Quantus Network Whitepaper

著者: Christopher Smith | **最終更新:** 2026年1月14日

はじめに

量子の脅威

従来のブロックチェーンは、量子コンピュータの登場により存亡の危機に直面しています。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いますが、量子アルゴリズム、特にショアのアルゴリズムは、古典的なコンピュータよりも指数関数的に速くDLPを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すことが可能になり、取引の偽造や機密性の高い財務データの復号が行われる恐れがあります。

その結果、壊滅的なシステム障害が発生する可能性があります。事前の耐量子アップグレードがなければ、数兆ドル規模の暗号経済は、こうした攻撃による突然の減価のリスクにさらされます。

> 💡 **TIP**
>
> **Quantusがこれを解決します。**

独自の価値提案

ラテン語で「どれほど」を意味する言葉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資産保全を提供します。Quantusは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。その代わりに、メニューのない高級レストランのように、Quantusは少数のことを他のどのchainよりも優れたレベルで行うことに重点を置いています。

具体的には、Quantusは以下を採用しています：

- すべてのトランザクションに対する耐量子signature
- ピア接続を保護するための耐量子signatureと暗号化（ML-DSAおよびML-KEM）
- 他のブロックチェーンへの耐量子Bridgeと、量子的に安全なラップドコインの作成
- スケーリングのための耐量子zero-knowledge-proofs
- 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判別可能なチェックフレーズ（check-phrases）

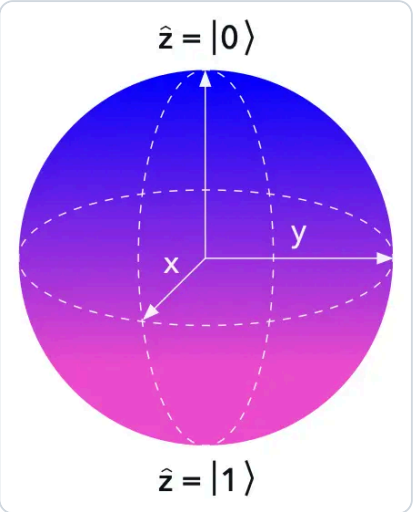
この焦点を絞ったアプローチにより、ユーザーは自信を持って資産を保全し、量子の脅威を機会に変えることができます。

> 💡 **TIP**
> Quantusは、あなたの資産を守るための未来を見据えた要塞です。

ブロックチェーンに対する量子の脅威

量子コンピュータの基礎

量子コンピュータは、重ね合わせや量子もつれ（エンタングルメント）といった原理を利用して、古典的なマシンでは不可能な計算を実行します。



0か1のいずれかである古典的なビットとは異なり、量子ビット（qubit）は複数の状態に同時に存在することができ、特定の問題に対して指数関数的な並列処理を可能にします。**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危機をもたらします。量子ハードウェア向けに開発されたアルゴリズムが、ほとんどの公開鍵暗号のセキュリティ前提を根底から覆すためです。**

ショアのアルゴリズム（Shor's Algorithm）

1994年にピーター・ショアによって発表されたこのアルゴリズムは、量子コンピュータ上で大きな整数の因数分解や離散対数問題を多項式時間で解く方法を提供します。本質的には、量子フーリエ変換（QFT）を利用して関数の周期を見つけ、RSAや楕円曲線暗号（ECC）などの方式の基礎となる落とし戸関数（トラップドア関数）を効率的に逆転させます。

ブロックチェーン金融にとって、これは十分に強力な量子コンピュータ（推定約2,300論理量子ビット）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。これは劇的な高速化であり、脆弱なシステムを一晩で時代遅れにしてしまいます。

グローバーのアルゴリズム（Grover's Algorithm）

1996年にラヴ・グローバーによって提案されたこのアルゴリズムは、非構造化探索問題に対して二次的な高速化を提供し、未ソートのデータベースから特定の項目を見つける時間を $O(n)$ から $O(\sqrt{n})$ の操作に短縮します。これは、量子干渉を通じてターゲット状態の振幅を反復的に増幅することで機能します。非対称暗号に対するショアのアルゴリズムほど壊滅的ではありませんが、**グローバーのアルゴリズムはハッシュ関数やAES暗号などの対称プリミティブに影響を与え、実質的にセキュリティレベルを半分にします**（例：256ビットの鍵が量子攻撃に対して128ビットのように振る舞う）。

影響はありますが、この攻撃は暗号方式を変更するのではなく、単にセキュリティビットを2倍にすることで軽減できます。さらに、グローバーの二次的な高速化は、高い量子ビット数とゲ

ート要件、並列化の制限を伴う数十億の逐次操作を必要とするため、将来のハードウェアであっても現実世界での逆転は非現実的です。

量子コンピュータがブロックチェーン金融にもたらす危険性は、以下の4つの領域に分類されます：

デジタルsignatureの偽造

ショアのアルゴリズムは、ほとんどのブロックチェーンで使用されているECCベースのsignature（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することを可能にします。このような能力は、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。

Zero-Knowledgeシステムにおける虚偽の証明の偽造

プライバシー重視の金融におけるzk-SNARKsなどの多くのzero-knowledge proofは、コミットメントのため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。ショアのアルゴリズムは、有効に見える無効な証明の作成を可能にし、攻撃者が新しいコインを鋳造したり、レイヤー2（L2）の状態を偽装したりすることを可能にする恐れがあります。

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において脆弱な公開鍵方式で保護された暗号化データを公開する可能性があります。また、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。

ハッシュ関数の逆転

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用されるSHA-256などのハッシュに対する原像攻撃（プリイメージ攻撃）を加速させる可能性がありますが、これは最も懸念の少ない脅威です。多くの耐量子暗号方式は、ハッシュが十分な長さのダイジェストであれば十分に安全であると考えられているため、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）は量子の脅威に対して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の障壁をもたらします。コンパクトな数学的構造に依存する楕円曲線方式とは異なり、PQCプリミティブは、古典的および量子的攻撃の両方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、およびsignatureが、多くの場合数桁分大幅に大きくなります。

以下の表は、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などの古典的な対応物と比較したものです：

アルゴリズム	公開鍵サイズ (バイト)	秘密鍵サイズ (バイト)	signatureサイズ (バイト)
ML-DSA-87 (Dilithium)	2,592	4,896	4,627
ECDSA (256ビット)	32	32	65

示されているように、ML-DSAのsignatureはECDSAの対応物の70倍以上、公開鍵は80倍以上大きくなる可能性があります。

他のPQCファミリーはこれをさらに悪化させます。SPHINCS+のようなハッシュベースの方式は最大41 KBのsignatureを生成する場合があり、FALCONのようなサイズ最適化された格子ベースのバリアントであっても、古典的なサイズを大幅に上回ります。

ブロックチェーンの文脈では、これらの膨張したサイズはシステム全体のスケーリング問題へとつながります。signatureが大きくなると個々のトランザクションが肥大化し、ブロックがすぐに埋まり検証に時間がかかるようになるため、秒間トランザクション数（TPS）が減少します。また、P2P通信にも負荷がかかり、帯域幅の需要と伝播遅延が増大します。これにより、プルーフ・オブ・ワークのようなコンセンサスメカニズムにおいて、ネットワークのフォークや孤立ブロック（orphan blocks）のリスクが高まる可能性があります。ストレージ要件も影響を受け、ノードの運用コストが上昇し、特にリソースの限られたユーザーやバリデーターにとっての参加障壁となります。

これらのスケーリングの課題は、将来的にすべてのブロックチェーンが対処しなければならない問題です。例えばビットコインは、最大ブロックサイズを増やさない限り、1 TPSを大幅に下回ることになります。

Quantus Networkのアーキテクチャ

耐量子暗号プリミティブ

Quantus Networkは、量子的な脅威に対し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確保するために、**NIST標準のPQC**プリミティブを採用しています。トランザクションの完全性の核となるのは、**ML-DSA（Module-Lattice-based Digital Signature Algorithm**、旧称CRYSTALS-Dilithium）です。これは、セキュリティ、効率性、および実装の容易さのバランスから選ばれた格子ベースのsignature方式です。**ML-DSAは、モジュール格子上のLearning With Errors (LWE) や Short Integer Solution (SIS) といった問題の困難さを利用しており**、ショアのアルゴリズムによる攻撃を含む、古典的および量子的攻撃の両方に対して強固な耐性を提供します。

トランザクションsignatureのために、**QuantusはML-DSA-87を統合しています**。これは、**格子問題における潜在的な暗号解読の進展から保護するために**、最高レベルのセキュリティ（NISTセキュリティレベル5、古典的な256ビットおよび量子的な128ビットのセキュリティに相当）を提供するパラメータセットです。格子暗号は古典的な方式に比べて比較的新しく、十分に検証されていないため、この選択は慎重さを優先しています。大きなパラメータは、格子暗号解読の潜在的な進歩によるリスクを軽減し、より小さな鍵サイズが容易な標的となる中で安全性を保ちます。

代替案

ML-DSAがFN-DSA（Falcon）などの代替案よりも選ばれた理由は以下の通りです：

- FN-DSAの実装の複雑さ（例：ブロックチェーンに適さない浮動小数点演算が必要）
- 仕様における決定論的な鍵生成の欠如
- 開発時点での未確定なステータス

SLH-DSAのようなハッシュベースのオプションは、signatureサイズがさらに大きい（17 KBを超える）ため却下されました。Substrateには暗号アジリティ（異なるsignature方式を入れ替えられる能力）が組み込まれているため、将来的に必要が生じた場合、これらの代替案を追加することは比較的容易です。

ML-DSA-87は鍵とsignatureが大きくなりますが、これらはストレージがまだボトルネックになっていないQuantusの初期段階のネットワークでは管理可能です。また、zero-knowledge proofを介したワームホールアドレス（wormhole addresses）のような将来の最適化によってスケーリングに対処します。

実装に関する技術的な詳細は、QIP-0006を参照してください。

LibP2P

Quantus Networkは、認証にML-DSA、暗号化にML-KEM（Module-Lattice-based Key Encapsulation Mechanism、旧称CRYSTALS-Kyber）を組み合わせて、ピアツーピア（P2P）ノード通信を保護します。

この統合により、PQCがlibp2pネットワーキングスタックに拡張され、耐量子性のためにコアコンポーネントが修正されています。具体的には、ピアIDにML-DSA-87 signatureを使用し、トランスポートセキュリティにML-KEM-768を使用しています（Noiseハンドシェイクを拡張し、耐量子共有秘密のための追加のKEMメッセージを追加）。

P2Pレイヤーは、量子セキュリティ分析においてしばしば軽視されます。ピアの認証は重要ですが、ピアレベルで攻撃者ができる最悪のことは、ノードになりすまして無効なメッセージを送信することであり、その結果はサービス拒否（DoS）にとどまります。この攻撃は、ブロックチェーンモデルにおいてノードが一般的に信頼されていないことや、攻撃が検出された場合にノードが容易に鍵を切り替えられるという事実によって、すでに軽減されています。同様に、P2P通信を復号しても攻撃者の利益は限られており（例：トランザクション経路の追跡。これはプロキシやTorで軽減可能）、ほとんどのデータはいずれにせよオンチェーンで公開されます。

それにもかかわらず、P2Pレイヤーを量子的に保護することは、盗聴、中間者攻撃、および量子復号から保護し、ノードのゴシップ、ブロックの伝播、および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かつ改ざん防止された状態を維持することを保証します。

実装に関する技術的な詳細は、QIP-0004を参照してください。

PQCのスケーリング

耐量子暗号に固有のスケーリングの課題に対処するため、**Quantus Networkは「ワームホールアドレス（Wormhole Addresses）」と呼ばれる革新的な集約型耐量子signature方式を導入しています。** このシステムは、Plonky2証明システム（基本的にはSTARKs）を介して生成されたzero-knowledge proofs（ZKPs）を利用して、残高検証をオフチェーンに移動させます。これにより、chainは個々のsignatureを処理することなく、単一のコンパクトな証明を検証できるようになります。

ワームホールアドレスは、1つの証明で大量のトランザクションの検証を可能にします。 公開入力（ヌルファイア、ストレージルート、出口アドレス、金額など）が主な制限要因となります。これにより、1トランザクションあたりの償却ストレージ需要は**約256バイト追加される程度に抑えられ、既知のどのPQC signature方式よりもはるかに小さくなります。**

この方式の量子セキュリティは、SNARKsで一般的に使用される量子的に脆弱な楕円曲線ペアリングの代わりに、FRI（Fast Reed-Solomon Interactive Oracle Proofs）を介したコミットメン

トに安全なハッシュ関数Poseidon2を使用することに由来しています。

さらに、認証の秘密はPoseidon2の背後に隠されています。安全なハッシュ関数はグローバーのアルゴリズムによって二次的に弱体化されるだけで、破壊されるわけではないため、ハッシュ原像証明は、SPHINCS+のようなハッシュベースの方式と同様に、ZKコンテキストにおける軽量な耐量子signatureとして機能します。

クライアント / 証明者（Prover）のフロー

ユーザーは、ソルト（salt）と秘密（secret）を連結したものを二重ハッシュ化することで、証明可能な使用不可能アドレスを生成します：

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

この構成は、偽陽性（例：単一ハッシュの公開鍵を使用不可能アドレスと誤認すること）を防ぎます。なぜなら、Substrate（および一般的）において、ブロックチェーンアドレスは公開鍵の単一ハッシュであり、公開鍵は何らかの代数的操作を介して秘密鍵から導出されるものであり、安全なハッシュを介したものではないからです。したがって、この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。このアドレスに送られたトークンは事実上バーン（焼却）されます。受け取ったアドレスに対応する秘密鍵が存在しないため、それらを使用することはできません。そのため、これらのコインは供給量を膨らませることなく再発行（re-mint）することができます。

各送金に対して、ユニークなグローバル送金カウントなどの詳細を含む 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ーのストレージルートからこの TransferProof のリーフ（末端）までの Merkle-Patricia-Trie (MPT) ストレージ証明を生成します。

ヌルファイア（nullifier）が計算されます：

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

これは、秘密が保持のためにウォレットのシードから決定論的に導出されることで、二重支払いを防ぐために行われます。

アグリゲーター（集約者）のフロー

あらゆる当事者（クライアント、マイナー、またはサードパーティ）は、Plonky2の再帰を利用して複数の証明を集約し、各親証明が子証明の検証となる証明のツリーを形成できます。子証明の公開入力は集約されます：

- ヌルファイアは変更されずに渡される
- 出口アドレスは重複排除される
- ブロックハッシュはリンクされていることが証明され、最新のもの以外は破棄される
- 重複する出口アドレスの金額は合算される この再帰は階層的な集約をサポートし、オンチェーンデータを劇的に削減します。

Chain / 検証者（Verifier）のフロー

ネットワークは、以下の項目をチェックすることで集約された証明を検証します：

- ブロックハッシュがオンチェーンにあり、最新であること
- ヌルファイアの一意性（二重支払いを防ぐため）
- 証明の有効性

ZK回路は以下を強制します：

- ストレージ証明の正しさ
- ヌルファイア計算の正確性
- アドレスの使用不可能性
- 入力と出力の残高の一致
- ブロックヘッダーのリンク

Plonky2が選ばれた理由は以下の通りです：

- すでに監査済みである
- 耐量子性がある
- 信頼できるセットアップ（trusted setup）が不要
- 効率的な証明/検証
- シームレスな証明の集約
- Rustネイティブな実装
- Substrateのno-std環境との互換性

パフォーマンスのハイライト：

170ミリ秒での再帰的証明とコンパクトなサイズ（集約証明あたり100 KB）により、圧倒的なスループットの向上が可能になります。

5 MBのブロックで、すべてのトランザクションが同じ出力に向かうという最適なケースでは、**ワームホールアドレスは1つのブロックに約153,000件のトランザクションを詰め込むことができます**（4.9 MB / ヌルファイアあたり32バイト）。これは、生のML-DSAトランザクション（5 MB / 各7.3 KB）の約685件と比較して223倍の改善です。

セキュリティ上の注意

潜在的なリスクには、回路や検証の実装ミスによるインフレバグが含まれますが、再発行されたコインがゼロ送信アドレスの残高を超えれば、経済的に検出可能です。ユーザーは、秘密を明かさずに最初のハッシュを公開することで、アドレスがワームホールであることをオプションで証明できます。検証トランザクションは署名されないため、失敗したトランザクションによるDoSは非財務的な方法で軽減する必要があります。再発行は新しいコインとして現れますが、バーンを通じて最大供給量の保証が維持されるため、トークン供給量の計算は維持されます。

実装に関するさらなる技術的詳細は、QIP-0005を参照してください。

コンセンスメカニズム

Quantus Networkは、ビットコインのコンセンスアルゴリズムの望ましい特性を維持しつつ、SHA-256をPoseidon2に置き換えることでZK証明システムとの互換性を向上させたプルーフ・オブ・ワーク（PoW）コンセンスアルゴリズムを使用しています。

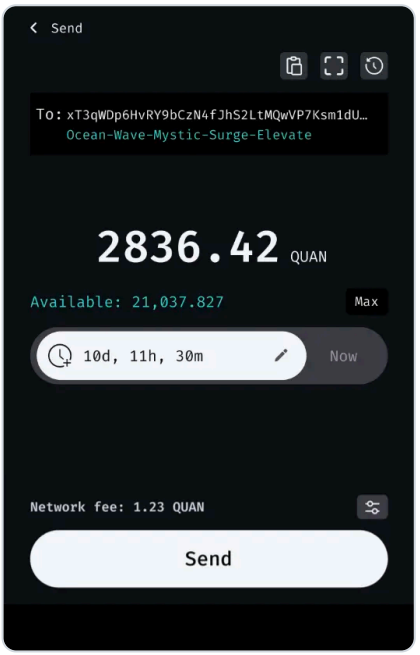
重要な点として、この変更は量子セキュリティのために行われるのではありません。SHA-256のような暗号ハッシュ関数は、量子アルゴリズム（特にグローバーのアルゴリズム）によって弱体化はしますが、破壊はされません。一部の耐量子signature方式が、この理由から安全なハッシュを構成要素として使用しています。

Poseidon2は、Poseidonハッシュ関数の改良版です。SHA-256のような従来のハッシュ関数を含む計算に対してSNARKsやSTARKsを作成する場合、ビットレベルの操作ではなく、フィールド要素上の代数関数のみに依存するPoseidonを使用する場合と比較して、100倍近いゲート数が必要になることがよくあります。効率を最大化するために、Poseidon2とPlonky2の両方でGoldilocksフィールドを使用しています。

資産保全

暗号通貨の鍵管理には多くのリスクがあります。そのほとんどは回避可能です。Quantus Networkは、チェーン自体に使いやすさを組み込み、専門家でなくても安心して取引できるようにしています。

取引の取り消し（Reversible Transactions）

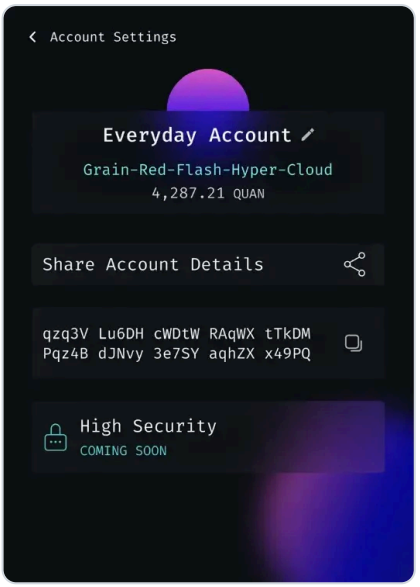


Quantus Networkは、ユーザーが設定可能な取り消し可能トランザクションを提供します。これにより、送信者は出金転送をキャンセルできる時間枠を設定でき、ブロックチェーンの核心である不可逆性を損なうことなく、盗難抑止とエラー修正を強化できます。 直感的な遅延のためにタイムスタンプを使用する、修正されたSubstrateの「scheduler pallet」を利用することで、システムはシンプルなインターフェースを介して転送をスケジュールすることを可能にします。ウォレットには、送信者（キャンセルボタン付き）と受信者（キャンセルされなければ完了することを示す）の両方に対してカウントダウンが表示されます。これにより、商取引のための迅速なファイナリティと、ミスの心配やエスクローサービスなしで誠実な預金を行いたいユーザーのための柔軟性が両立されます。

取り消し可能トランザクションは、オンチェーンでの強制を通じて分散化を維持しつつ、斬新なセキュリティプロトコルのための強力な構成要素を形成します。

技術的な詳細については、QIP-0009を参照してください。

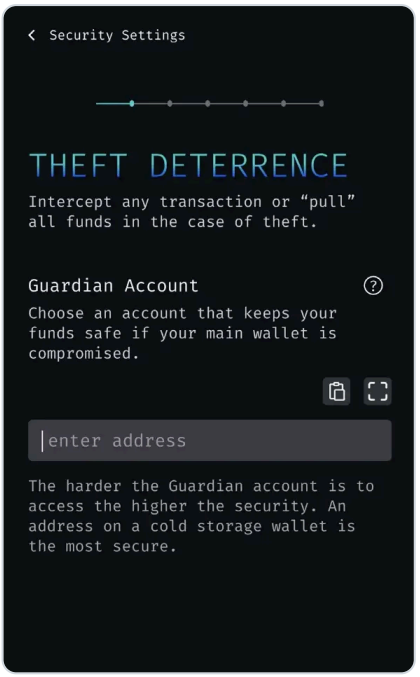
チェックフレーズ（Check-Phrases）



Quantus Networkは、ブロックチェーンアドレスやその他の人間による検証が必要なデータのための、暗号的に安全で人間が判読可能なチェックサムである「チェックフレーズ（check-phrases）」を導入します。 **アドレスをハッシュ化してBIP-39ニーモニックリストから覚えやすい単語の短いシーケンスを生成することで、チェックフレーズは迅速でエラーのない完全性チェックを可能にし、誤入力、改ざん、およびアドレスポイズニング（address poisoning）のような攻撃から保護します。** このツールにより、ユーザーは切り詰められた表示や弱いチェックサムに頼ることなく、送金中に自信を持ってアドレスを確認できます。特定のチェックサムに対するレインボーテーブルの作成を非常に高コストにするために、50,000回の反復を伴う鍵導出関数が使用されています。もちろん、多額の取引の場合、ユーザーは依然としてアドレスのすべての文字を手動で確認して正確さを確かめるべきです。

技術的な詳細については、QIP-0008を参照してください。

高セキュリティアカウント



Quantus Networkは、あらゆるアカウントを「高セキュリティアカウント」にアップグレードする機能を提供します。これは、すべての出金転送に対して強制的な取り消し期間を課し、ハードウェアウォレット、マルチシグ、あるいはユーザーが選んだ信頼できる第三者などの指定された「ガーディアン（guardian）」アカウントが、取り消し期間中に不審な取引を独占的にキャンセルできるようにするものです。キャンセルされた資金は、送信者や受信者ではなくガーディアンに送られます。このオプトイン方式の永続的な機能は、取り消し可能転送に基づいて構築されており、ユーザーは有効化時に遅延とインターセプター（遮断者）を指定し、泥棒がそれを無効にすることを防ぎます。

インターセプター自体が、独自のガーディアンを持つ別の高セキュリティアカウントになることも可能で、各ガーディアンが保護対象のアカウントに対して上位の権限を持つ階層構造を構成できます。この設計は、伝統的な金融における裁判所命令による取り消しを模倣していますが、ユーザーによる制御が可能です。高価値のアカウントに対してセキュリティと利便性のバランスを取り、正当なフローに対するブロックチェーンのファイナリティを損なうことなく、不正な活動を検出して対応するための時間を提供します。

技術的な詳細については、QIP-0011を参照してください。

鍵の復旧

多くの暗号資産が、所有者と共に墓場へと消えていきました。Quantus Networkは、一定の遅延を条件として、いつでも資金を引き出すことができる復旧アドレスを指定するシンプルな方法を提供します。この期間中、所有者は鍵にアクセスできれば復旧を拒否することができます。この機能は生存性の確保を可能にします。ユーザーは裁判所や遺産管理を必要とせずに、オンチェーンの遺言を持つことができます。

HD-Lattice

階層的決定論的（HD）ウォレットはブロックチェーンの業界標準であり、ユーザーがすべての鍵に対して1つのシードフレーズをバックアップすることを可能にし、アクションごとの手動バックアップに比べてセキュリティと利便性を向上させます。

これをDilithiumのような格子方式に適応させるには、2つの課題があります：

- HMAC-SHA512の出力は、格子秘密鍵を直接形成できません。格子秘密鍵には、棄却サンプリング（rejection sampling）による「良好な基底」多項式が必要です。
- 非ハードン化（non-hardened）鍵導出は楕円曲線の加算に依存していますが、格子にはそれが欠けています（公開鍵はいかなる代数的操作の下でも閉じていません）。

Quantus Networkは、HMACの出力を秘密鍵そのものとしてではなく、秘密鍵を決定論的に構築するためのエントロピーとして使用することで、最初の問題に対処します。2番目の問題はそれほど重要ではなく、格子暗号をこれに対処するために適応できるかどうかは未解決の研究課題として残っています。

技術的な詳細については、QIP-0002を参照してください。

トークノミクスとガバナンス

Quantus Networkは変化する環境の中に存在しており、最初の試みですべてが正しく行われるとは限りません。このため、私たちはシンプルな出発点を選択し、新しい情報が得られるにつれてガバナンスシステムが変更を行えるようにしています。この設計により、ブロックチェーンは環境に自在に適応できる生きた実体となります。特に、Substrateのガバナンスプロセスは、さまざまなノードランナー間での最小限の調整で、チェーンに深い変更を加えることを可能にします。

ブロック報酬（Block Rewards）

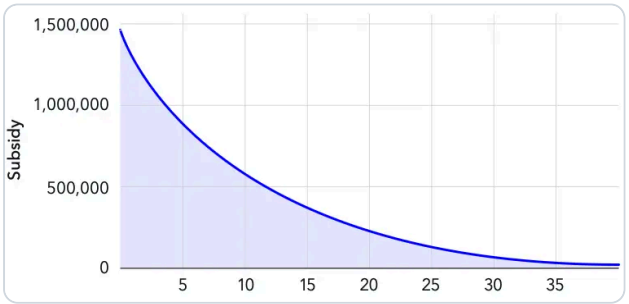
Quantus Networkは、ビットコインを模倣した直接的なトークノミクスモデルを採用しています。最大供給量は21,000,000コインで、シンプルなヒューリスティックによって各ブロックの報酬が決定されます。

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

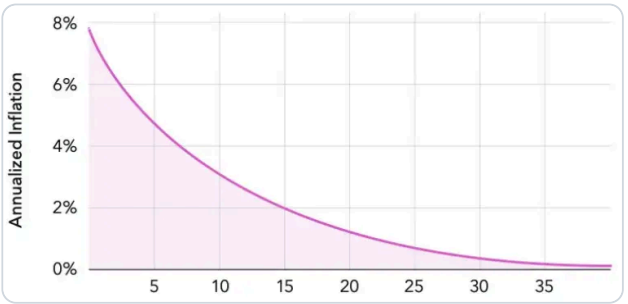
このヒューリスティックは、block_rewardがcurrent_supplyに寄与し、それが次のブロックで計算されるblock_rewardを減少させるため、滑らかな指数関数的減衰曲線を形成します。

手数料などによるバーンはcurrent_supplyを減少させ、実質的にブロック報酬の予算の一部となります。定数は、バーンがない場合に約40年でコインの99%が発行されるように選ばれています。

年間ブロック報酬



年間インフレ率



投資家への配分

Quantus Networkは、資金提供において大きなリスクを負ったエンジェル投資家の助けを借りて構築されました。投資家のロックアップが生み出す供給のオーバーハングを避けるため、公的および私的を問わず、すべての投資家を初日から流動的な状態にします。この配分が唯一の

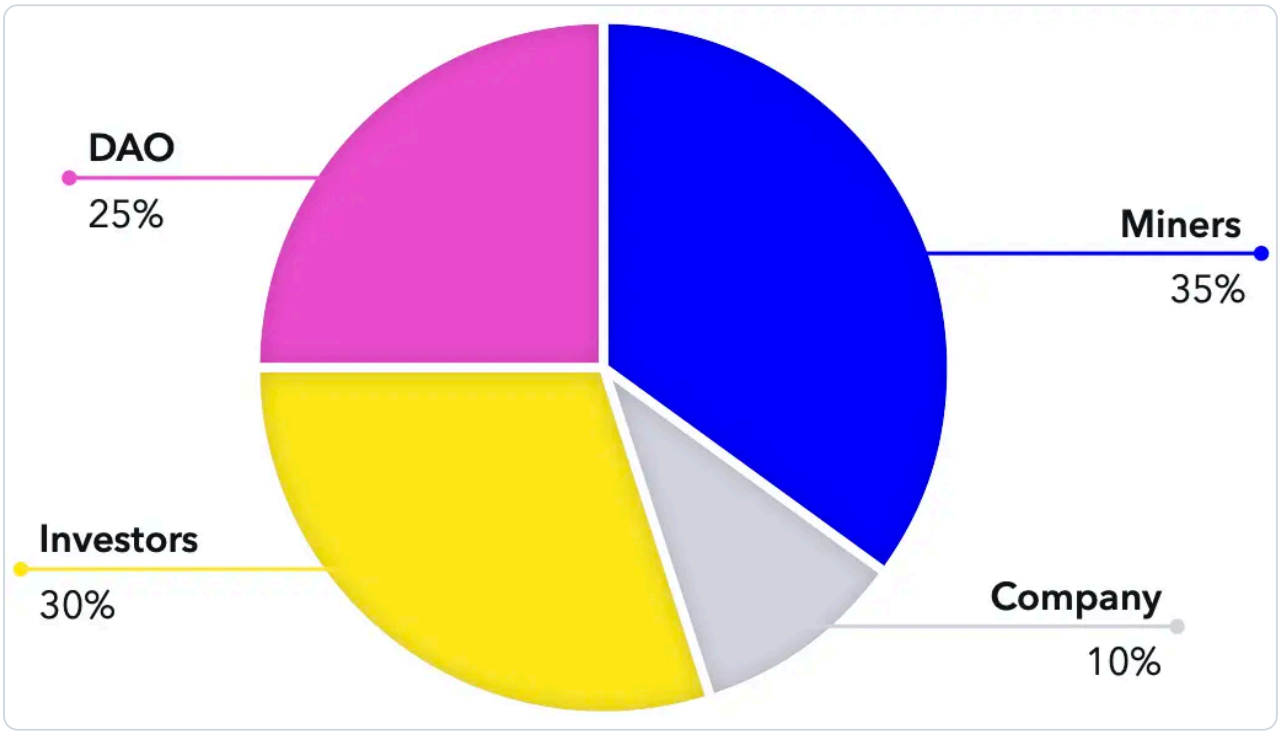
「プレマイン（事前採掘）」となります。他のすべてのトークンは、採掘によって存在させる必要があります。公募の成功度合いによりますが、この部分は総供給量の20〜30%を占めることになります。

会社への配分

成功の保証がない中で新しい技術を構築するというリスクを負ったチームに報いるため、ブロック報酬を2つの半分に分けます。最初の半分はマイナーに送られます。約4年間、残りの半分は会社に送られます。これにより、総供給量の約10%が事実上のベスティングスケジュールとして会社に割り当てられます。この間、マイナーは同量の新しく鋳造されたコインを受け取ります。

その後、会社のブロック報酬分は、トークン保持者によって管理される財務（トレジャリー）に転送され、実質的にDAOを形成します。

推定供給配分



取引手数料

標準的なトランザクションにはマイナーに支払われる手数料があり、トランザクションをブロックに含めるインセンティブを提供します。高セキュリティアカウントからの取り消されたトランザクションには、ボリュームベースで1%の手数料が課され、その半分はマイナーに、もう半分はバーンされ、将来のセキュリティ予算に充てられます。zk集約システムを経由するトランザクションにも、ボリュームベースで0.1%の手数料が課され、マイナー、証明アグリゲーター、およびバーンに分配されます。

フォークレスアップグレード（Forkless Upgrades）

Quantus Networkは、Substrateのランタイムアップグレードを通じて「フォークレス」アップグレードをサポートしています。これにより、ネットワークを混乱させたりコミュニティを分裂させたりするハードフォークなしに、ブロックチェーンのコアロジック（「ランタイム」）を進化させることができます。これはオンチェーンガバナンスの国民投票（レファレンダム）を通じて達成されます。承認された提案はランタイムの入れ替えをトリガーし、既存のWASMコードブロブを単一のブロック内で新しいものに置き換えることで、状態と運用の継続性を確保します。このアップグレードパスはダウンタイムとリスクを最小限に抑え、コミュニティがプロトコルを反復的に洗練させることを可能にします。

ガバナンスシステム

Quantus Networkは、Substrateを介してポルカドット（Polkadot）のOpenGovシステムからガバナンスフレームワークを継承しています。トークン保持者はコンビクション投票（conviction voting）を通じて参加します。これは、資産をさまざまな期間ロックすることに同意することで、投票の重みを増幅させる仕組みです。この増幅は1倍（ロックなし）から6倍（最大ロック）までの範囲で設定可能です。この設計は、影響力をコミットメントに結びつけることで、長期的な整合性を促します。

提案は「オリジン（origins）」と呼ばれる複数の投票トラックに分類されます。各オリジンには、承認のしきい値（例：影響の大きい変更には圧倒的多数が必要）、スパムを抑止するための最小デポジット、準備/施行期間、および停滞を防ぐための決定タイムラインなど、カスタマイズされたパラメータがあります。このマルチトラック設計により、日常的な財務支出から重要なランタイムアップグレードまで、多様な国民投票の並列処理が可能になります。

テクニカルコレクティブ（Technical Collective）は、選ばれた技術専門家のグループであり、緊急の技術的事項を提案、レビュー、またはホワイトリストに登録するための専門機関として機能します。コミュニティの監視を維持しつつ、専用のトラックを通じてそれらを迅速に処理します。

Quantusはこのシステムを変更なしに採用していますが、初期段階での複雑さを避けるために最小限のセットアップから開始します。当初はテクニカルコレクティブのトラックのみがアクティブであり、プロトコルのアップグレードやパラメータの微調整など、拘束力のある高特権の決定に使用されます。

その後、機能の提案やエコシステムのアンケートなど、強制力のないトピックに関する感情を測定するための、拘束力のないコミュニティ投票トラックを導入します。このシステムは、会社がネットワークをDAOに引き渡す際に拘束力を持つようになります。

この段階的なアプローチにより、初期段階で不要な複雑さをユーザーに強いることなく、将来のガバナンス投票を通じてネットワークを有機的に進化させることができます。

ロードマップ

Heisenberg Inception

2024年12月

資金調達完了、Substrate選定

Resonance Alpha

2025年7月

公開テストネット、Dilithium署名、取り消し可能トランザクション

Schrödinger Beta

2025年10月

機能完成、監査準備完了

Dirac Beta

2025年11月

PoWをPoseidon2に変更、監査への対応

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

Bell Mainnet

2026年第1四半期

メインネットローンチ

Fermi Upgrade

2026年第2四半期

ZK集約

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：** ソフトウェアロジックの欠陥は、最高に設計されたシステムであっても深刻な障害を引き起こす可能性があります。
- **NISTアルゴリズム選定の問題：** 選択された耐量子標準（例：ML-DSA、ML-KEM）における潜在的な欠陥やバックドアが、標準化後に出現する可能性があります。最悪の場合、そのような欠陥により、攻撃者が公開鍵から秘密鍵を導き出してsignatureを偽造できるようになり、チェーンの壊滅的な失敗モードを招きます。そのような欠陥が公表された場合、Quantus Networkは新しいアルゴリズムにアップグレードできますが、欠陥が密かに利用された場合、発見されない可能性があります。
- **量子コンピュータのタイムライン：** 量子のブレイクスルーが予想よりも大幅に遅れ、PQCの必要性が先延ばしになる可能性があります。逆に、政府などによる秘密裏の開発により、ブロックチェーンコミュニティが迅速に更新できない場合、突然の脅威につながる可能性があります。
- **その他の考慮事項：** 一般的な普及の障壁、金融/ブロックチェーンにおける規制の不確実性、および暗号エコシステム固有のボラティリティ。

結び

QUANTUS

私たちは、オープンプロトコル、プルーフ・オブ・ワーク、そして主権的な所有権の力を信じています。デスクトップとモバイルで利用可能なQuantus Networkアプリにより、ユーザーはデジタル資産を保存し、新しいブロックを採掘し、仲介者のいないより公正な金融の未来に参加することができます。

私たちは、透明性、プライバシー、そして安全な自己管理型ツールを通じて個人を力づけることに取り組んでいます。