mengintegrasikan **ML-DSA-87**, set parameter dengan tingkat keamanan tertinggi (NIST Security Level 5, setara 256-bit klasik dan 128-bit kuantum) untuk melindungi dari kemungkinan terobosan kriptanalisis lattice. Pilihan ini memprioritaskan kehati-hatian, karena kriptografi lattice relatif baru dan kurang teruji di medan perang dibanding skema klasik. Parameter yang lebih besar memitigasi risiko dari kemajuan potensial dalam kriptanalisis lattice, yang masih akan meninggalkan ukuran kunci lebih kecil sebagai target yang lebih lunak.

alternatif yang dipertimbangkan

ML-DSA dipilih dibanding alternatif seperti FN-DSA (Falcon) karena kompleksitas implementasi FN-DSA yang lebih besar (mis. memerlukan operasi floating-point, yang tidak ramah blockchain), tidak adanya generasi kunci deterministik dalam spesifikasinya, dan statusnya yang belum final pada saat pengembangan.

Opsi berbasis hash seperti SLH-DSA tidak dipilih karena ukuran tanda tangan yang bahkan lebih besar (melebihi 17 KB). Crypto-

agility (kemampuan menukar skema tanda tangan berbeda) sudah tertanam dalam Substrate, sehingga relatif mudah menambahkan alternatif ini di tanggal mendatang jika diperlukan.

Meskipun ML-DSA-87 menghasilkan kunci dan tanda tangan lebih besar, ini dapat dikelola di jaringan tahap awal Quantus, di mana penyimpanan belum menjadi bottleneck, dan optimisasi seperti alamat wormhole melalui bukti zero-knowledge akan mengatasi penskalaan.

Untuk detail teknis implementasi lihat QIP-0006.

libp2p - jaringan aman kuantum

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 stack jaringan libp2p, memodifikasi komponen inti untuk resistensi kuantum: menggunakan tanda tangan ML-DSA-87 untuk identitas peer dan ML-KEM-768 untuk keamanan transport (memperpanjang handshake Noise dengan pesan KEM tambahan untuk rahasia bersama tahan kuantum). [5]

Lapisan P2P sering diabaikan dalam analisis keamanan kuantum. Autentikasi peer penting, tetapi yang terburuk yang dapat dilakukan penyerang di level peer adalah menyamar sebagai node dan mengirim pesan tidak valid, yang dapat mengakibatkan penolakan

layanan. Serangan ini sudah dimitigasi oleh fakta bahwa node umumnya tidak dipercaya dalam model blockchain dan node dapat dengan mudah mengganti kunci jika serangan terdeteksi. Demikian pula, mendekripsi komunikasi P2P memberikan manfaat penyerang terbatas (mis. melacak jalur transaksi, dimitigasi oleh proxy atau Tor), dan sebagian besar data menjadi publik di chain.

Namun, mengamankan lapisan P2P secara kuantum melindungi dari penyadapan, serangan man-in-the-middle, dan dekripsi kuantum, memastikan gossip node, propagasi blok, dan interaksi jaringan lainnya tetap rahasia dan bebas gangguan untuk masa mendatang.

Untuk detail teknis implementasi lihat QIP-0004.

penskalaan pqc - alamat wormhole

Untuk mengatasi tantangan penskalaan yang melekat dalam kriptografi pasca-kuantum, Quantus Network memperkenalkan skema tanda tangan pasca-kuantum agregatif inovatif bernama **“Wormhole Addresses”**. Sistem ini memanfaatkan bukti zero-knowledge (ZKP) yang dihasilkan melalui sistem pembuatan bukti Plonky2 (pada dasarnya STARKs) untuk memindahkan verifikasi saldo off-chain, memungkinkan chain memverifikasi satu bukti ringkas tanpa memproses tanda tangan individu. Wormhole Addresses memungkinkan verifikasi sejumlah besar transaksi dengan satu bukti, dengan input publik (mis. nullifier, akar penyimpanan, alamat keluar, dan jumlah) menjadi faktor pembatas

utama. Ini mengurangi kebutuhan penyimpanan per transaksi yang diamortisasi menjadi sekitar 256 byte tambahan per transaksi, jauh lebih kecil daripada skema tanda tangan PQC yang diketahui.

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

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

alur klien / prover

Pengguna menghasilkan alamat yang terbukti tidak dapat dibelanjakan dengan menggandakan hash garam yang digabungkan dengan rahasia:

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

Konstruksi ini mencegah positif palsu (mis. mengira kunci publik hash tunggal sebagai alamat yang tidak dapat dibelanjakan) karena di Substrate (dan umumnya) alamat blockchain adalah hash tunggal dari kunci publik, yang diturunkan dari kunci privat melalui operasi aljabar tertentu, bukan melalui hash aman. Keamanan konstruksi

karenanya berkurang menjadi menemukan preimage-dari-preimage dari hash aman. Token yang dikirim ke alamat ini secara efektif dibakar. Tidak dapat dibelanjakan karena tidak ada kunci privat untuk alamat yang menerimanya. Koin ini karena itu dapat dicetak ulang tanpa membengkak pasokan.

Untuk setiap transfer, objek penyimpanan TransferProof dibuat, berisi detail seperti penghitungan transfer global unik. Dompet pengguna menghasilkan bukti penyimpanan Merkle-Patricia-Trie (MPT) dari akar penyimpanan header blok terkini ke daun untuk TransferProof ini. Nullifier dihitung untuk mencegah double-spend:

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

alur agregator

Pihak mana pun (klien, penambang, atau pihak ketiga) dapat mengagregasi banyak bukti menggunakan rekursi Plonky2, membentuk pohon bukti di mana setiap bukti induk adalah verifikasi bukti anak, dengan input publik anak diagregasi:

— Nullifier lewat tanpa berubah

— Alamat keluar dideduplikasi

— Hash blok dibuktikan terhubung lalu semua kecuali yang terbaru dibuang

— Jumlah untuk alamat keluar duplikat dijumlahkan

alur chain / verifikator

Jaringan memverifikasi bukti agregat dengan memeriksa: hash blok ada di chain dan baru-baru ini, keunikan nullifier (untuk mencegah double- spend), dan validitas bukti. Sirkuit ZK menegakkan kebenaran bukti penyimpanan, akurasi komputasi nullifier, alamat tidak dapat dibelanjakan, kecocokan saldo antara input dan output, dan penautan header blok.

mengapa plonky2

— Sudah diaudit

— Pasca-kuantum

— Tanpa trusted setup

— Pembuatan/verifikasi efisien

— Agregasi bukti mulus

— Implementasi asli Rust

— Kompatibel dengan lingkungan no-std Substrate

> **KINERJA**
>
> Bukti rekursif selesai dalam 170 milidetik dengan ukuran ringkas (100 KB per bukti agregat). Dalam kasus optimal dengan blok 5 MB dan semua transaksi menuju output yang sama, Wormhole Addresses dapat memuat ~153.000 transaksi dalam satu blok (4,9 MB / 32 byte per nullifier) — peningkatan 223x dibandingkan ~685

> transaksi ML-DSA mentah (5 MB / 7,3 KB masing-masing).

catatan keamanan

Risiko potensial termasuk bug inflasi dari implementasi sirkuit/verifikasi yang cacat, meskipun ini akan terdeteksi secara ekonomi jika koin yang dicetak ulang melebihi saldo alamat kirim nol. Pengguna secara opsional dapat membuktikan alamat adalah wormhole dengan mempublikasikan hash pertama tanpa mengungkap rahasia. Transaksi verifikasi tidak ditandatangani, sehingga penolakan layanan melalui transaksi gagal perlu dimitigasi non-keuangan. Perhitungan pasokan token terjaga, karena cetak 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 sifat menguntungkan konsensus Bitcoin sementara meningkatkan kompatibilitas dengan sistem bukti ZK dengan mengganti SHA-256 dengan **Poseidon2**.

Penting, perubahan ini tidak dilakukan untuk keamanan kuantum. Fungsi hash kriptografis seperti SHA-256 dilemahkan tetapi tidak

dimusnahkan oleh algoritma kuantum, terutama Grover. Beberapa skema tanda tangan pasca-kuantum menggunakan hash aman sebagai blok bangunan karena alasan ini.

Poseidon2 adalah penyempurnaan fungsi hash Poseidon. Membuat SNARK atau STARK untuk komputasi yang melibatkan hash tradisional seperti SHA-256 sering memerlukan hampir 100x lebih banyak gerbang dibandingkan menggunakan Poseidon, yang sepenuhnya mengandalkan fungsi aljabar atas elemen lapangan, bukan operasi bit.

Kami menggunakan **lapangan Goldilocks** untuk Poseidon2 dan Plonky2. Urutan lapangan Goldilocks muat dalam bilangan bulat tak bertanda 64-bit, yang meningkatkan efisiensi tanpa mengorbankan soundness.

05

pelestarian kekayaan

Ada banyak risiko dalam mengelola kunci kripto. Sebagian besar dapat dihindari.

transaksi reversibel

Quantus Network menawarkan transaksi reversibel yang dapat dikonfigurasi pengguna. Pengirim menetapkan jendela waktu di mana mereka dapat membatalkan transfer keluar. Ini mencegah pencurian dan memperbaiki kesalahan tanpa mengorbankan finalitas. Sistem menggunakan pallet Substrate “scheduler” yang dimodifikasi dengan timestamp. Dompet menampilkan hitung mundur untuk pengirim (dengan tombol batal) dan penerima.

Transaksi reversibel memungkinkan protokol keamanan baru sambil mempertahankan desentralisasi melalui penegakan on-chain.

Untuk detail teknis lebih lanjut lihat QIP-0009.

frasa pemeriksaan

Quantus Network memperkenalkan “check-phrases,” checksum yang dapat dibaca manusia dan aman secara kriptografis untuk alamat blockchain. Alamat di-hash untuk menghasilkan urutan kata pendek yang mudah diingat dari daftar mnemonik BIP-39. Check-

phrases melindungi dari typo, manipulasi, dan serangan racun alamat. Fungsi derivasi kunci 50.000 iterasi membuat serangan rainbow table mahal. Untuk transaksi besar, pengguna tetap harus memverifikasi setiap karakter alamat.

Untuk detail teknis lihat QIP-0008.

akun keamanan tinggi

Akun mana pun dapat ditingkatkan menjadi “akun keamanan tinggi” dengan periode pembalikan wajib pada semua transfer keluar. **Wali** yang ditunjuk (dompet perangkat keras, multisig, atau pihak ketiga tepercaya) dapat membatalkan transaksi mencurigakan selama periode pembalikan, mengirim dana ke wali alih-alih pengirim atau penerima. Fitur opt-in ini permanen setelah diaktifkan, mencegah pencuri menonaktifkannya.

Wali dapat dirantai: wali akun keamanan tinggi dapat sendiri menjadi akun keamanan tinggi dengan walinya sendiri. Ini menciptakan hierarki yang dapat dikomposisikan di mana setiap wali memiliki izin superior terhadap akun yang dilindungi. Desain ini memberi pengguna waktu untuk mendeteksi dan merespons aktivitas tidak sah tanpa mengorbankan finalitas untuk transfer sah.

Untuk detail teknis lebih lanjut lihat QIP-0011.

pemulihan kunci

Banyak kekayaan kripto ikut ke kubur bersama pemiliknya. Quantus Network menawarkan cara sederhana untuk menentukan alamat pemulihan yang dapat menarik dana Anda kapan saja, tunduk pada penundaan tetap. Selama waktu ini, pemilik dapat menolak pemulihan jika mereka memiliki akses ke kunci. Fitur ini memungkinkan survivorship: pengguna memiliki wasiat on-chain tanpa pengadilan atau perwalian.

hd-lattice

Dompet Hierarchical Deterministic (HD) adalah standar industri untuk blockchain, memungkinkan pengguna mencadangkan satu frasa benih untuk semua kunci, meningkatkan keamanan dan kenyamanan dibanding cadangan manual per tindakan. Mengadaptasi ini ke skema lattice seperti Dilithium melibatkan dua tantangan:

— Keluaran HMAC-SHA512 tidak dapat langsung membentuk kunci privat lattice, yang merupakan polinomial yang disampel dari ring dengan properti tertentu.

— Derivasi kunci non-hardened mengandalkan penjumlahan kurva eliptik, yang tidak ada pada lattice (kunci publik tidak tertutup di bawah operasi aljabar apa pun).

Quantus Network mengatasi masalah pertama dengan menggunakan keluaran HMAC sebagai entropi untuk membangun

kunci privat secara deterministik, bukan sebagai kunci privat itu sendiri. Masalah kedua kurang kritis dan tetap pertanyaan riset terbuka apakah kriptografi lattice dapat diadaptasi untuk mengatasinya.

Untuk detail teknis lebih lanjut lihat QIP-0002.

06

tokenomik dan tata kelola

Quantus Network berada di lingkungan yang berubah, dan kami tidak dapat menganggap semuanya benar pada percobaan pertama. Oleh karena itu, kami memilih titik awal sederhana dan memungkinkan sistem tata kelola membuat perubahan seiring informasi baru diperoleh. Desain ini menjadikan blockchain entitas hidup yang dapat beradaptasi pada lingkungannya. Khususnya, proses tata kelola Substrate memungkinkan perubahan mendalam pada chain dengan koordinasi minimal antara berbagai pengelola node.

hadiah blok

Quantus Network menggunakan model tokenomik lugas yang meniru Bitcoin. Ada pasokan maksimum **21.000.000 koin** dan heuristik sederhana menentukan hadiah setiap blok:

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

Heuristik ini membentuk kurva peluruhan eksponensial halus karena block_reward berkontribusi pada current_supply yang mengurangi block_reward yang dihitung pada blok berikutnya. Pembakaran dari biaya atau lainnya mengurangi current_supply dan pada dasarnya menjadi bagian dari anggaran hadiah blok.

Konstanta dipilih sehingga, tanpa pembakaran apa pun, 99% koin akan dikeluarkan dalam sekitar 30 tahun.

alokasi investor

Quantus Network dibangun dengan bantuan investor yang mengambil risiko besar dalam pendanaan. Investor privat tunduk pada jadwal vesting 4 tahun, seperti tim. Investor penjualan publik akan sepenuhnya likuid pada hari pertama. Dana yang terkumpul dalam penjualan publik akan dicocokkan dengan token dan digunakan untuk likuiditas (DEX, CEX, dan market maker). Alokasi investor ini serta likuiditas akan menjadi satu-satunya “pre-mine”. Semua token lain harus ditambang ke dalam keberadaan.

Jika kurang dari maksimum 10% terjual selama penjualan publik, akan ada pengurangan proporsional pada token likuiditas dan sisanya akan dikeluarkan ke penambang melalui hadiah blok.

alokasi perusahaan

Untuk mengompensasi tim karena mengambil risiko membangun teknologi baru tanpa jaminan kesuksesan, sebagian hadiah blok dikirim ke perusahaan selama sekitar empat tahun. Ini memberikan jadwal vesting de facto sekitar **15% dari total pasokan** ke perusahaan.

Setelah itu, bagian perusahaan dari hadiah blok dapat dimatikan, disesuaikan atau dialihkan sesuai suara pemegang token.

biaya transaksi

JENIS TRANSAKSI	STRUKTUR BIAYA	TUJUAN
Standar	Biaya tetap	Penambang
Reversibel (keamanan tinggi)	1% berbasis volume	Dibakar
Agregat ZK	0,1% berbasis volume	50% penambang / 50% dibakar

peningkatan tanpa fork

Quantus Network mendukung peningkatan “tanpa fork” melalui peningkatan runtime Substrate, memungkinkan logika inti blockchain (“runtime”) berkembang tanpa hard fork yang dapat mengganggu jaringan atau memecah komunitas. Ini dicapai melalui referendum tata kelola on-chain, di mana proposal yang disetujui memicu swap runtime — pada dasarnya mengganti blob kode WASM yang ada dengan yang baru dalam satu blok, memastikan kontinuitas status dan operasi. Jalur peningkatan ini meminimalkan downtime dan risiko, memberdayakan komunitas untuk menyempurnakan protokol secara iteratif seiring penggunaan dunia nyata mengungkap perbaikan potensial.

Seiring komunitas memperoleh kepercayaan pada sistem dari waktu ke waktu, kekuatan untuk mengubah runtime akan dikurangi

secara signifikan untuk membatasi permukaan serangan, jika aktor jahat memperoleh kendali atas proses peningkatan.

sistem tata kelola

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

Proposal dikategorikan ke beberapa trek voting yang disebut “origins”. Setiap origin memiliki parameter yang disesuaikan seperti ambang persetujuan (mis. supermayoritas untuk perubahan berdampak tinggi), deposit minimum untuk mencegah spam, periode persiapan/pelaksanaan, dan timeline keputusan untuk mencegah kebuntuan. Desain multi-trek ini memungkinkan pemrosesan paralel referendum beragam, dari pengeluaran treasury rutin hingga peningkatan runtime kritis.

Technical Collective adalah kelompok kurasi ahli teknis yang bertindak sebagai badan khusus untuk mengusulkan, meninjau, atau mendaftar urusan teknis mendesak, mempercepatnya melalui trek khusus sambil mempertahankan pengawasan komunitas.

Quantus mengadopsi sistem ini tanpa modifikasi tetapi memulai dengan setup minimalis untuk menghindari kompleksitas di tahap awal. Awalnya, hanya trek Technical Collective yang aktif, yang akan digunakan untuk keputusan mengikat berprivilegi tinggi seperti peningkatan protokol atau penyesuaian parameter.

Nanti, Quantus dapat menambahkan trek suara komunitas non-mengikat untuk mengukur sentimen pada topik tidak dapat ditegakkan, seperti saran fitur atau polling ekosistem. Sistem ini menjadi mengikat ketika perusahaan menyerahkan jaringan ke DAO. Pendekatan bertahap ini memungkinkan jaringan berkembang secara organik melalui suara tata kelola mendatang tanpa membebani pengguna dengan kompleksitas yang tidak perlu di awal.

07

peta jalan

Peta jalan saat ini hingga 2026, dapat berubah.

heisenberg inception Desember 2024	Pendanaan terjamin, Substrate dipilih.
resonance alpha Juli 2025	Testnet publik, tanda tangan Dilithium, transaksi reversibel.
schrödinger beta Oktober 2025	Fitur lengkap, siap audit.
dirac beta November 2025	PoW diganti Poseidon2, audit ditindaklanjuti.
planck beta Januari 2026	Akun keamanan tinggi, multisig, dompet perangkat keras, integrasi ZK.
bell mainnet Kuartal 2 2026	Peluncuran mainnet.
fermi upgrade Kuartal 4 2026	Infrastruktur agregasi bukti ZK.

08

risiko

Membangun Quantus Network disertai risiko inheren.

masalah implementasi

Kekacauan logika perangkat lunak dapat menyebabkan kegagalan serius bahkan pada sistem yang paling baik dirancang.

masalah pemilihan algoritma nist

Kekacauan atau pintu belakang potensial dalam standar pasca-kuantum terpilih (mis. ML-DSA, ML-KEM) yang dapat muncul pasca-standardisasi. Dalam kasus terburuk, kekacauan tersebut memungkinkan penyerang memalsukan tanda tangan dengan menurunkan kunci privat dari publik, mewakili mode kegagalan katastrofik chain. Jika kekacauan tersebut diumumkan, Quantus Network dapat ditingkatkan ke algoritma baru, tetapi jika dieksploitasi jarang mungkin tidak pernah terdeteksi.

timeline komputasi kuantum

Terobosan kuantum mungkin datang jauh lebih lambat dari perkiraan, menunda kebutuhan PQC; sebaliknya, pengembangan rahasia (mis. oleh pemerintah) dapat menyebabkan ancaman mendadak jika komunitas blockchain gagal memperbarui dengan cepat.

pertimbangan lain

Hambatan adopsi umum, ketidakpastian regulasi dalam keuangan/blockchain, dan volatilitas inheren ekosistem kripto.

09

referensi & bacaan lanjutan

[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