分散台帳技術によって、望まれないハッキングから解放され、デバイス間における
自由と、世界初の耐量子ブロックチェーンを通じた迅速なコミュニケーションを。

Quantarium

White paper v3.0

ホワイトペーパー日本語版



Steve Jung
共同創業者, CEO

Quantarium Coin White Paper

CONTENTS

1 序文 *(Executive Summary)*

2 市場背景および脅威モデル *(Market Context & Threat Model)*

3 Quantarium ソリューションおよび設計哲学 *(Solution & Philosophy)*

4 QUANTA-X: 中核耐量子暗号エンジン

5 Quantarium PQC セキュリティスタック *(Quantarium PQC Security Stack)*

6 Layer 1 アーキテクチャおよび Proof of Authority(PoA)コンセンサス

7 PoA ガバナンスおよびバリデータ運用ポリシー *(Governance & Validator Policy)*

8 耐量子環境におけるスマートコントラクト *(Smart Contracts in PQC Environment)*

9 Quantarium エコシステム概要 *(Ecosystem Overview)*

10 Quantarium アプリケーションエコシステムおよび貢献価値化
(The Quantarum Application Ecosystem & Contribution Valuation)

11 Quantarium デュアルトークン・エコノミー *(Quantarium Dual Token Economy)*

12 結論 *(Conclusion)*

13 参考文献 *(References)*

1. 序文 (Executive Summary)

1.1 プロジェクト概要：ネイティブ耐量子ブロックチェーンの必要性 (Project Overview: The Necessity of Native Quantum-Resistant Blockchain)

デジタル経済の基盤を成す暗号学的信頼（Cryptographic Trust）は、いま重大な転換点に直面しています。過去数十年にわたりインターネットおよびブロックチェーン産業を支えてきた RSA および楕円曲線暗号（ECC/ECDSA）体系は、量子コンピューティング（Quantum Computing）の飛躍的進展によって、その数学的難題である素因数分解および離散対数問題の計算複雑性が崩壊する危機にあります。

誤り訂正が可能な論理キュービット（Logical Qubit）の実質的実装と、ハイブリッド量子アルゴリズムの進展は、「量子優位（Quantum Supremacy）」の到来時期を前倒ししており、これは既存の公開鍵基盤（PKI）に依存するあらゆるブロックチェーンネットワークにとって実存的脅威となっています。とりわけ、現在暗号化されているデータを攻撃者がいま収集・保存し、将来の量子コンピュータで解読する「Harvest Now, Decrypt Later（先に収集し、後で解読する）」攻撃シナリオは、将来の問題ではなく、現在進行形の喫緊のセキュリティ課題です。

現存する大多数のブロックチェーン（Bitcoin、Ethereum など）は、耐量子計算機暗号（Post-Quantum Cryptography, PQC）を前提とせずに設計されています。将来的にソフトフォーク等を通じて PQC 署名へアップグレードするとしても、過去に生成されたジェネシスブロックからアップグレード時点以前までのすべてのトランザクション記録は、依然として脆弱な旧来暗号体系のまま残存します。これを「量子レガシー脆弱性（Quantum Legacy Vulnerability）」と定義し、資産の永続的な所有権保証を本質的価値とするブロックチェーンの根幹を損なうものと位置づけます。

Quantarium は、このような構造的ジレンマを解決するために誕生しました。Quantarium は、既存体系に耐量子機能を後付けする事後的アプローチを採りません。その代わり、ネットワークの起点であるジェネシスブロックの時点から、すべてのトランザクション、署名、検証プロセスに耐量子暗号アルゴリズムを適用した「ネイティブ（Native）耐量子 Layer 1 ブロックチェーン」です。Quantarium は、量子時代においても変わらないデータ完全性と資産安全性を保証する、次世代デジタル信頼インフラの標準を提示します。

1.2 Quantarium の中核価値提案 (Core Value Proposition)

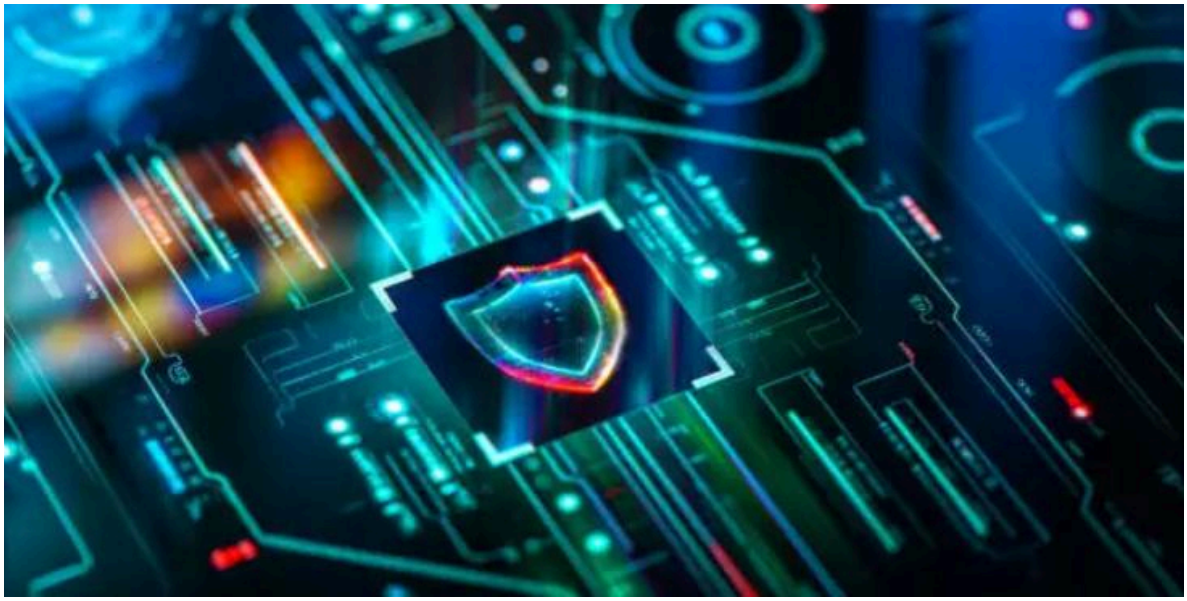
Quantarium は、単なる技術実験ではなく、エンタープライズおよび公共インフラ水準の要求事項を満たす実用的なブロックチェーン・ソリューションです。その中核価値は、以下の四つの軸によって定義されます。

- **NIST 標準に基づく信頼性(Standard Compliance):** Quantarium は、独自仕様または未検証の暗号アルゴリズムを使用しません。当社は、米国国立標準技術研究所(NIST)が耐量子電子署名標準として最終選定した SPHINCS+ 系列アルゴリズムを、コア・セキュリティエンジン(QUANTA-X)として採用しました。SPHINCS+ は、数学的難題に依存しない完全ハッシュベース(Hash-based)署名方式を用いることで、未知の数学的攻撃手法が将来発見された場合でも崩れにくい、最も保守的かつ確実な安全性を提供します。

- **レガシー・フリーの完全性(Legacy-Free Integrity):** 設計段階から PQC を適用した「Native Layer 1」構造は、過去データに対する遡及的ハッキング脅威を根本から遮断します。これは、長期的価値保存が必要な金融資産、不動産トークン化(RWA)、国家記録物管理など、超長期の信頼が要求される領域に対し、実質的に唯一の解答を提示します。

- **エンタープライズ級の性能とコンセンサス(High Performance & Consensus):** セキュリティは性能低下を意味してはなりません。Quantarium は、Proof of Authority(PoA)コンセンサス機構を導入することで、不必要なマイニング競争を排除しました。本人性が検証されたノード(Validator)を通じて、高いスループット(Throughput)と即時的なファイナリティ(Finality)を保証し、リアルタイム決済および大規模トランザクション処理が可能な商用環境を構築しています。

- **統合セキュリティ・エコシステム(Unified Security Ecosystem):** Quantarium は、単なるブロックチェーン・ネットワークを超えた「耐量子セキュリティ・ループ(Quantum-Resilient Security Loop)」を提供します。ユーザーの秘密鍵生成から資産移転(Wallet)、ネットワーク合意(Consensus)、さらにデータ通信(QRCHAT Messenger)に至るまで、全工程に同一の PQC セキュリティスタックを適用することで、システム内の単一障害点(Single Point of Failure)を排除した完結的なセキュリティ環境を実現します。



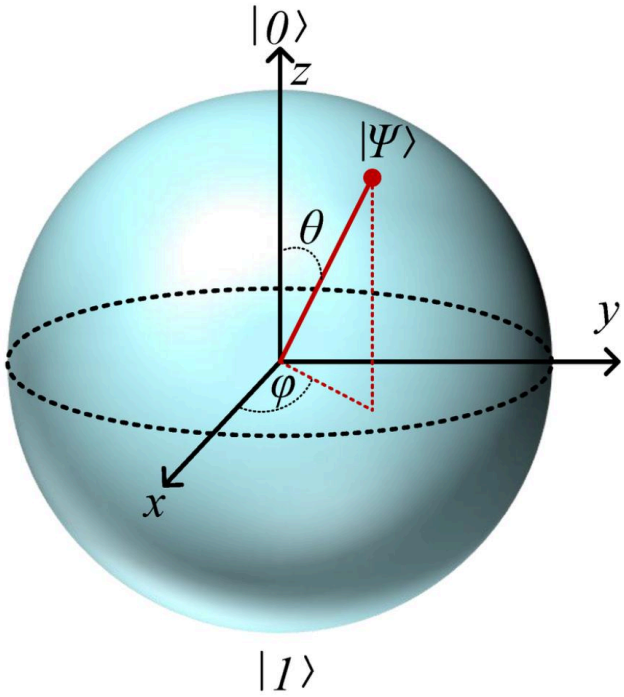
2.1 量子コンピューティングの進展状況と暗号学的危機

(Advancement of Quantum Computing & The Cryptographic Crisis)

現代の情報技術(IT)インフラは、0 と 1 のビット(Bit)演算を行う古典計算機の限界を前提として設計された暗号体系に依存しています。しかし、量子力学の原理である重ね合わせ(Superposition)と量子もつれ(Entanglement)を利用する量子コンピューティング技術の急速な発展は、この前提自体を根本から揺るがしています。

近年、IBM、Google、Quantinuum などの主要技術企業は、数百キュービット(Qubit)級のプロセッサを超え、誤り訂正(Error Correction)が可能な「論理キュービット(Logical Qubit)」段階へと入りつつあります。これは、量子コンピュータが実験室の域を超え、実用的な演算能力を備えた商用化段階へ進んでいることを示唆します。

暗号学の観点から見れば、この進展は「危機」と定義されます。現代の公開鍵基盤(PKI)の安全性は、「大きな整数の素因数分解」や「離散対数問題」を解くのに天文学的時間を要するという計算複雑性(Computational Complexity)の仮定に依拠しています。しかし、Shor's Algorithm を搭載した量子コンピュータは、これらの数学的難題を多項式時間(Polynomial Time)内で解ける可能性を持つため、既存のインターネット通信や金融取引を支えてきたセキュリティの防壁を突き崩し得ます。



Visualization of the state of a qubit Ψ in the Bloch sphere

「ブロッホ球におけるキュービット Ψ の状態可視化」

2.2 レガシーブロックチェーン（RSA/ECC 基盤）の構造的崩壊リスク
（Structural Collapse Risk of Legacy Blockchains based on RSA/ECC）

ブロックチェーン技術の核心は分散化された信頼であり、この信頼はデジタル署名（Digital Signature）によって担保されます。Bitcoin、Ethereum を含む現在の主要ブロックチェーン・ネットワークの大半は、楕円曲線暗号（ECC）、具体的には ECDSA（Elliptic Curve Digital Signature Algorithm）または RSA アルゴリズムを使用しています。

量子優位（Quantum Supremacy）の時代が到来した場合、これらのレガシー・ブロックチェーンは、次のような構造的崩壊リスクに直面します。

1. 公開鍵逆算とウォレット奪取: Shor のアルゴリズムを用いれば、ブロックチェーン上で公開されている公開鍵（Public Key）から、ユーザーの秘密鍵（Private Key）を導出し得ます。これは、攻撃者が正当な所有者の知らないうちに資産を移転したり、スマートコントラクトの権限を奪取したりできることを意味します。

2. トランザクション改ざん: 楕円曲線離散対数問題（ECDLP）が無力化されれば、攻撃者は有効な電子署名を偽造できるようになります。これはブロックチェーンの完全性（Integrity）を破壊し、二重支払い（Double Spending）攻撃を可能にし、ネットワークの経済価値を「0」に収斂させるおそれがあります。

3. コンセンサス・アルゴリズムの麻痺: PoS（Proof of Stake）などの合意形成プロセスにおいても、バリデータの署名は不可欠です。署名体系が破られれば、ネットワーク全体の合意を操作したり機能停止に追い込んだりすることが可能になります。

4. ハッシュアルゴリズムの安全強度低下（Weakening of Hash Algorithms via Grover’s Algorithm）: Shor のアルゴリズムが非対称鍵暗号（電子署名）を無力化する一方で、Grover’s Algorithm は、ブロックチェーンの連結構造と完全性を支えるハッシュ関数（Hash Function）を脅かします。

    - 量子加速と安全水準の半減: Grover のアルゴリズムは、非構造化データ探索を量子的に加速（Quadratic Speedup）することで、ハッシュ関数の衝突耐性（Collision Resistance）を弱めます。理論上、これは現在用いられている SHA-256 などのハッシュアルゴリズムの安全強度を半分程度（128 ビット相当）に低下させる効果を持ちます。
    - 対処法の違い: ハッシュ関数については、出力長を拡張する方法（例: SHA-256 → SHA-512）により、量子脅威への防御を一定程度強化できます。しかし、電子署名（ECDSA）は Shor のアルゴリズムにより数学的難題そのものが崩壊するため、単純な鍵長拡張では防御できず、耐量子暗号（PQC）への全面的なアルゴリズム置換だけが唯一の解決策となります。

5. 結論: 構造的転換の不可避性（Inevitability of Structural Transition） 結果として、既存ブロックチェーンは、ウォレットの安全性と所有権証明を担う電子署名領域において「存在論的脅威（Existential Threat）」に直面しています。したがって、ブロックチェーンの持続可能な安全性を確保するには、既存体系の漸進的修正ではなく、設計段階から PQC 電子署名を搭載したインフラへの構造的転換が不可欠です。

2.3 「Harvest Now, Decrypt Later」攻撃とレガシー脆弱性
(HNDL Attack & Legacy Vulnerability)

量子コンピュータがまだ商用化されていない現時点においても、セキュリティ脅威は現実のものです。その理由はまさに、「Harvest Now, Decrypt Later(HNDL)」攻撃シナリオの存在にあります。

1. 攻撃メカニズム: ハッカーや敵対的国家機関は、現在の暗号技術で保護されたデータ(トランザクション記録、通信パケット等)を現時点では解読できなくても、大量に収集・保存します。そして数年後、十分な性能を持つ量子コンピュータが開発された時点で、一括して解読します。

2. ブロックチェーンのジレンマ(Immutability Paradox): ブロックチェーンの「不変性」は、この攻撃シナリオにおいて致命的弱点となり得ます。ブロックチェーンに一度記録されたデータは削除も修正もできません。したがって、現在 RSA/ECC ベースで生成されたトランザクション記録は、将来にわたり恒久的に露出する運命に置かれています。

3. レガシー脆弱性: 既存ブロックチェーンが将来ソフトフォークを通じて PQC へアップグレードされたとしても、アップグレード以前に生成された過去のアドレスやトランザクションは依然として旧式アルゴリズムで署名されたままです。攻撃者はこれら過去データを通じて初期侵入点(Entry Point)を確保したり、長期間移動していない資産(Sleeper Wallets)を奪取したりできます。これを「量子レガシー脆弱性」と呼び、事後的対応では解決できない根本問題と位置づけます。

2.4 耐量子(PQC)移行の緊急性およびグローバル標準動向
(Urgency of PQC Transition & Global Standardization)

量子脅威に対応するためのグローバルな標準化作業は、すでに「準備」の段階を超え、「移行」の段階へと入りつつあります。

- NIST 標準化の完了: 米国国立標準技術研究所(NIST)は、2016 年から進めてきた耐量子暗号公募を経て、2024 年 8 月に SPHINCS+(SLH-DSA)、Kyber(ML-KEM)、Dilithium(ML-DSA)を最終標準アルゴリズム(FIPS)として正式発表しました。これは、PQC がもはや実験的技術ではなく、産業標準であることを確定づける出来事です。
- 各国政府による義務化: 米国ホワイトハウスは国家安全保障覚書(NSM-10)を通じ、すべての連邦機関システムを 2035 年までに PQC へ移行するよう指示しており、NSA(国家安全保障局)も CNSA 2.0 スイートを公表して移行を促進しています。
- 緊急性: システム移行には通常、数年以上の時間を要します。量子コンピュータの進展速度が想定以上に速い可能性(Y2Q 問題)を考慮すると、今ただちに PQC を導入しないシステムは、将来の技術的負債(Technical Debt)ではなく、「セキュリティ破綻」に至ることになります。

したがって、NIST 標準である SPHINCS+ を搭載した Quantarium の登場は、単なる技術的進歩ではなく、変化しつつあるグローバル・セキュリティ標準に適合する、唯一かつ緊急性の高い代替案です。

3. Quantarium ソリューションおよび設計哲学 (Solution & Philosophy)

Quantarium は、既存ブロックチェーンの限界を克服するための漸進的改善（Incremental Improvement）ではなく、量子コンピューティング時代の到来というパラダイム転換に対応するための根本的再設計（Fundamental Redesign）です。当社のソリューションは、セキュリティを妥協不可能な最優先価値として位置づけ、その実現のために「ネイティブ PQC」と「NIST 標準準拠」の二つを中核軸として設計されています。

3.1 設計原則：セキュリティ優先（Security-First）と不変性 （Design Principles: Security-First & Immutability）

Quantarium のアーキテクチャは、あらゆる設計段階において「Security-First（セキュリティ優先）」原則に従います。これは、性能（Scalability）や利便性（Usability）のためにセキュリティを犠牲にしないことを意味します。

- 真の不変性（True Immutability）の定義: 既存ブロックチェーンが主張する不変性は、「現在の計算能力」を前提としています。しかし、量子コンピュータの演算能力の前でもデータが改変されず保護されてこそ、真の不変性と呼べます。Quantarium は、「現在記録されたデータは、将来のいかなる技術的進歩によっても改ざんされない」という命題を満たすよう設計されています。
- Zero Trust に基づく設計: 当社は、ネットワーク参加者だけでなく、将来の計算環境すらも無条件には信頼しません。そのため、潜在的な解読技術の発展を前提に置き、最も保守的かつ検証済みの暗号学的方法論のみを適用してリスクを最小化します。
- 長期的データ生存性（Long-term Data Survivability）: 金融資産、本人情報、公共記録などは、数十年以上保存されなければなりません。Quantarium は、短期的なトランザクション処理速度競争よりも、50 年後、100 年後においてもデータ完全性を保証する「デジタル永続性」を目標としています。

3.2 ネイティブ耐量子性（Native PQC）アーキテクチャ （Native Post-Quantum Cryptography Architecture）

多くのブロックチェーン・プロジェクトは、既存アルゴリズム（RSA/ECC）の上に PQC を付加するハイブリッド方式、あるいはソフトフォークによる移行を計画しています。しかし Quantarium は、ジェネシスブロック（Genesis Block）の時点から PQC を適用する「ネイティブ（Native）」アプローチを採用します。

- **レガシーゼロ（Zero Legacy）:** 既存チェーンのアップグレード方式は、アップグレード以前の過去データ（Old Tx）を旧式暗号体系のまま残す「レガシー脆弱点」を抱えます。Quantarium は開始点から耐量子アルゴリズムを適用するため、ネットワーク全履歴にわたり、量子攻撃に脆弱な弱い輪（Weak Link）が存在しません。

- 全方位的セキュリティ適用 (Full-Stack Security) : 耐量子性は特定レイヤーのみに限定されません。

  1. Wallet Layer : アドレス生成および鍵管理の段階から PQC を適用します。
  2. Transaction Layer : 資産移転に関する署名および検証を担います。
  3. Consensus Layer : 検証ノード間の合意メッセージおよびブロック提案署名を保護します。このように、システムの全階層が同一水準の PQC セキュリティ強度によって保護されます。

- Harvest Now, Decrypt Later への防御: ネイティブ PQC アーキテクチャは、現在収集されている暗号化データ・パケットさえも、将来の量子コンピュータによって解読されないようにします。これにより、データの機密性と完全性は将来時点にまで拡張されます。

3.3 NIST 標準準拠および構造的回復力の確保
(NIST Standard Compliance & Structural Resilience)

独自暗号アルゴリズムには、未検証の脆弱性を内包するリスクがあります。Quantarium はグローバルなセキュリティ標準に準拠することで、エンタープライズ級の信頼性を確保しています。

- NIST 標準 SPHINCS+ の採用: 当社は、米国国立標準技術研究所(NIST)が耐量子電子署名標準として選定した SPHINCS+ 系列を中核エンジンとして採用しました。これは、世界の暗号学界による長年の公開検証(Public Review)を経たアルゴリズムであり、数学的安全性が立証されています。

- ハッシュベース署名の構造的回復力: SPHINCS+ は、格子基盤(Lattice-based)暗号とは異なり、特定の数学的難問(SVP など)に依存せず、暗号学的ハッシュ関数(Hash Function)の安全性のみに依存します。これは、将来新たな数学的解読法が見つかって他の PQC アルゴリズムが脅かされたとしても、ハッシュ関数が安全である限り、システムが崩れないことを意味します。Quantarium は、この「構造的回復力(Structural Resilience)」によって、最後の砦に相当する安全性を提供します。

- 規制適合性(Regulatory Compatibility): NIST 標準の採用は、今後各国政府および金融規制当局が求めるセキュリティ・ガイドライン(例:CNSA 2.0)を先取りして満たすものです。これは、Quantarium が制度金融および公共インフラに採用される上で決定的な競争優位をもたらします。

4. QUANTA-X: 中核耐量子暗号エンジン

Quantarium は、単一の暗号アルゴリズムの適用にとどまらず、システム全体を包含する包括的な「PQC セキュリティ・スタック（PQC Security Stack）」を構築しました。このスタックは、自社開発の QUANTA-X エンジンを中核とし、NIST 標準アルゴリズムである SPHINCS+ の完全性と Stateless 構造の安定性を結合することで、エンタープライズ級のブロックチェーン基盤を完成させます。

4.1 QUANTA-X エンジン：次世代セキュリティの中核

（QUANTA-X Engine: The Core of Next-Gen Security）

QUANTA-X は、Quantarium ネットワークにおける暗号学的演算を専担する高性能セキュリティ・エンジンです。単なるアルゴリズム・ライブラリではなく、ブロックチェーン環境に最適化された統合暗号モジュールとして、以下の中核機能を担います。

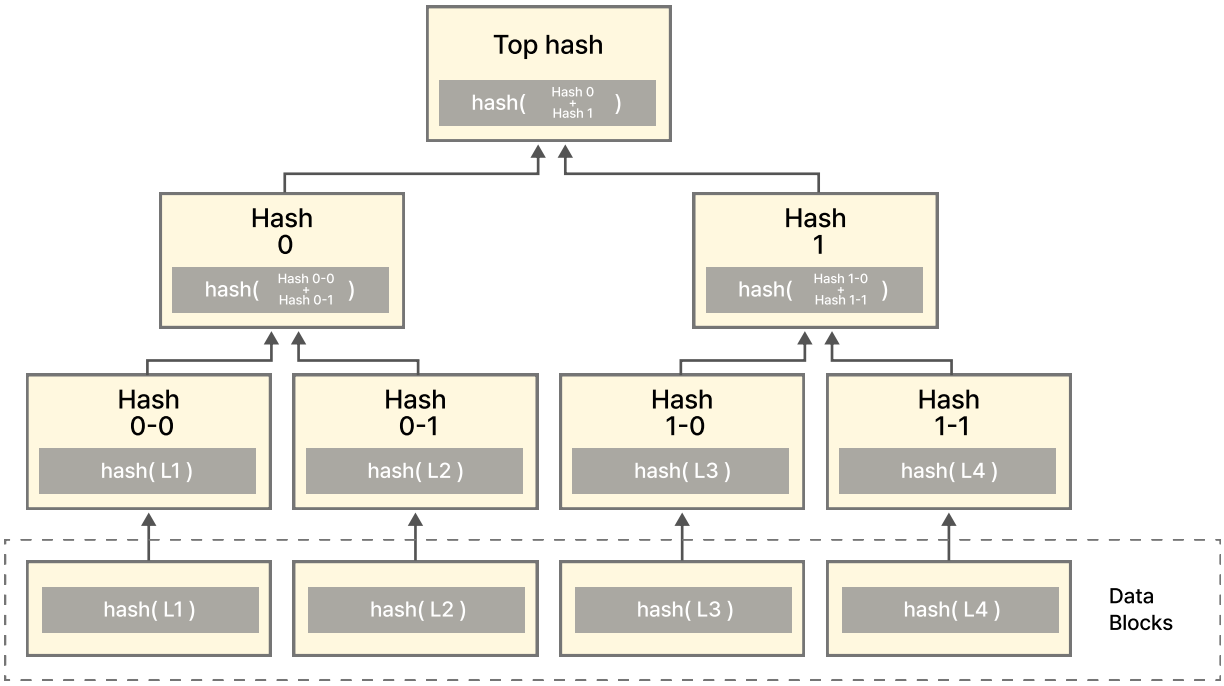
- ハイブリッド鍵管理システム（KMS）：耐量子鍵対の生成・保存・読み込みを隔離メモリ空間で処理し、サイドチャネル攻撃を防御します。
- 署名速度最適化（Signature Acceleration）：ハッシュベース署名に伴う比較的大きな署名サイズと検証時間を、ブロックチェーンのリアルタイム処理要件に合わせて最適化します。
- 柔軟な抽象化層（Abstraction Layer）：将来、暗号標準が変更されたり新規アルゴリズムが登場したりしても、ハードフォークなしでエンジン・レベルで柔軟に置換・更新できるモジュール構造を備えます。

4.2 QUANTA-X アルゴリズム：完全ハッシュベース電子署名

（QUANTA-X Engine: The Core of Next-Gen Security）

Quantarium は、米国国立標準技術研究所（NIST）が FIPS 205 標準として制定した SPHINCS+（SLH-DSA）を、メインネットの基本署名アルゴリズムとして採用しました。これは、格子基盤暗号とは異なり、数学的難問に依存しない、最も保守的かつ安全な選択です。

- セキュリティ仮定の最小化：SPHINCS+ の安全性は、暗号学的ハッシュ関数の安全性（衝突耐性および原像耐性）のみに依存します。
- 長期的信頼性：特定数学構造を用いないため、量子アルゴリズム進展の予測が不確実な環境下でも、最も低リスクな Fail-Safe ソリューションとして評価されます。
- 検証済み標準：世界中の暗号学者による公開検証を経た NIST 標準アルゴリズムを用いることで、独自アルゴリズムに潜むバックドアや設計不備の可能性を原理的に排除しています。



A structure where data blocks are connected in a tree-like form and converge to the top-level root hash

データブロックがツリー状に連結され、最上位のルートハッシュに集約される構造

4.3 Stateless 構造による安定性確保 (Stability via Stateless Architecture)

初期のハッシュベース署名(XMSS、LMS など)は、鍵使用回数を記録しなければならない Stateful 方式でした。これは、状態同期に失敗すると同一のワンタイム鍵を再利用することになり、セキュリティが崩壊するという致命的欠点を持っていました。Quantarium は、SPHINCS+ の Stateless 特性により、これを解決しています。

- 複数署名およびバックアップ安全性:ウォレット復旧やクラウド VM 複製の状況でも、署名カウントを管理する必要がありません。
- FORS & WOTS+ 構造:状態を記憶せずとも確率的に鍵再利用を防止し、分散台帳環境に必要な非同期的安全性を提供します。
- 完全性保証:数十億件のトランザクションが発生しても署名鍵の安全強度は低下せず、ブロックチェーンの無停止運用を技術的に下支えします。

NIST SPHINCS+の実装および暗号学的完全性

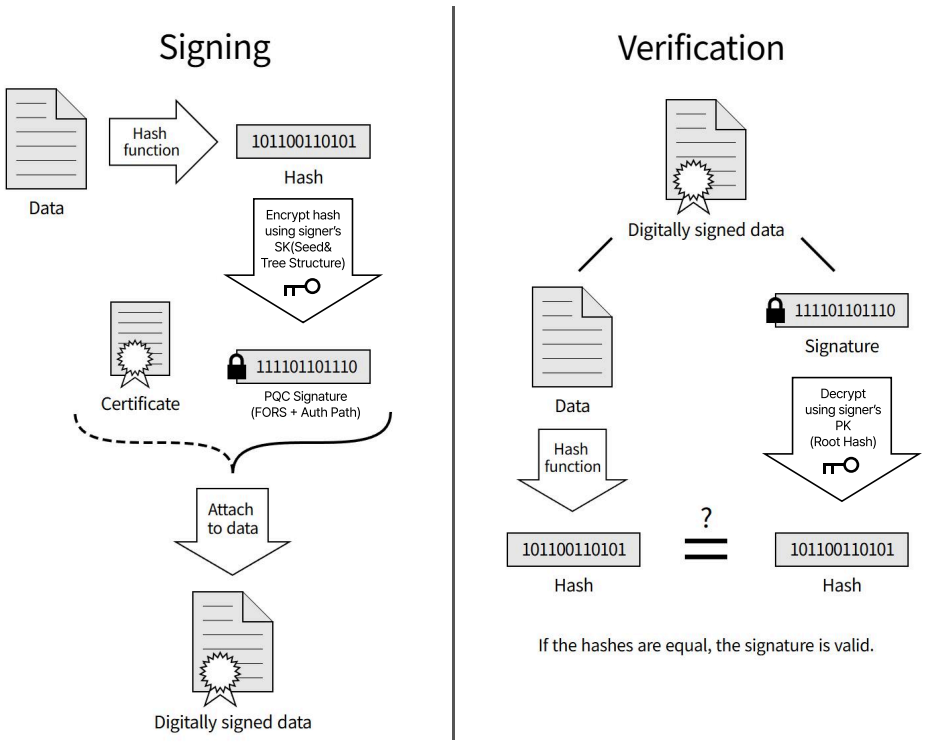
Quantarium のセキュリティ・スタックは、ネットワーク・アーキテクチャ内部で作動する純粋な暗号エンジンとプロトコルの集合体です。当社は、NIST 標準である SPHINCS+ を単に導入するだけでなく、これをブロックチェーン環境の制約条件に合わせて最適化し、鍵管理の安全性を最大化する独自実装技術を適用しました。

5.1 SPHINCS+：構造的回復力を備えた完全ハッシュベース署名

（SPHINCS+: Structural Resilience via Hash-Based Signature）

Quantarium は、格子基盤暗号とは異なり、量子コンピュータ環境下でも長期的な暗号安全性を提供するよう設計された SPHINCS+ を採用しています。

- 数学的難問からの独立：既存公開鍵暗号が依存する素因数分解や離散対数問題に依存しない、完全なハッシュベース・ポスト量子電子署名方式です。
- 構造的回復力：特定の数学的仮定が崩壊してもシステム全体の安全性は崩れず、将来の暗号環境の不確実性の中でも根源的耐性を提供します



送信者（Proposer）が秘密鍵でデータに署名 → ネットワーク送信

→ 受信者（Validator）が公開鍵で署名を検証。

5.2 PQC 署名メカニズムの中核適用範囲 （Core Application of PQC Mechanism）

Quantarium は、SPHINCS+ 系列の構造を選択的オプションではなく、ネットワーク全体を制御する基本電子署名メカニズムとして採用しました。このセキュリティ・スタックは、以下の中核行為に必須的に使用されます。

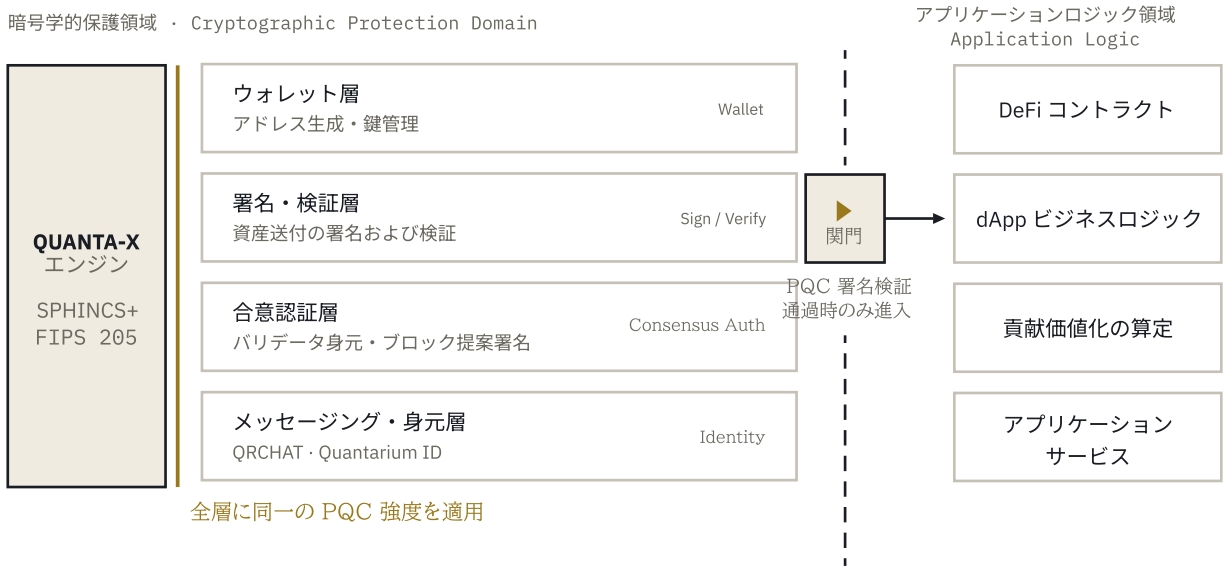
1. トランザクション生成および署名：資産移転やスマートコントラクト呼出時に、利用者秘密鍵を保護し、取引完全性を証明します。
2. 検証者の本人認証および権限証明：PoA 合意に参加するノードの正当性を耐量子暗号により認証します。
3. 合意過程の暗号学的証明：ブロック提案、検証、確定に至る全過程の署名行為を保護します。

5.3 階層別統合およびセキュリティ領域の明確化 (Layered Integration & Domain Definition)

Quantarium の PQC セキュリティ・スタックは、ウォレット層、署名・検証（Sign/Verify）層、合意認証（Consensus Auth）層、メッセージングおよび本人性（Identity）層全体に一貫して適用されます。特に、このセキュリティ・スタックは、システム・アーキテクチャ内において暗号学的保護領域（Cryptographic Protection Domain）とアプリケーション・ロジック領域（Application Logic Domain）を明確に分離する基準点となります。

- 透明な責任定義: セキュリティ・スタックは中核暗号演算を専担し、アプリケーション・ロジックはビジネス・プロセスのみを処理するよう隔離することで、システムの安全範囲と責任境界を透明に定義します。これにより、複雑な dApp ロジックの不具合がメインネットの安全基盤を揺るがさないようにする安全装置として機能します。

PQC セキュリティスタックと責任領域の分離 PQC Stack & Domain Separation



右側領域のロジック欠陥は、左側領域の合意や資産の安全性に伝播しない — 責任の境界が構造として定義される。
スマートコントラクト言語に暗号演算を持ち込まず、認証層でセキュリティを強制する（8.1）。

6. Layer 1 アーキテクチャおよび Proof of Authority

高性能な量子耐性合意モデル（High-Performance PQC Consensus）

Quantarium は、他ブロックチェーンに従属するトークンやサイドチェーンではなく、独自のプロトコルと台帳を有する独立した Layer 1 ブロックチェーンです。当社は、PQC に伴うデータ・オーバーヘッドをシステム水準で受け止めつつ、エンタープライズ級サービスに必要な高速トランザクション処理と予測可能なネットワーク性能を保証するため、Proof of Authority（PoA）合意方式を採用しました。

6.1 独立 Layer 1 インフラの設計目的
（Purpose of Independent Layer 1 Infrastructure）

既存の EVM ベース Layer 2 ソリューションは拡張性問題を緩和し得ても、基底レイヤーである Ethereum 等が有する量子脆弱性（ECDSA 依存性）を継承せざるを得ません。

- ネイティブ最適化：QUANTA-X および SPHINCS+ のような大容量署名データを効率的に処理できる専用ブロック構造とガス政策を独自実装しています。
- 主権的ガバナンス：外部メインネットのハードフォークや政策変更に左右されず、NIST 標準変更など暗号学的課題に即応できる技術的主権を確保しています。

6.2 PoA コンセンサスメカニズムの作動原理
（Operational Mechanics of PoA Consensus）

Quantarium の PoA は、匿名多数が競争する仕組みではなく、検証済み少数ノードが協働する構造です。

- 計算競争の排除（No Mining Competition）：PoW と異なり、無意味なハッシュ計算競争を排除することでエネルギー消費を大幅に削減し、資源を取引検証とスマートコントラクト実行へ集中させます。
- 低遅延・高スループット：限定数の検証ノード間で最適化された P2P 通信経路を構成し、数千 TPS 超の処理量とリアルタイム決済に近い応答性を提供します。
- 予測可能な性能：ブロック生成周期が決定論的に維持されるため、企業向けアプリケーション運用に必要な SLA 水準の予測可能性を提供します。

6.3 暗号学的に検証された権限モデル
（Cryptographically Verifiable Authority）

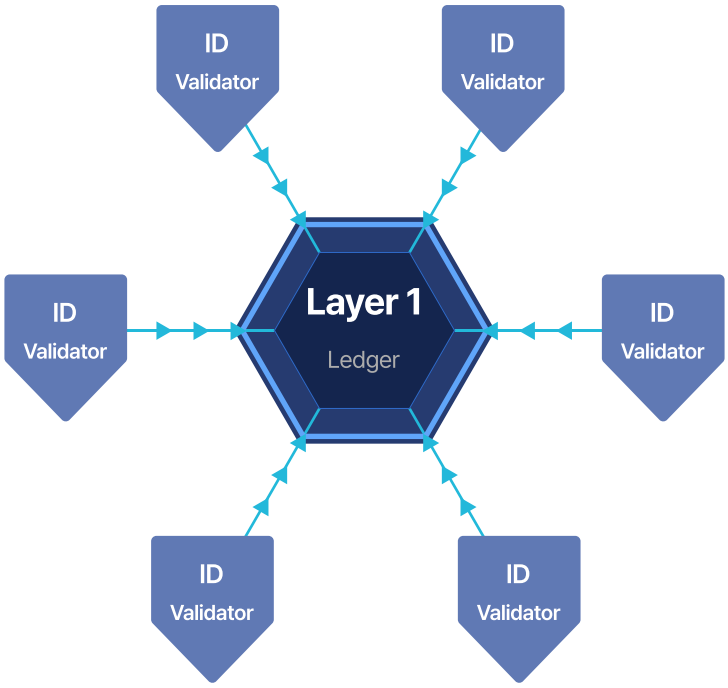
従来の PoA が中央集権的評判のみに依存していたのに対し、Quantarium の PoA は PQC 技術と結合した信頼モデルを提示します。

- QUANTA-X および SPHINCS+ に基づく本人性証明：すべての検証ノードは、ネットワーク参加時に SPHINCS+ 鍵対を用いて自らの身元を証明しなければなりません。
- 検証可能な権限委任：合意参加者の信頼性は、中央機関の恣意的判断ではなく、スマートコントラクトに明示されたガバナンス規則とオンチェーン証拠によって保証されます。
- 説明責任（Accountability）：ブロック生成者が自己の秘密鍵でブロックに署名するため、悪意ある行為が発生した場合には当該ノードを即時に識別・排除できます。

6.4 結論：実用主義とセキュリティの均衡

結論として、Quantarium の Layer 1 PoA アーキテクチャは、耐量子性という「極限の安全」と、商用サービスが要求する「快適な速度」とを同時に実現するための最適解です。当社は、暗号学的に検証された権限モデルを通じて、分散化の理念を損なうことなく、現実世界のビジネスを受け入れられる高効率ブロックチェーン環境を提供します。

Quantarium PoA Consensus Architecture



透明性と説明責任に基づくオンチェーン・ガバナンス

Quantarium のガバナンス・モデルは、分散ネットワークの柔軟性とエンタープライズ環境が求める厳格な統制力を結合しています。匿名性に依拠した無責任な合意参加を排除し、数学的に検証された身元と明確なプロトコル規則に基づいてネットワークを運営します。

7.1 信頼基盤の参入障壁：検証者資格要件 (Validator Qualification)

Quantarium・ネットワークのバリデーター(Validator)になるためには、単に資本(Stake)を預けるだけでは不十分であり、厳格な技術的・法的基準を満たす必要があります。

- PQC ベース暗号学的身元バインディング：候補検証者は QUANTA-X エンジンで生成した SPHINCS+ 鍵対をネットワークに登録しなければなりません。
- インフラ完全性検証：24/7 可用性を保証するハードウェア仕様とセキュリティ・モジュール連携環境を備え、テストネット段階で事前検証されます。
- KYC/KYB 認証：匿名攻撃者によるネットワーク掌握を防ぐため、運営主体の実在性を確認する手続きを経ます。

7.2 責任性強化メカニズム：スラッシングおよび自動失効 (Slashing & Automatic Revocation)

ネットワークの信頼を損なう行為に対しては、スマートコントラクトにより即時かつ自動化された制裁措置が講じられます。これにより、「善意」ではなく「システム」によって担保される信頼を構築します。

- 二重署名(Double Signing)の検知：同一ブロック高で複数ブロックに署名する行為をリアルタイムで検知し、直ちに権限を停止します。
- 可用性不足(Downtime)：定められた順序でブロックを生成できない、または同期を遅延させる場合、評判スコアに基づき合意グループから除外または資格剥奪となります。
- 預託金のスラッシング(Slashing)：悪意ある行為が立証された場合、保証金は焼却されるか、被害補填基金へ転換されます。

7.3 透明なオンチェーン・ガバナンス・プロセス
（On-Chain Governance Process）

Quantarium におけるすべての政策変更は、ブロックチェーン上で透明に決定されます。

- 提案および投票：ガス費政策、ブロックサイズ調整、PQC パラメータ更新等の主要変数は検証者投票により変更され、すべての記録が台帳に恒久保存されます。
- 緊急セキュリティ・プロトコル：緊急の安全脅威が検知された場合、全検証者の 3 分の 2 以上の同意により、即時にセキュリティ・パッチを適用し、またはネットワークを Safe Mode に移行できます。

7.4 規制準拠および監査容易性
（Compliance & Auditability）

このようなガバナンス構造は、金融機関および公共部門がブロックチェーンを導入する際に直面する最大の障壁である「不確実性」を除去します。

- 法的責任の所在明確化：すべてのトランザクションとブロックは、身元確認済み検証者によって処理されます。
- リアルタイム監査追跡：規制当局や外部監査人は、複雑な追加手続なくブロックチェーン・データを参照し、運営状況と資金フローを監視できます。

実行完全性とアクセス制御の分離

Quantarium のスマートコントラクト・アーキテクチャは、「言語の複雑性」ではなく「実行の安全性」に焦点を当てます。当社は、耐量子機能がコントラクト言語構文そのものに内在すべきだという通念を退け、代わりにアクセス制御と実行ロジックを明確に分離する実務的アプローチを採用します。

8.1 PQC の適用位置：言語ではなく認証層
（PQC Location: Auth Layer, Not Language Syntax）

Quantarium においてスマートコントラクトを記述する言語自体には、量子力学的アルゴリズムや複雑な暗号演算は含まれません。耐量子性は、スマートコントラクトが呼び出される時点、すなわち電子署名および認証層（Authentication Layer）において提供されます。コントラクト関数を実行しようとするすべてのトランザクションは、必ず SPHINCS+ ベース署名を通過して初めて実行エンジン内部へ進入できます。

- ロジックと安全性の分離: 開発者はビジネス・ロジック実装に集中し、誰が当該ロジックを実行できるかに関する安全性は Core Layer が PQC 署名を通じて保証します。

8.2 セキュリティ監査容易性（Ease of Security Auditing）

新しく難解なプログラミング言語を導入することは、むしろ潜在的バグや脆弱性を増大させる要因となり得ます。

- 検証済み標準準拠：業界標準に適合する実行環境を提供することで、既存の監査ツールや形式検証手法をそのまま適用できます。
- コード可読性：複雑な暗号演算をシステム・レベルへ抽象化することにより、監査者はロジック欠陥の検証に集中できます。

8.3 実行予測可能性 （Execution Predictability）

エンタープライズ環境におけるスマートコントラクトは、結果が決定論的でなければなりません。

- 隔離サンドボックス：スマートコントラクトは、合意エンジンおよび PQC 暗号モジュールと分離された環境で実行され、ネットワーク全体の合意へ影響を与えません。
- ガス費の明確性：PQC 署名検証コストとロジック実行コストを分離算定することで、利用者は実行費用を事前に予測できます。

9. Quantarium エコシステム概要 (Ecosystem Overview)

統合された耐量子セキュリティループ（Quantum-Resilient Security Loop）

Quantarium エコシステムは、個別サービスの単純な集合ではありません。ウォレット、決済、通信、資産移転というデジタル経済の四大要素が、一つの途切れない「耐量子セキュリティ・ループ」の中で有機的に統合された構造です。

9.1 単一のPQCセキュリティ哲学の共有 （Shared PQC Security Philosophy）

エコシステム内のすべてのアプリケーションおよびインフラは、「最初から最後まで安全に（Secure from End-to-End）」という共通のセキュリティ哲学を共有します。

- セキュリティの統一性： ユーザーがウォレットを生成する瞬間から、メッセンジャーでのコミュニケーション、資産の送信、決済の完了に至るまで、あらゆるプロセスにおいて、NIST標準のSPHINCS+に基づく同一のセキュリティ強度が適用されます。これは、サービス間を移行する際にセキュリティ水準が低下する「弱いリンク（Weak Link）」が生じないことを意味します。
- ユーザー体験（UX）の一貫性： 複雑なPQC鍵管理および署名プロセスはバックグラウンドで処理されるため、ユーザーはエコシステム全体を通じて、一貫性があり直感的なインターフェースを体験できます。

9.2 エコシステム中核構成要素 （Core Ecosystem Components）

1. Quantum-Resistant Wallet：PQC 鍵対の安全な生成と保管を担う、エコシステムの入口です。
2. QRCHAT：ウォレット・アドレスと連動した暗号化通信チャネルであり、量子コンピュータでも解読不能なメッセージ伝送を志向します。
3. Asset Bridge：他ブロックチェーン資産を Quantarium ネットワークへ安全に移送する経路であり、ブリッジ過程でも PQC 検証を実施します。

9.3 構造的隔離と拡散防止 （Structural Isolation & Containment）

Quantarium エコシステムは高度に相互接続されている一方で、セキュリティの観点からは厳格に区画化（Compartmentalization）されています。

- 脆弱性拡散の遮断：特定 dApp または構成要素の脆弱性がメインネット安全へ波及しないよう設計されています。
- モジュール型セキュリティ：各構成要素は独立した安全モジュールを通じて Core Layer と通信するため、システム全体崩壊へ直結しない回復弾力性を有します。
- 安全性の統一：ウォレット生成から会話、資産移転、決済に至るまで、NIST 標準 SPHINCS+ ベースの同一安全強度が適用されます。
- ユーザー体験の一貫性：複雑な鍵管理と署名処理はバックグラウンドで実行され、利用者は一貫的かつ直感的なインターフェースを体験します。

実利用によって証明されるインフラ（Infrastructure Proven by Real Usage）

セキュリティインフラの価値は仕様書ではなく、その上で実際に行き交うトランザクションの量によって証明されます。Quantarium は耐量子 Layer 1 を構築するにとどまらず、その上で日常的なコミュニケーションと取引が実際に発生するアプリケーションクラスタを併せて設計しました。本章では、QRCHAT をハブとするアプリケーションエコシステムの構造と、利用者の実利用行為をネットワークに対する検証可能な貢献として計量し報酬を配分する **貢献価値化（Contribution Valuation, CV）** 配分モデルを定義します。

10.1 設計背景: PoA ネットワークにおける参加の空白　(The Participation Gap in PoA)

第6章で述べたとおり、Quantarium は権威証明（PoA）合意を採用し、無意味な演算競争を排除しました。これは性能と予測可能性の面で明確な利点である一方、ひとつの構造的な空白を残します。

- **経済的な参加経路の不在**：作業証明（PoW）は採掘を通じて、持分証明（PoS）はステーキングを通じて、一般参加者にネットワークへの貢献経路を提供します。しかし Quantarium のバリデータ資格は、7.1 に定めるとおり KYC/KYB 認証と高可用性インフラを備えた少数の検証主体に限定されます。したがって、一般利用者がネットワークに貢献し、その対価を受け取る経路は構造的に存在しません
- **空白の解消方法**：Quantarium はこの空白を「演算量」や「保有持分」ではなく、実利用による貢献 で埋めます。利用者がエコシステム内のアプリケーションで行う通信・取引・本人確認の行為は、それ自体がネットワークに有効トランザクションと PQC 署名需要を発生させる実質的な貢献です
- **貢献価値化（Contribution Valuation）の定義**：貢献価値化とは、ネットワークに検証可能な需要を発生させた行為を計量し、事前に配分されたインセンティブ数量を配分する 経済的配分ポリシー（Distribution Policy） です。

[重要 — 必ず明示すること] 貢献価値化は合意アルゴリズムではありません。Quantarium メインネットにおけるブロック生成と確定は、第6章に定める PoA 合意によってのみ行われます。貢献価値化が合意層の信頼モデルに影響を及ぼすことは一切ありません。

10.2 アプリケーションクラスタ　(The Application Cluster)

1. ハブ・アンド・スポーク構造（Hub & Spoke Architecture）

   QRCHAT は単なるメッセンジャーではなく、エコシステム全体の ID・通信ハブ です。利用者は QRCHAT において SPHINCS+ 鍵ペアに基づく単一の ID（Quantarium ID）を生成し、この ID がクラスタ内すべてのアプリケーションの認証手段として用いられます。

   - **単一 ID、複数サービス**：利用者はアプリケーションごとに別個のアカウントを作成しません。ひとつの PQC 鍵ペアが、メッセンジャーへのログイン、取引の署名、決済の承認、本人性の証明に一貫して使用されます。
   - **9.1 の拡張**：これは 9.1 に定める「セキュリティの統一性」の原則をアプリケーション層まで拡張したものであり、サービス間を移動する際に認証強度が低下する「弱い環」を排除します。
   - **クロスアプリのネットワーク効果**：あるアプリケーションで獲得した利用者は、追加の登録手続きなしに他のアプリケーションの潜在利用者となります。これは個別サービス単位の成長曲線ではなく、エコシステム単位の複合的な成長構造を形成します

2. クラスタの構成

Quantarium アプリケーションクラスタは、貢献価値化の適用可否に応じて三つの層に区分されます。すべてのアプリケーションが同一のセキュリティスタックと ID 体系を共有する一方で、報酬の対象は規制適合性が確認されたサービスに限定 されます

Tier 1 - 貢献価値化の対象(Consumer Applications)

アプリケーション	カテゴリ	貢献の類型	発生するオンチェーン需要
QRCHAT	セキュアメッセンジャー（ハブ）	ID・通信	PQC ID 登録、ウォレットアドレス連携、暗号化セッション鍵の検証
RINGO	チャネル型通知・発信	通信	チャネル購読の認証、一斉配信の完全性記録
Right Now	超短期の生活オンデマンド	取引・決済	マッチング契約の成立・履行証明、精算トランザクション
Quantaro	匿名ハイパーローカル中古取引	コンテンツ・継続	コンテンツ利用記録、継続利用の証明
QRLIVE	ライブコマース	取引・コンテンツ	販売精算、インフルエンサー収益配分の記録
MOODI	感性 SNS・多人数音声/映像	通信・コンテンツ	多者間セッション認証、コンテンツ原本証明
Gcon	番号ベースのプライバシー通信	通信・ID	番号所有権の証明、通話・メッセージセッションの認証
Eggplant	占い・コンテンツ	取引・ID	匿名取引の接続、取引確定署名、揮発性セッションの検証

Tier 2 - ネットワーク需要は発生、個人報酬は対象外 (B2B / B2G)

アプリケーション	カテゴリ	役割
ANBANG	不動産仲介プラットフォーム (B2B·B2C·B2G)	事業者契約およびセキュア送信のトランザクションを発生させる。報酬は個人ではなく事業者向け精算体系で処理
CallAI	AI 電話応対・予約	予約台帳の完全性を記録。事業者向け SaaS であり、個人の貢献報酬の対象外

Tier 3 - 貢献価値化の適用除外 (Compliance Exclusion)

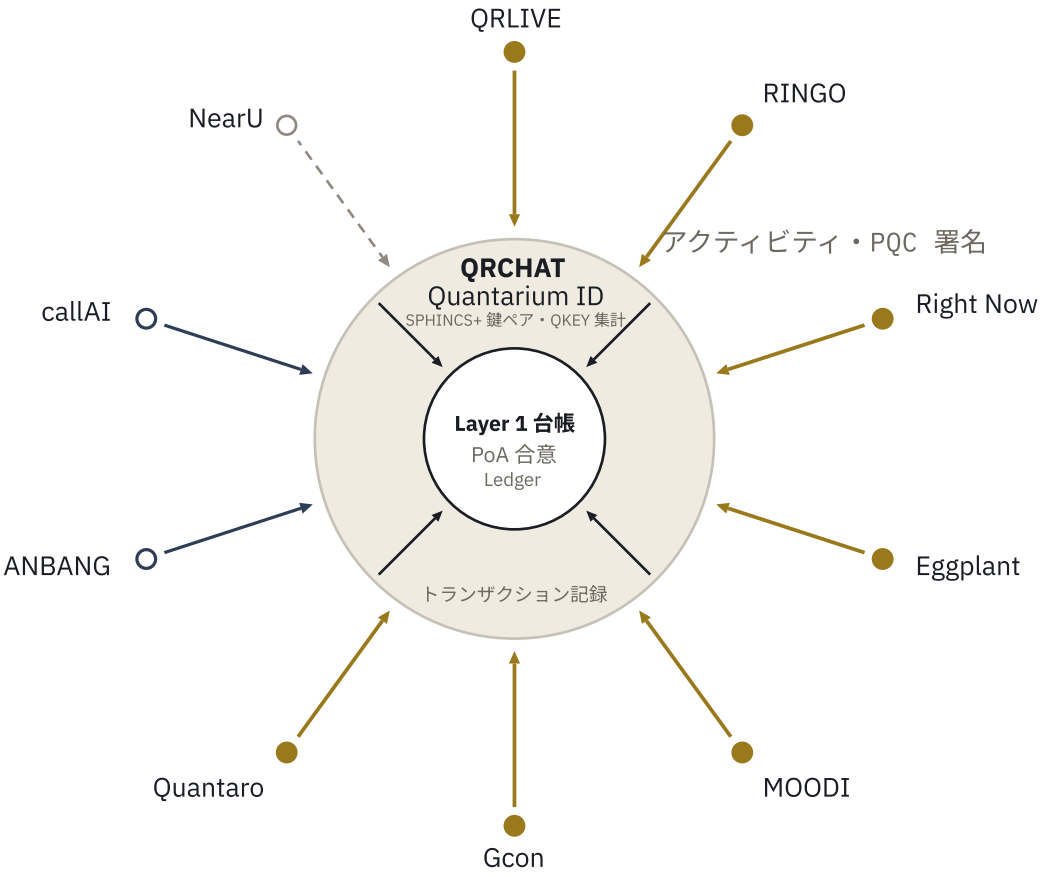
アプリケーション	除外の理由
NearU	児童安全サービス。未成年者が主たる利用者 であるため、暗号資産による報酬の対象から全面的に除外

別枠 - 取引所

QuantaEX	グローバルデジタル資産取引所。取引・流動性の貢献は貢献価値化ではなく **QX 報酬体系** が担う（10.8 参照）

アプリケーションクラスタと貢献経路

Application Cluster & Contribution Path



- Tier 1 — 貢献価値化の対象（QRCHAT を含む 8 種）
- Tier 2 — ネットワーク需要は発生、個人報酬は対象外（B2B・B2G）
- Tier 3 — 貢献価値化の対象外（未成年者向けサービス）

実線 = 報酬対象のアクティビティ

破線 = 需要のみ発生、報酬なし

10.3 貢献の定義と計量　(Contribution Metrics)

報酬の正当性は「何を貢献と認めるか」の明確さから生まれます。Quantarium は、ネットワーク価値に実質的に貢献する四つの類型のみを計量の対象として定義します。

類型	定義	代表的な行為	ネットワークへの貢献
ネットワーク貢献 (Network)	PQC 署名を伴う有効トランザクションの発生	決済、エスクロー取引、資産移転、セキュア通信セッションの開設	メインネット利用量の増加およびガス焼却の誘発
ID 貢献 (Identity)	エコシステムの ID 信頼度を高める行為	本人確認の完了、ウォレット連携、複数アプリの接続	シビル耐性の強化、ネットワーク信頼資本の蓄積
成長貢献 (Growth)	検証済みの新規参加者の流入	招待後に被招待者が実利用に到達すること、コミュニティへの貢献、公式イベントへの参加	利用者基盤の拡大
継続貢献 (Retention)	長期的・継続的な参加	継続利用期間、資産の長期保有およびロックアップ	流通数量の安定化、離脱率の低下

計量の原則

- **結果基準の計量**：単なるアクセスや滞在時間は貢献として認めません。貢献は、ネットワークに実需を発生させた 完結した行為 のみを基準として算定します。
- **重み付けのガバナンス統制**：各貢献類型の重み（Weight）および単位報酬係数は財団が恣意的に決定するものではなく、7.3 に定めるオンチェーンガバナンスのプロセス（提案および投票）を通じてのみ変更されます。すべての変更履歴は台帳に恒久的に記録され、監査が可能です。

10.4 3 層報酬アーキテクチャ　(Three-Layer Reward Architecture)

数千万人規模のマイクロな活動をすべてオンチェーンに記録することは、技術的にも経済的にも合理的ではありません。Quantarium は活動の **集計** と価値の **精算** を構造的に分離します。

層構造

① **アクティビティ層（Activity Layer）- オフチェーン アプリケーション**内の貢献行為はリアルタイムに集計され、**QKEY** として付与されます。この段階は台帳の外部で処理されるため手数料が発生せず、利用者は即時のフィードバックを体験します。QKEY は QRCHAT において既に稼働している付与体系であり、貢献価値化モデルはこれをエコシステム全体の標準的な活動単位へ拡張したものです。

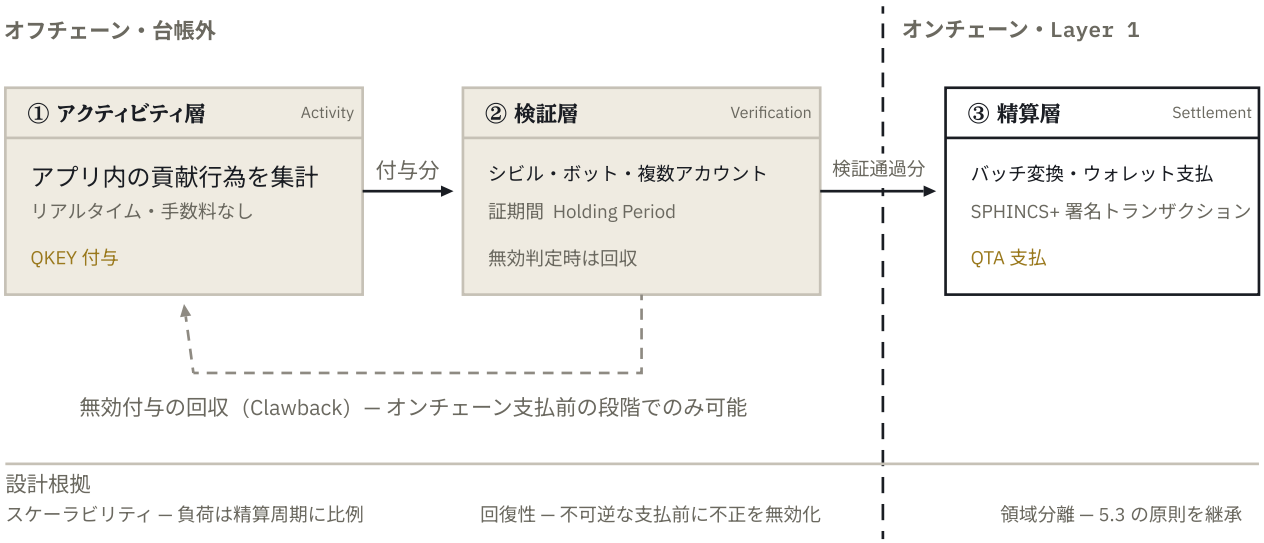
② **検証層（Verification Layer）** 付与された QKEY は直ちに確定せず、検証期間（Holding Period）を経ます。この層でシビル攻撃、自動化ボット、複数アカウント、異常な行動パターンが除外され、無効と判定された付与分は回収（Clawback）されます

③ **精算層（Settlement Layer）** - オンチェーン 検証を通過した QKEY は、定められた周期でバッチ方式により QTA へ転換され、利用者のウォレットへ支払われます。この転換は SPHINCS+ 署名を付したオンチェーントランザクションとして処理され、転換の記録は台帳に恒久的に残ります。

設計の根拠

- **スケーラビリティ（Scalability）**：マイクロな活動を個別のトランザクションとして記録すると、ブロック空間とガス負荷が利用者数に比例して急増します。バッチ精算はオンチェーン負荷を 活動量ではなく精算周期に比例 するよう定数化し、6.2 で保証したネットワーク性能（SLA）を損ないません。
- **回復可能性（Recoverability）**：オンチェーンの支払は不可逆です。オフチェーンの付与段階を置くことで、不正利用を確定支払の前に無効化でき、誠実な参加者の取り分が希薄化されません。
- **責任領域の分離（Domain Separation）**：この構造は 5.3 に定める「暗号学的保護領域とアプリケーションロジック領域の分離」の原則をそのまま継承します。報酬算定ロジックの欠陥が、メインネットの合意や資産の安全性に波及することはありません。

3 層報酬アーキテクチャ　Three-Layer Reward Architecture



10.5 排出ポリシーおよびデフレ構造との整合性 (Emission Policy & Deflationary Consistency)

貢献報酬モデルは Quantarium トークンエコノミーの既存原則を修正するものではなく、その枠内でのみ機能します。

(1) 新規発行なし (Zero New Issuance)

QTA の総発行量 1,000 億枚(100,000,000,000 QTA)は固定 され、貢献報酬のための追加発行は一切行いません。報酬の原資は、初期配分時点で確定した Mining & Community Incentives 20%(200 億 QTA) の数量の範囲内でのみ執行されます。

項目	内容
原資	QTA 初期配分のうち Mining & Community Incentives (20%、20,000,000,000 QTA)
新規発行	なし（総発行量は不変）
執行方式	四半期ごとの排出上限（Emission Cap）内でのバッチ精算
上限の変更	オンチェーンガバナンス投票によってのみ可能（7.3）

(2) 焼却連動の排出原則 (Burn-linked Emission)

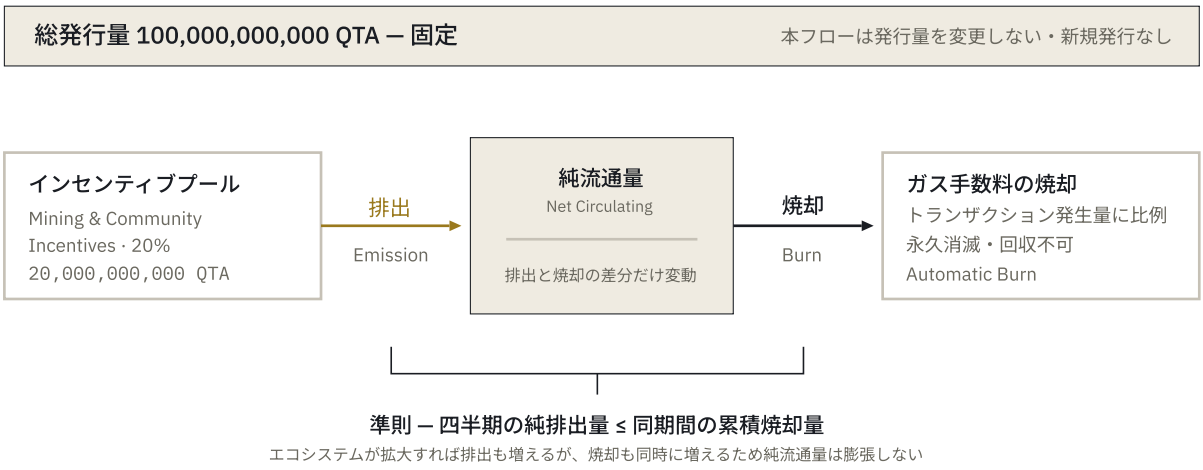
エコシステムの活性化は二方向に同時に作用します。アプリケーションの利用量が増えれば報酬の排出も増えますが、同時にオンチェーントランザクションが増加し、10.2(現 11.2)に定める 自動焼却メカニズムによるガス焼却量も併せて増加 します。

Quantarium はこの二つの流れを連動させて運用します。すなわち、四半期の純排出量が同期間の累積焼却量を超えないこと を排出ポリシーの準則とします。これにより、貢献報酬が拡大しても純流通量が構造的に膨張することはなく、本ホワイトペーパーが提示するデフレ構造は維持されます

(3) 逓減排出 (Decay Schedule)

単位貢献あたりの報酬係数は、累積参加者数および累積執行量に応じて段階的に低下します。これは初期参加者に過大な数量が集中し、価格ショックと即時の売り圧力を生む構造を防ぐための装置です

排出と焼却の整合性　Emission–Burn Consistency



10.6 規制遵守の原則 (Compliance Principles)

Quantarium は貢献報酬モデルを規制のグレーゾーンに置くことはせず、次の原則を設計上の制約として宣言します。

- **収益期待の排除**：貢献報酬は事業収益の分配ではなく、財団または第三者の努力による収益を約束または示唆するものではありません。報酬は利用者本人のサービス利用実績に対する対価です。
- **QKEY の非支払手段性**：QKEY は財貨または役務の対価として発行されるものではなく、財団は QKEY について預託・払戻の義務を負いません。
- **ゲーム的要素の範囲の限定**：報酬の対象となるゲーム的要素は、アプリケーション内のイベント、ミッション、ミニゲームなど **付加機能に限定** されます。ゲーム等級分類の対象に該当するサービスは貢献報酬の対象から除外され、当該サービスの財は QKEY および QTA と相互に転換されません。
- **未成年者の除外**（Minor Exclusion）：未成年者を主たる利用者とするサービスは貢献価値化の対象から全面的に除外され（10.2 Tier 3）、年齢確認を通過していないアカウントは QKEY の付与の有無にかかわらず QTA への転換が許可されません。
- **独立ポイント経済との分離**：個別のサービスが独自のポイント体系を運用する場合、当該ポイントは QKEY および QTA と相互に転換されず、別個の利用規約と精算体系に従います。これにより、サービス固有の規制リスクがメインネットのトークンエコノミーへ波及することを遮断します。
- **法域別の差異適用（Jurisdictional Compliance）**：貢献報酬の方針は、各法域の暗号資産規制、ゲーム関連法令、広告・景品規制に応じて、地域別に異なる形で適用され、または制限される場合があります。
- **AML/CFT との連動**：QKEY → QTA の転換は、マネーロンダリング防止および利用者保護の手続と連動して執行されます。

10.7 デュアルトークン構造との接点 (Interface with the Dual Token Structure)

貢献報酬モデルは、次章に定めるデュアルトークン構造の役割分担をそのまま踏襲します。

区分	報酬の流れ	原資
アプリケーション貢献（QKEY）	アプリ活動 → **QKEY** 付与 → **QTA** 精算	QTA 初期配分のうち Mining & Community Incentives 20%
取引所での活動	取引・流動性の供給 → **QX** 支払	QX 配分のうち Trading Rewards & Liquidity Incentives 35%

二つの報酬の流れは原資と対象行為が明確に分離されており、相互に干渉しません。QTA は **ネットワークの利用** に対する報酬資産として、QX は **取引所への参加** に対する報酬資産として、それぞれの位置づけを保ちます。

10.8 アプリケーションエコシステムの戦略的意義 (Strategic Implications)

- **インフラの検証**：クラスタは、Quantarium メインネットの性能と安定性を実利用環境において常時検証するリファレンスとなります。
- **自前の需要の確保**：大多数の Layer 1 プロジェクトが外部 dApp の誘致に依存するのとは異なり、Quantarium は自社のアプリケーションクラスタを通じて初期のトランザクション需要を内部で確保します。
- **PQC 普及への経路**：利用者は耐量子暗号を学ぶことなく、日常的なメッセンジャーや取引の利用を通じて PQC セキュリティ環境へ自然に組み込まれます。これは 3.1 の「セキュリティ優先」の原則が、利用者の利便性を犠牲にすることなく実装された事例です。

11.1 概要 (Overview)

Quantarium エコシステムは、技術的安定性と経済的流動性を同時に確保するため、メインネット基盤資産である QTA と、取引所エコシステムのユーティリティ資産である QX を分離運用するデュアルトークン構造を採用しています。

11.2 Quantarium メインネットコイン

(1) 定義および役割

QTA は Quantarium 耐量子メインネットのネイティブ資産であり、すべてのトランザクション手数料の支払い、スマートコントラクト実行、検証ノードの合意参加のための基軸通貨として用いられます。

(2) 発行およびバーンモデル (Supply & Burn)

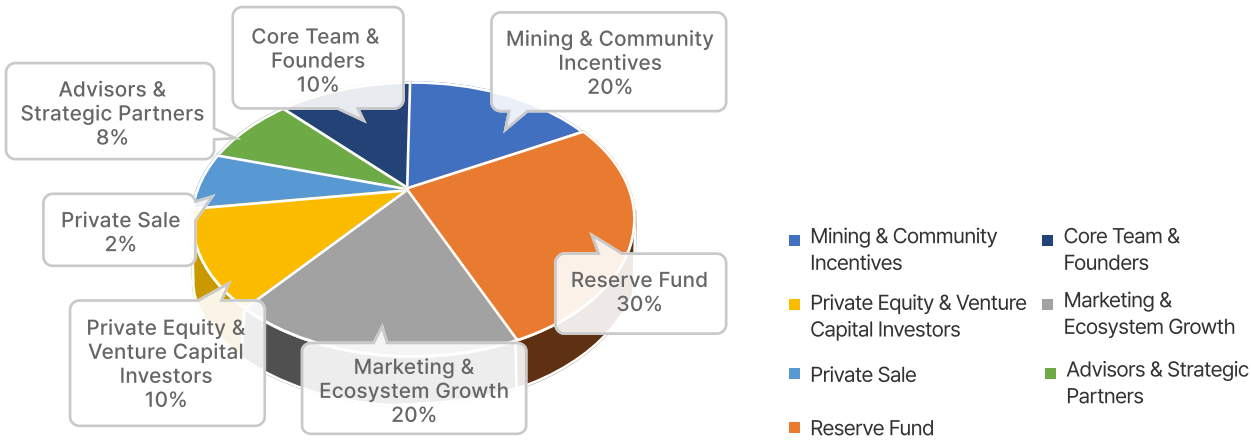
- 総発行量:1,000億枚 (100,000,000,000 QTA)
- 自動バーン・メカニズム(Deflationary Model) : QTAには、ネットワーク利用量に比例してガス手数料の一定割合が自動的にバーンされるアルゴリズムが実装されています。これにより、エコシステムが活性化するほど流通量が減少し、コインの希少価値が高まるデフレ構造が形成されます。

(3) QTA初期配分構造 (Initial Allocation)

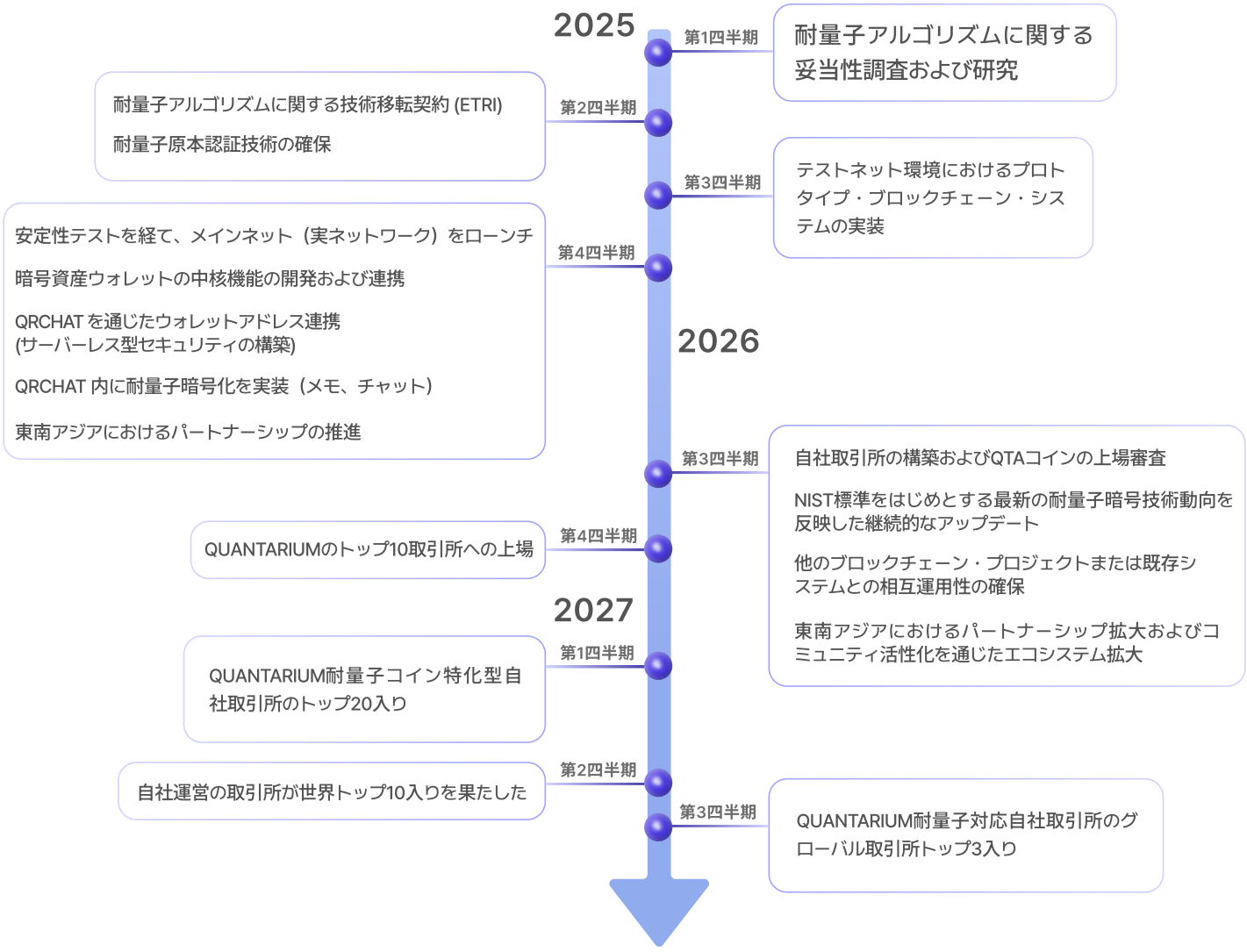
Quantarium財団は、長期的なエコシステム運営と分散化の実現に向けて、以下のとおり戦略的にトークンを配分しました。

Category (分類)	Allocation (%) (配分比率)	トークン数量 (Token Amount, QTA)	Description (説明)
Core Team & Founders (中核チームおよび創業者)	10%	10,000,000,000	核運営・技術保守・戦略ガバナンス
Advisors & Strategic Partners (アドバイザーおよび戦略的パートナー)	8%	8,000,000,000	法務・技術・事業助言
Marketing & Ecosystem Growth (マーケティングおよびエコシステムの成長)	20%	20,000,000,000	ブランド・コミュニティ・採用拡大
Private Equity & Venture Capital Investors (個人投資家およびベンチャー投資家)	10%	10,000,000,000	機関投資家・戦略投資家向け
Private Sale (プライベートセール)	2%	2,000,000,000	プライベートセール
Mining & Community Incentives (マイニングおよびコミュニティへのインセンティブ)	20%	20,000,000,000	採掘報酬・ステーキング・参加インセンティブ
Reserve Fund (予備金／準備金)	30%	30,000,000,000	安定性・R&D・戦略準備金
総発行量 (Total Supply)	**100%**	**100,000,000,000**	

QTA 初期の配分構造（Initial Allocation）



QUANTARIUM ロードマップ (ROAD MAP)



11.3 Quantarium Exchange ユーティリティトークン

(1) 定義と特徴

QX は、Quantarium 財団が構築する独自暗号資産取引所の中核ユーティリティ・トークンです。QTA がインフラ燃料であるなら、QX はサービス参加権と便益を付与するメンバーシップ・トークンとしての性格を持ちます

(2) 発行およびユーティリティ (Supply & Utility)

- 総発行量:10億個(1,000,000,000 QX)。追加発行のない固定数量
- 主なユーティリティ:

A. 取引手数料の割引:QXの保有量に応じた段階的な手数料優遇措置を提供

B. ランチパッド(Launchpad)への参加:有望なプロジェクトの初期トークン割り当てにおける優先権の付与

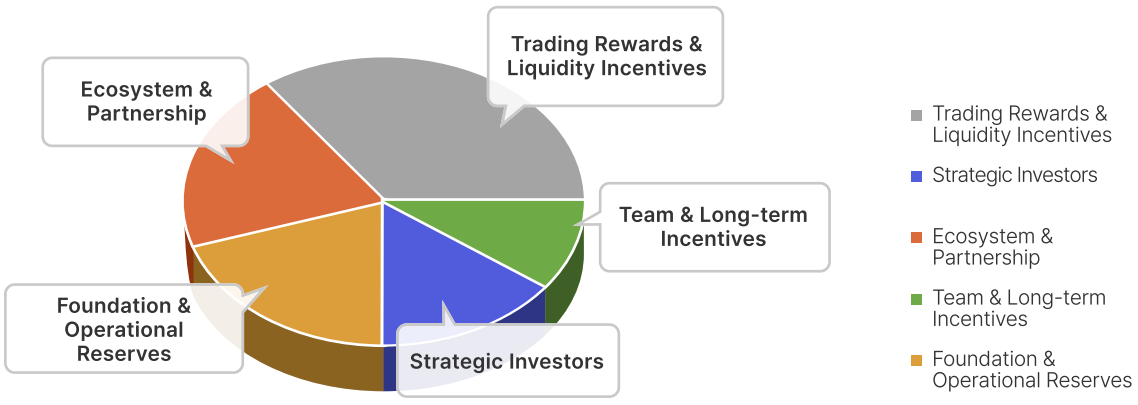
C. ガバナンス投票:上場審査および取引所の主要な方針に関する議決権の行使

D. PQCセキュリティ連携:ユーザーウォレット間の送金および出金時に、メインネットのPQC電子署名を適用し、量子耐性のあるセキュリティを確保

(3) QXの流通および配分構造　取引所のエコシステムにおける流動性の供給と参加者への報酬に重点を置いた配分方針を実施します。

Category (分類)	Allocation (%) (配分比率)	トークン数量 (Token Amount, QX)	Description (説明)
Trading Rewards & Liquidity Incentives (取引リワードおよび流動性報酬)	35%	350,000,000	流動性供給・取引活性化
Ecosystem & Partnership (生態系およびパートナーシップ)	20%	200,000,000	パートナーシップ・マーケティング・エコシステム基金
Foundation & Operational Reserves (基金および運営準備金)	20%	200,000,000	運営費・緊急準備金・R&D
Strategic Investors (戦略的投資家)	15%	150,000,000	初期資金確保・ネットワーク活用
Team & Long-term Incentives (チームおよび長期インセンティブ)	10%	100,000,000	中核人材の動機付け・採用
총 발행량 (Total Supply)	100%	1,000,000,000	

※ すべてのチーム分および投資家分トークンには、厳格なベスティング（Vesting）およびロックアップ（Lock-up）政策が適用されます。



11.4 QTA と QX の相互補完的シナジー（Structural Synergy）

QTA と QX は役割が明確に区分されつつも、相互補完的に機能します。QTA の価値はメインネット利用量に比例して上昇し、QX の価値は取引所プラットフォームの成長と利用者拡大に連動します。

比較項目	QTA (Mainnet Coin)	QX (Exchange Token)
位置づけ	メインネットのネイティブコイン (Infrastructure)	取引所ユーティリティトークン（Service）
総発行量	1,000億枚（100 Billion）	10億枚（1 Billion）
主要機能	ガス手数料（Gas）、 オンチェーン実行、コンセンサス検証	手数料割引、ローンチパッド、投票、VIP特典
価値向上要因	自動バーン（Burn）、ネットワーク需要の増加	流通量の削減（Lock-up）、プラットフォーム収益モデル
セキュリティ技術	Native PQC Layer 1による保護	出金・移転時におけるPQC署名連携

11.5 市場成長潜在力および展望（Market Potential Outlook）

Quantarium メインネットは、既存ブロックチェーンが解決できていない量子セキュリティ脅威を構造的に解決する次世代インフラです。

- セキュリティ・プレミアムの浮上：PQC ベース・メインネットへのデジタル・マイグレーション需要の増加が見込まれます。
- 時価総額成長シナリオ：保守的定着シナリオから、グローバル標準メインネットとして定着する楽観シナリオまで、段階的な価値上昇が想定されます。



これらの展望は、単なる期待値ではなく、変化するグローバルなセキュリティ標準（NIST等）と市場の構造的需要に基づく分析です。

12. 結論 (Conclusion)

量子時代を貫く不変の信頼（Immutable Trust for the Quantum Era）

デジタル資産の歴史とは、「信頼」を技術によって実装してきた過程でした。しかし、到来しつつある量子コンピューティング（Quantum Computing）の波は、既存の暗号体系（RSA、ECC）に依存してきた過去数十年の信頼構造を根本から脅かしています。

Quantarium のホワイトペーパーを締めくくるにあたり、私たちは自らの技術的指向をあらためて明確に定義するとともに、未来に向けたビジョンを提示したいと考えます。

12.1 Quantarium のアイデンティティ：誤解と真実（Identity of Quantarium: Clarification）

多くの人々は、「量子」という言葉から生じる混乱を抱えています。これに対し、Quantarium は自らの技術的本質を次のように明確に規定します。

「Quantarium は量子コンピュータを用いるブロックチェーンではありません。」

「Quantarium は量子コンピューティング時代においても生き残るブロックチェーンです。」

私たちは、量子力学的現象（重ね合わせ、エンタングルメント）を利用して演算を行うハードウェアではありません。

Quantarium は、量子コンピュータが槍のように既存のセキュリティを突破してくるとき、それを防ぎ得る唯一の盾である「耐量子暗号（Post-Quantum Cryptography）」を備えたソフトウェア・プロトコルです。私たちは攻撃のための道具ではなく、人類のデジタル資産を守る防御体系です。

12.2 不確実性を超える構造的回復力（Structural Resilience Beyond Uncertainty）

「Harvest Now, Decrypt Later（今収集し、後で解読する）」という攻撃シナリオは、未来の脅威ではなく、現在進行形の危機です。Quantarium はこれに対応するため、NIST 標準の SPHINCS+ を採用しました。これは、特定の数学的難問（素因数分解など）の崩壊の影響を受けないハッシュベース構造によって、量子コンピュータの進展速度やアルゴリズムの変化にかかわらず、システムの安全性を保証する構造的回復力（Structural Resilience）を確保したものです。

12.3 実用主義的イノベーション：セキュリティと速度の共存（Pragmatic Innovation: Coexistence of Security and Speed）

従来のセキュリティ強化技術は、必然的に性能低下を伴ってきました。しかし、Quantarium は独立した Layer 1 アーキテクチャと PoA（Proof of Authority）コンセンサス・アルゴリズムを組み合わせることで、このジレンマを解決しました。暗号学的に検証された信頼ノードを通じて、耐量子暗号に伴う重い演算負荷を吸収し、エンタープライズ環境で求められる即時ファイナリティ（Instant Finality）と高速トランザクションを実現しました。これは、Quantarium が理論上の実験室段階を離れ、現実経済を支える準備を整えたことを意味します。

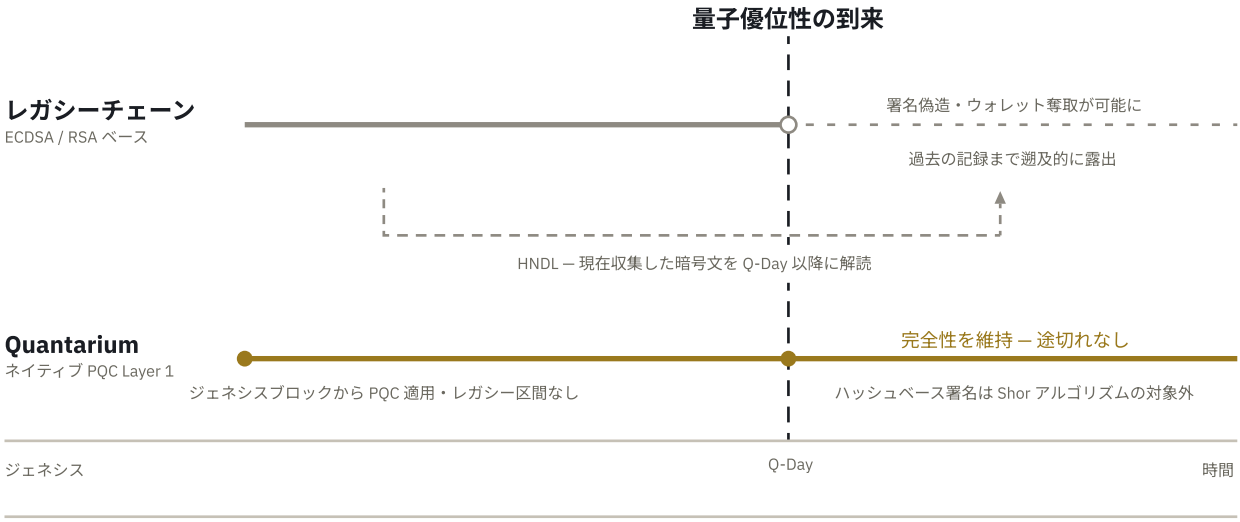
13.4 結び：デジタル・ノアの方舟　（Closing: The Digital Noah's Ark）

技術の進歩は祝福である一方、備えなき者にとっては災厄ともなり得ます。量子優位（Quantum Supremacy）の時代が到来し、既存のレガシー・ブロックチェーンの防御壁が崩れ落ちるとき、Quantarium は価値を安全に保全し、未来へと引き渡す「デジタル・ノアの方舟」となるでしょう。

Quantarium エコシステムは、ウォレット、決済、通信、資産移転に至る全プロセスを、ひとつの強固な PQC セキュリティループへと統合しました。いま私たちは、開発者、企業、そしてすべてのユーザーに提案します。最も安全な基盤の上で、揺るぎない未来をともに設計してください。

Quantarium は到来する未来を待つのではありません。私たちは、その未来を耐え抜くための準備をすでに整えています。

レガシーチェーンと Quantarium の生存曲線　Structural Resilience Across Q-Day



事後のアップグレードはそれ以前の区間を救済できない。差は Q-Day 以降ではなく、ジェネシスの時点ですでに決まっている。

13. 参考文献(References)

本ホワイトペーパーに記載された Quantarium のセキュリティ・アーキテクチャ、耐量子暗号標準、ならびにコンセンサス・アルゴリズムは、以下の国際標準、学術論文、および技術報告書に基づいて設計されています。

1. National Institute of Standards and Technology (NIST). (2016–2024). *Post-Quantum Cryptography Standardization. U.S. Department of Commerce.*
2. National Institute of Standards and Technology (NIST). (2024). *FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA). U.S. Department of Commerce.*
3. Bernstein, D. J., Hülsing, A., et al. (2019). *SPHINCS+: Submission to the NIST Post-Quantum Cryptography Project.*
4. European Telecommunications Standards Institute (ETSI). *ETSI GR QSC 013: Quantum-Safe Cryptography; Threat Assessment.*
5. Mosca, M. (2018). *Cybersecurity in an Era with Quantum Computers. IEEE Security & Privacy.*
6. Shor, P. W. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS).*
7. Grover, L. K. (1996). *A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC).*
8. Barker, E. *Digital Signature Standard (DSS). NIST FIPS 186-5. National Institute of Standards and Technology.*
9. Kahn Academy / IBM Research. *Quantum Computing and Cryptography Overview.*
10. European Union Agency for Cybersecurity (ENISA). (2021). *Post-Quantum Cryptography : Current State and Quantum Mitigation.*
11. National Security Agency (NSA). (2022). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).*
12. ISO/IEC JTC 1/SC 27. *IT Security Techniques – Cryptographic Algorithms. International Organization for Standardization.*
13. Buterin, V. *On Public and Private Blockchains. Ethereum Research.*
14. Wood, G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper.*
15. BFT Consensus Research. *Authority-based Consensus Mechanisms in Permissioned Blockchains.*