quantus

量子セキュアで暗号化されたマネー

公開
2026年3月21日

バージョン
0.3.3

区分
public

本ホワイトペーパーは情報提供のみを目的としており、いかなる有価証券、投資、または金融商品の売却の申し出、買付けの申し出の勧誘、または推奨を構成するものではありません。読者は投資判断を行う前に独自のデューデリジェンスを行い、資格を有する専門家に相談してください。Quantus Networkは、ここに含まれる情報の正確性または完全性について表明または保証を行いません。

目次

01

はじめに

量子の脅威

従来のブロックチェーンは、暗号学的に意味のある量子コンピュータ（CRQC）による存亡の脅威に直面しています。ブロックチェーンの暗号基盤は離散対数問題（DLP）の困難さに依存しており、量子アルゴリズム、特にショアのアルゴリズムは、古典コンピュータよりもDLPを指数的に速く解くことができます。この脆弱性により、量子的な攻撃者が公開鍵から秘密鍵を導き出し、取引の偽造や機密性の高い金融データの復号が可能になる恐れがあります。

> 耐量子計算への先回り的なアップデートがなければ、数兆ドル規模の暗号経済は、こうした攻撃による突然の価値毀損のリスクにさらされます。

独自の価値提案

ラテン語で「どれほど」を意味する語にちなんで名付けられたQuantus Networkは、スケーラブルで量子的に安全なプライベートマネーを実現します。Quantusは汎用スマートコントラクト・プラットフォームではありません。少数の料理に徹して磨きをかけるレストランのように、Quantusは次を提供します。

– すべてのトランザクションに対する耐量子署名

– ピア間接続を保護する耐量子署名と暗号化（ML-DSAおよびML-KEM）

– スケーリングのための耐量子ゼロ知識証明

– 盗難を抑止し、ミスからの回復を可能にする高セキュリティアカウント

– アドレス確認を容易にする人間が読めるチェックフレーズ

スケーラブルで量子的に安全なプライベートマネーに焦点を当てる判断は、CRQCが業界にもたらす脅威と、ビットコインがこれらの課題に対処できないことに由来します。

02

ブロックチェーンに対する量子の脅威

量子計算の基礎

量子コンピュータは、重ね合わせやもつれなどの原理を利用して、古典マシンでは扱いにくい計算を行います。0または1である古典ビットとは異なり、量子ビット（qubit）は複数の状態に同時に存在でき、特定の問題に対して指数的な並列性を可能にします。この能力は、ブロックチェーン金融を支える暗号システムに存亡のリスクをもたらします。量子ハード向けに開発されたアルゴリズムが、公開鍵暗号の大半のセキュリティ前提を覆すためです。

ショアのアルゴリズムは、1994年にピーター・ショアによって発表され、量子コンピュータ上で大きな整数の因数分解と離散対数問題を多項式時間で解く手法を示しました。量子フーリエ変換（QFT）を用いて関数の周期を求め、RSAや楕円曲線暗号（ECC）などの方式の基盤となる落とし戸関数を効率的に反転できます。ブロックチェーン金融では、十分に強力な量子コンピュータ（推定約2,000論理量子ビット[6][7][8][9]）を持つ攻撃者が、多項式時間 $O(n^3)$ で公開鍵から秘密鍵を導き出せることを意味します。極めて大きな加速であり、脆弱なシステムを一晩で時代遅れにします。[1]

グローバーのアルゴリズムは、1996年にラヴ・グローバーによって提案され、非構造化探索に対して二次の加速を与え、探索時間を

O(n) から O(√n) 操作に短縮します。非対称暗号に対するショアほど壊滅的ではありませんが、グローバーはハッシュ関数やAES暗号などの対称プリミティブに影響し、実質的にセキュリティレベルを半分にします（例：256ビット鍵が量子攻撃下では128ビット相当に振る舞う）。この攻撃は、暗号方式を変えるのではなくセキュリティビットを倍にすることで緩和されます。また、グローバーの二次加速は量子ビットとゲート要件が高く、並列化が限られた数十億の逐次操作を要するため、将来のハードでも現実世界での逆転には不向きです。[2]

4つの脅威カテゴリ

01 - デジタル署名の偽造

ショアのアルゴリズムは、多くのブロックチェーンで使われるECCベースの署名（例：ビットコインのsecp256k1曲線）を直接脅かし、攻撃者がユーザーになりすまして不正なトランザクションを承認できるようにします。この能力は、ブロックチェーンの最も基本的な機能の致命的な失敗を意味します。

02 - ゼロ知識システムにおける偽証明の偽造

プライバシー重視の金融におけるzk-SNARKなど、多くのゼロ知識証明は、コミットメントに楕円曲線ペアリングを介した離散対数の困難さに依存しています。ショアにより、有効に見える無効な証明が作れ、攻撃者が新規コインを鋳造したりL2の状態を偽装したりできる可能性があります。

03 - 秘密情報の復号

量子攻撃は、ZcashやMoneroなどのプライバシー・プロトコルで脆弱な公開鍵方式で保護された暗号化データを露呈させる可能性があります。金融プロトコルにおけるP2P通信を復号し、機密性の高い資産の詳細を明らかにし、標的を絞った盗難を可能にする恐れもあります。

04 - ハッシュ関数の反転

グローバーのアルゴリズムは、プルーフ・オブ・ワークやアドレス生成に使われるSHA-256などのハッシュに対する原像攻撃を加速しうるが、最も心配の少ない脅威です。多くの耐量子方式は、十分な大きさのダイジェストであればハッシュは十分安全とみなされるハッシュベースの構成を取り入れています。

耐量子暗号におけるスケーリングの課題

耐量子暗号（PQC）は量子脅威に対する不可欠な保護を提供しますが、これらのアルゴリズム固有の設計により、重大なスケーリング上の障壁を生みます。コンパクトな数学構造に依拠する楕円曲線方式とは異なり、PQCプリミティブは古典および量子の両方の攻撃者に対してセキュリティを維持するために、より大きなパラメータを必要とします。その結果、公開鍵、秘密鍵、署名がしばしば桁違いに大きくなります。次の表は、128ビットの耐量子セキュリティレベルにおけるML-DSAの代表的なサイズを、256ビットECDSAなどの古典的対応物と比較したものです。[10]

アルゴリズム	公開鍵	秘密鍵	署名
ML-DSA-87 (Dilithium)	**2,592 bytes**	**4,896 bytes**	**4,627 bytes**
ECDSA (256-bit)	**32 bytes**	**32 bytes**	**65 bytes**

128ビット耐量子セキュリティレベルにおけるサイズ。出典：Open Quantum Safe Project [10]

ご覧のとおり、ML-DSAの署名はECDSA相当より70倍以上、公開鍵は80倍以上大きくなり得ます。他のPQCファミリーはさらに悪化します。SPHINCS+のようなハッシュベース方式は最大41 KBの署名を生み、FALCONのようなサイズ最適化格子バリアントでも古典サイズを大きく上回ります。

ブロックチェーンの文脈では、これらの肥大化したサイズがシステム全体のスケーリング問題に積み上がります。大きな署名は個々のトランザクションを膨らませ、ブロックが早く埋まり検証に時間がかかることで秒間トランザクション数（TPS）を下げます。P2P通信にも負荷がかかり、帯域と伝播遅延が増し、プルーフ・オブ・ワークなどのコンセンサスでフォークや孤立ブロックのリスクを高めうります。ストレージ要件も影響を受け、ノードの運用コストが上がり、特にリソースの限られたユーザーやバリデータの参加障壁となります。

> 注

> こうしたスケーリング課題は、将来すべてのブロックチェーンが対処しなければなりません。例えばビットコインは、最大ブロックサイズを増やさなければ1 TPSを大きく下回ります。

03

移行の危機

調整問題

ビットコインの保守的文化はプロトコル変更に抵抗します。PQCの改善には、移行期限、コインの没収の可能性、ブロックサイズの増加など、論争的な事項についてのコンセンサスが必要です。たとえコミュニティが合意しても、各ユーザーは資金を量子的に安全な新しいアドレスへ移行しなければなりません。移行はすべての暗号資産保有者の行動を要し、その多くはウォレットへのアクセスを失っているか、脅威を認識していません。

これらの問題は公開ブロックチェーン全体にありますが、明確なリーダーシップの欠如と技術的硬直化の哲学により、ビットコインでは特に困難です。

紛失コインの問題

推定2,500億～5,000億ドル相当のビットコインが、紛失した鍵、死亡した保有者、忘れられたウォレットにより恒久的にアクセス不能です。[3] これらのコインは移行できず、暗号学的に意味のある量子コンピュータ（CRQC）を作るための公的報酬として機能します。量子攻撃者は移行されていない公開鍵から秘密鍵を導き出し、数十億ドル相当のBTCを市場に流し込む可能性が高いでしょう。

> 技術的に唯一の解は、移行されないコインを凍結する厳格な期限を設けることだが、 政治的には不可能である。

そのような期限がなければ、移行されないコインは盗まれ売却され、市場を押し下げ、ネットワークへの信頼を損ないます。

移行スケジュールの問題

耐量子署名は現行のビットコイン署名の20～80倍の大きさです。根本的なアーキテクチャ変更なしに、ビットコインの性能はすでに限られた容量のわずかな割合に崩落します。

ビットコインが政治的・技術的課題を解決したとしても、移行自体は数ヶ月から年単位かかります。各保有者は、資金を量子的に安全なアドレスへ動かすために少なくとも1件のトランザクションを送る必要があります。多くはまずテスト送金を行います。肥大したPQC署名が性能を窒息させる中、脆弱なコインがさらさら露呈したまま、ネットワークは数ヶ月から年単位のキューに直面します。

> **QUANTUSの答え**
>
> こうした積み重なった課題により、既存チェーンへの量子セキュリティ追加は極めて困難です。 Quantus Networkは、初日からチェーンに量子セキュリティを組み込むことでこれを回避します。

04

quantus networkのアーキテクチャ

基礎

Quantus Networkは、EthereumとPolkadotの背後にあるParity Technologiesチームが開発したブロックチェーンSDK、Substrateの上に構築されています。Substrateは高度にモジュール式であり、Quantusを独自にする部分に集中するためにコンポーネントを容易に差し替えられます。

QuantusはSubstrateを次のように強化します。

- 耐量子署名方式のサポート追加
- P2Pネットワークのセキュリティを耐量子に更新
- ユーザー制御のトランザクション可逆性の追加
- すべてのデータ型をフィールド要素の境界に揃え、データベースをZK互換にする

耐量子暗号プリミティブ

Quantus Networkは、NISTが標準化したPQCを用いて、トランザクションとネットワーク通信のセキュリティを量子脅威から保護します。トランザクション整合性の中核には**ML-DSA**（モジュール格子ベースのデジタル署名アルゴリズム、旧称CRYSTALS-Dilithium）があり、セキュリティ、効率、実装のしやすさのバランスから格

子ベースの署名方式として選ばれています。ML-DSAは、モジュール格子上のLearning With Errors（LWE）やShort Integer Solution（SIS）などの問題の困難さを利用し、ショアのアルゴリズムを含む古典・量子攻撃に対して頑健な耐性を提供します。[4]

トランザクション署名には、Quantusが**ML-DSA-87**を統合しています。これはNISTの最高セキュリティレベル（レベル5、古典256ビット・量子128ビット相当）のパラメータ集合であり、格子暗号解析の進展に備えた慎重さを優先します。格子暗号は比較的新しく、古典方式ほど実戦で試されていません。より大きなパラメータは格子解析の潜在的進展によるリスクを緩和し、小さな鍵サイズはより弱い標的のまま残ります。

検討した代替案

ML-DSAは、FN-DSA（Falcon）などの代替より選ばれました。Falconは実装が複雑（例：ブロックチェーンに不向きな浮動小数点演算が必要）、仕様に決定論的鍵生成がなく、開発当時は最終化されていませんでした。

SLH-DSAのようなハッシュベース方式は、さらに大きな署名（17 KB超）のため選ばれませんでした。暗号アジリティ（署名方式の切り替え能力）はSubstrateに組み込まれており、将来状況が変わればこれらの代替を比較的容易に追加できます。

ML-DSA-87は鍵と署名が大きいものの、初期段階のQuantusネットワークではストレージがまだボトルネックではなく管理可能であ

り、ワームホールアドレスによるゼロ知識証明などの最適化がスケーリングに対処します。

実装の技術詳細は QIP-0006 を参照してください。

libp2p - 量子的に安全なネットワーク

Quantus Networkは、ピアツーピア（P2P）ノード間通信を、認証に**ML-DSA**、鍵のカプセル化に**ML-KEM**（モジュール格子ベース鍵カプセル化メカニズム、旧CRYSTALS-Kyber）を組み合わせて保護します。この統合はPQCをlibp2pスタックまで拡張し、量子耐性のため中核コンポーネントを変更します。ML-DSA-87によるピア識別と、共有秘密の量子耐性のためNoiseハンドシェイクをKEMメッセージで拡張したML-KEM-768によるトランスポートセキュリティです。[5]

P2P層は量子セキュリティ分析で見落とされがちです。ピア認証は重要ですが、ピア層で攻撃者が最悪行えるのはノードになりすまして無効なメッセージを送ることであり、これはサービス拒否にすぎません。この攻撃は、ブロックチェーンではノードは通常信頼されず、攻撃が検知されれば鍵を容易に変更できるため、すでに緩和されています。同様に、P2P通信の復号は攻撃者への利益が限定的（例：トランザクション経路の追跡はプロキシやTorで緩和）で、多くのデータは最終的にチェーン上で公開されます。

それでも、P2P層を量子的に保護することは、盗聴、中間者攻撃、量子による復号から守り、ノードのゴシップ、ブロック伝播、そ

の他のネットワーク相互作用が予見可能な将来にわたって機密性と整合性を保つことを意味します。

技術詳細は QIP-0004 を参照してください。

pqcスケーリング - ワームホールアドレス

耐量子暗号に内在するスケーリング課題に対処するため、Quantus Networkは**「ワームホールアドレス」**と呼ばれる、革新的な集約耐量子署名方式を導入します。このシステムは、Plonky2証明システム（基本的にSTARK）で生成されたゼロ知識証明（ZKP）を利用し、残高検証をオフチェーンに移し、チェーンは個々の署名を処理せず単一のコンパクトな証明だけを検証できます。ワームホールアドレスは、1本の証明で多数のトランザクションを検証でき、公開入力（例：ヌリファイア、ストレージルート、出力アドレス、金額）が主な制約要因です。これにより、トランザクションあたり償却されるストレージ需要は約256バイトの追加に抑えられ、既知のいかなるPQC署名方式よりもはるかに小さくなります。

方式の量子セキュリティは、従来のSNARKで量子に弱い楕円曲線ペアリングの代わりに、FRI（Fast Reed-Solomon Interactive Oracle Proofs）によるコミットメントに**Poseidon2**という安全なハッシュ関数を用いることに由来します。

さらに、認証秘密はPoseidon2の背後に隠されます。安全なハッシュ関数はグローバーのアルゴリズムでせいぜい二次的に弱まるだけであり、破られません。ハッシュ原像証明はZK文脈で

SPHINCS+のようなハッシュベース方式に似た、軽量の耐量子署名として機能し得ます。

クライアント／証明者フロー

ユーザーは、ソルトと秘密を連結したものを二重ハッシュし、支出不能であることが証明可能なアドレスを生成します。

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

この構成は、単純ハッシュ公開鍵と二重使用不能アドレスを混同するような偽陽性を防ぎます。Substrate（および一般的にブロックチェーン）では、アドレスは安全なハッシュではなく、秘密鍵から代数演算で導かれた公開鍵の単純ハッシュです。構成のセキュリティは、安全なハッシュの原像の原像を見つけることに帰着します。このアドレスへ送られたトークンは事実上バーンされます。受取アドレスに対応する秘密鍵が存在しないため使用できません。これらのコインは供給を膨らませずに再鋳造できます。

各送金ごとに、グローバルな一意の送金回数などの詳細を含むTransferProofストレージオブジェクトが作成されます。ユーザーのウォレットは、最近のブロックヘッダのストレージルートからこのTransferProofのリーフまでのMerkle-Patricia-Trie（MPT）ストレージ証明を生成します。二重使用を防ぐためヌリファイアを計算します。

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

アグリゲーターフロー

任意の当事者（クライアント、マイナー、第三者）がPlonky2の再帰により複数の証明を集約し、各親証明が子を検証する証明の木を形成し、子の公開入力を集約します。

- ヌリファイアはそのまま渡る
- 出力アドレスは重複除去される
- ブロックハッシュは連鎖が証明され、最新以外は破棄される
- 重複出力アドレスの金額は合算される

チェーン／検証者フロー

ネットワークは集約証明を検証し、ブロックハッシュがチェーン上で最近であること、ヌリファイアの一意性（二重使用防止）、証明の有効性を確認します。ZK回路はストレージ証明の正しさ、ヌリファイアの正確さ、アドレスの使用不能性、入出力の残高一致、ブロックヘッダの連鎖を課します。

plonky2を選ぶ理由

- すでに監査済み
- 耐量子
- 信頼初期設定不要
- 証明／検証が効率的
- 証明の集約がスムーズ
- Rustでのネイティブ実装

— Substrateのno-std環境と相性が良い

> **性能**
>
> 再帰証明は約170ミリ秒で終了し、サイズはコンパクトです（集約証明あたり100 KB）。5 MBブロックで最適な場合、すべてのトランザクションが同一出力先なら、ワームホールアドレスは1ブロックあたり約153,000件を詰め込めます（4.9 MB／ヌリファイア32バイト）：生のML-DSA約685件（5 MB／7.3 KB）に対して約223倍の改善です。

セキュリティ上の注意

潜在的リスクには、回路／検証実装の不具合によるインフレーション・バグが含まれますが、再鋳造コインがゼロ送金元アドレスの残高を超えるなら経済的に検出可能です。ユーザーは秘密を開示せず最初のハッシュを公開することで、任意にワームホールアドレスであることを証明できます。検証トランザクションは署名されないため、失敗トランザクションによるDoSは金融的手段なしで緩和する必要があります。トークン供給の計算は維持され、再鋳造は新規コインとして現れますが、バーンにより最大供給保証が保たれます。

さらなる技術詳細は QIP-0005 を参照してください。

コンセンサスメカニズム

Quantus Networkは、ビットコインのコンセンサスの望ましい性質を保ちつつ、ZK証明システムとの親和性を高めるためSHA-256を

Poseidon2に置き換えることで、プルーフ・オブ・ワーク（PoW）コンセンサスアルゴリズムを用います。

重要：この変更は量子セキュリティのためではありません。SHA-256のような暗号ハッシュ関数は、特にグローバーのアルゴリズムにより弱まりますが破壊されません。一部の耐量子署名方式はこの理由で安全なハッシュを基本ブロックとして使います。

Poseidon2はPoseidonハッシュ関数の改良版です。SHA-256のような従来ハッシュでの計算用にSNARKやSTARKを作ると、Poseidonを使う場合の約100倍のゲートが必要になることが多く、Poseidonはビット演算ではなくフィールド要素上の代数関数のみに依拠します。

Poseidon2とPlonky2には**ゴールドィロックス体**を用います。ゴールドィロックス体の位数は64ビット符号なし整数に収まり、堅牢性を損なわず効率を高めます。

05

資産の保全

暗号資産の鍵管理には多くのリスクがありますが、ほとんどは避けられます。

可逆トランザクション

Quantus Networkは、ユーザーが設定できる可逆トランザクションを提供します。送信者は、送金をキャンセルできる時間窓を設定します。これにより盗難を抑止し、ファイナリティを犠牲にせずミスを修正できます。システムはタイムスタンプ付きの修正されたSubstrate「scheduler」パレットを用います。ウォレットは送信者（キャンセルボタン付き）と受取人にカウントダウンを表示します。

可逆トランザクションは、オンチェーン適用によって分散性を保ちながら、新しいセキュリティ・プロトコルを可能にします。

技術詳細は QIP-0009 を参照してください。

チェックフレーズ

Quantus Networkは「check-phrases」を導入します。これはブロックチェーンアドレスに対する、人間が読め暗号的に安全なチェックサムです。アドレスをハッシュしてBIP-39の単語リストから短い覚えやすい語列を生成します。チェックフレーズは誤字、改ざん、住所汚染攻撃から保護します。50,000回反復の鍵導出関数

によりレインボーテーブル攻撃を高コストにします。大金の送金では、ユーザーは引き続きアドレスを文字単位で確認すべきです。

技術詳細は QIP-0008 を参照してください。

高セキュリティアカウント

任意のアカウントを、すべての送金に必須の可逆期間を伴う「高セキュリティアカウント」に格上げできます。指定した**ガーディアン**（ハードウェアウォレット、マルチシグ、または信頼できる第三者）が可逆期間中に疑わしいトランザクションをキャンセルし、資金を送信者または受取人ではなくガーディアンへ送れます。このオプトイン機能は一度有効化すると恒久的で、盗賊が無効化できません。

ガーディアンは連鎖できます。高セキュリティアカウントのガーディアン自体を、独自のガーディアンを持つ高セキュリティアカウントにできます。これにより、保護するアカウントに対して上位の権限を持つ合成可能な階層が生まれます。正当な送金のファイナリティを損なわず、ユーザーが不正活動に気づき対応する時間を確保する設計です。

技術詳細は QIP-0011 を参照してください。

鍵の回収

多くの暗号資産の富は、所有者とともに墓場へ運ばれました。Quantus Networkは、固定遅延のもとでいつでも資金を引き出せる

回復用アドレスを簡単に指定する方法を提供します。その間、所有者が鍵にアクセスできれば回復を拒否できます。この機能は存続を可能にします。裁判所や正式な遺言なしにオンチェーンの遺言を持てます。

hd-lattice

階層的決定論的（HD）ウォレットは業界標準であり、すべての鍵を1つのシードフレーズでバックアップでき、手動コピーよりセキュリティと利便性が向上します。Dilithiumのような格子方式に適合させると2つの課題があります。

– HMAC-SHA512の出力は、特定の性質を持つ環からサンプリングされた多項式である格子秘密鍵を直接形成できない。

– 非ハード化鍵導出は楕円曲線上の加算に依拠するが、格子には存在しない（公開鍵はどの代数演算でも閉じない）。

Quantus Networkは前者を、HMAC出力を鍵そのものではなく、秘密鍵を決定論的に構築するエントロピーとして用いることで対処します。後者は格子暗号がそれを解決するよう適合できれば未解決の研究課題にすぎず、緊急度は低いです。

技術詳細は QIP-0002 を参照してください。

06

トークノミクスとガバナンス

Quantus Networkは変化する環境にあり、初手で正解だと仮定することはできません。そこで単純な出発点を選び、新たな情報に応じてガバナンスが変更できるようにしました。この設計により、ブロックチェーンは環境に適応できる生きた実体になります。特にSubstrateのガバナンスプロセスは、各種ノード運用者間の調整を最小限に、チェーンへの深い変更を可能にします。

ブロック報酬

Quantus Networkは、ビットコインを模した単純なトークノミクスモデルを採用します。最大供給は**2,100万枚**で、単純なヒューリスティックがブロック報酬を決めます。

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

このヒューリスティックは、block_rewardがcurrent_supplyに寄与するにつれ滑らかに指数関数的に減少する曲線を形成し、次ブロックで計算されるblock_rewardを下げます。手数料などによるバーンはcurrent_supplyを減らし、ブロック報酬の予算の一部になります。定数は、バーンが全くない場合に約30年でコインの99%が発行されるよう選ばれています。

投資家への割当

Quantus Networkは、資金提供で大きなリスクを負った投資家の支援により構築されました。プライベート投資家はチームと同様に4年のベスティングに服します。公募投資家は初日から完全に流動性があります。公募で調達した資金はトークンとペアリングされ、流動性（DEX、CEX、マーケットメイカー）に使われます。これらの投資家割当と流動性が唯一の「プレマイン」です。残りのトークンは存在するまでマイニングで発行されます。

公募で最大10%未満しか売れなかった場合、流動性トークンは比例して削減され、残りはブロック報酬としてマイナーに発行されます。

会社への割当

新技術を成功の保証なく構築するリスクを負ったチームへの補償として、約4年間、ブロック報酬の一部が会社に送られます。これは会社への**総供給の約15%**に相当する事実上のベスティングです。

その時点以降、ブロック報酬における会社のシェアは、トークン保有者の投票によりオフ、調整、または再配向できます。

トランザクション手数料

トランザクション種別	手数料構造	行き先
標準	固定手数料	マイナー
可逆（高セキュリティ）	取引高の1%	バーン
ZK集約	取引高の0.1%	マイナー50%／バーン50%

フォークレスアップグレード

Quantus Networkは、Substrateのランタイムアップグレードにより「フォークレス」アップグレードをサポートし、ブロックチェーンの中核ロジック（「ランタイム」）を、ネットワークを混乱させたりコミュニティを分断するハードフォークなしに進化させられます。オンチェーンガバナンスの公投で実現し、承認された提案がランタイムの入れ替えを発動します。既存のWASMコードblobを新しいものに実質1ブロックで置き換え、状態と運用の連続性を保ちます。この経路はダウンタイムとリスクを最小化し、実利用から改善が見えてくるにつれコミュニティが反復的にプロトコルを洗練できるようにします。

コミュニティがシステムへの信頼を深めるにつれ、悪意ある主体がアップグレード過程を掌握した場合の攻撃面を抑えるため、ランタイム変更の権限は大幅に縮小されます。

ガバナンス体制

Quantus Networkのガバナンス枠組みは、Substrate経由でPolkadotのOpenGovを継承します。トークン保有者は**信念投票**に参加し、資産を可変期間ロックして票の重みを増幅します。増幅は1倍（ロックなし）から最大6倍（最大ロック）までです。この設計は、コミットメントに影響力を結びつけることで長期の利害一致を促します。

提案は**オリジン**と呼ばれる複数の投票トラックに分類されます。各オリジンは、高影響変更の超過半数などの承認閾値、スパム対策の最低預金、準備／実行期間、膠着回避の決定期限など、カスタムパラメータを持ちます。このマルチトラック設計により、日常のトレジャリー支出から重要なランタイム更新まで、多様な公投を並行処理できます。

Technical Collectiveは、技術専門家のキュレートされたグループで、緊急の技術案件を提案・レビュー・ホワイトリストし、コミュニティ監督を維持しつつ専用トラックで迅速化する専門機関として機能します。

Quantusはこのシステムを改変せず採用しますが、初期段階の複雑さを避けるためミニマルな設定から始めます。当初はTechnical Collectiveのトラックのみが有効で、プロトコル更新やパラメータ調整などの高権限の拘束力ある決定に用いられます。

のちにQuantusは、機能提案やエコシステム調査など執行力のない事項についてコミュニティ向けの非拘束投票トラックを追加でき

ます。会社がネットワークをDAOに引き渡したとき、この仕組みは拘束力を持ちます。この段階的アプローチにより、ネットワークは将来のガバナンス投票で有機的に進化でき、初期からユーザーに不要な複雑さを負わせません。

07

ロードマップ

2026年までの現行ロードマップ（変更の可能性あり）。

heisenberg inception 2024年12月	資金調達完了、Substrate採用。
resonance alpha 2025年7月	パブリックテストネット、Dilithium署名、可逆トランザクション。
schrödinger beta 2025年10月	機能フル、監査準備完了。
dirac beta 2025年11月	PoWをPoseidon2に変更、監査対応。
planck beta 2026年1月	高セキュリティアカウント、マルチシグ、ハードウェアウォレット、ZK統合。
bell mainnet 2026年Q2	メインネット公開。
fermi upgrade 2026年Q4	ZK証明集約インフラ。

08

リスク

Quantus Networkの構築には固有のリスクが伴います。

実装上の問題

設計の優れたシステムでも、ソフトウェアロジックの欠陥は重大な障害を引き起こし得ます。

nistアルゴリズム選定上の問題

標準化後に、選ばれた耐量子標準（例：ML-DSA、ML-KEM）に欠陥やバックドアが現れる可能性。最悪の場合、そのような欠陥は公開鍵から秘密鍵を導き署名を偽造できる攻撃者を可能にし、チェーンに壊滅的な故障モードをもたらします。欠陥が公表されればQuantus Networkは新アルゴリズムへ更新できますが、希少な悪用では発見されないかもしれません。

量子計算のタイムライン

量子の進展は予想よりずっと遅れ、PQCの必要性を先延ばしにする可能性があります。逆に、政府による秘密開発などが、ブロックチェーンコミュニティが迅速に更新しなければ突然の脅威となる可能性があります。

その他の考慮

一般的な採用障壁、金融／ブロックチェーンにおける規制の不確実性、暗号エコシステムに内在するボラティリティ。

09

参考文献と関連資料

[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