MISAKA NETWORK

ポスト量子ネイティブ・プライバシーブロックチェーン

ホ　ワ　イ　ト　ペ　ー　パ　ー

Version 1.0 · 2025 年

ティッカー: **MISAKA**

https://github.com/MISAKA-BTC/Quantum-MISAKA

本文書は情報提供のみを目的としており、金融アドバイス、有価証券の売り出し、または投資勧誘を構成するものではありません。暗号資産への投資には重大なリスクが伴います。

要旨（Abstract）

Misaka Network は、量子コンピュータによる攻撃に対して設計段階から耐性を持つ Layer-1 プライバシーブロックチェーンです。Monero や Zcash をはじめとする既存のプライバシー暗号資産は楕円曲線暗号（ECC）に依存していますが、これは将来の量子コンピュータによって解読される可能性が指摘されています。Misaka は米国国立標準技術研究所（NIST）のポスト量子暗号標準をプロトコルのすべての層に採用することで、この根本的な問題を解決します。

ネットワークは Seraphis スタイルのトランザクションモデルと Jamtis ステルスアドレッシングを実装し、ポスト量子格子リング署名（LaRRS）と秘匿コミットメントを通じて、送信者・受信者・取引金額の無条件プライバシーを提供します。軽量プルーニングノードアーキテクチャにより、モバイルウォレットや低スペックバリデータが完全なトランザクション履歴を保存することなくネットワークに参加できます。

MISAKA トークンは、確立された DeFi 流動性インフラを活用するため Solana ブロックチェーン上で初期発行され、メインネットローンチ時に Misakanetwork へのブリッジが提供される予定です。Misaka はすべてのネットワークトランザクションのガストークン、バリデータ参加のステーキング資産、オンチェーンガバナンスの投票手段として機能します。

※solana 上の Misaka を MISAKA とし、将来の MISAKAnetwork トークンを stMISAKA と定義する。

1 はじめに

暗号技術の歴史は、絶え間ない技術的な攻防の連続です。各世代のセキュリティプリミティブはやがて数学とコンピューティングの進歩に屈してきました。量子コンピューティングの出現は、このパターンにおける質的な変化を意味します。それは緩やかなセキュリティの侵食ではなく、突然の断絶です。

1994 年に発表された Shor のアルゴリズムは、十分に大きな量子コンピュータが多項式時間で大きな整数の因数分解と離散対数問題を解けることを示しています。これらはほぼすべての現代公開鍵暗号—楕円曲線方式を含む—が依拠している数学的問題です。NISBT は暗号学的に関連する量子コンピュータが 10〜15 年以内に実用化される可能性があると推定しています。

プライバシーブロックチェーンは、この脆弱性において特別な立場に置かれています。そのセキュリティ保証は永続的かつ歴史的です。今日ブロードキャストされたトランザクションは、今だけでなく数十年後も秘匿されていなければなりません。今日暗号化されたブロックチェーンデータを収集し、2035 年に量子コンピュータで復号する攻撃者は、そのチェーンで取引をしたすべてのユーザーのプライバシーを遡って破ることができます。この「今収集して後で復号する（harvest now, decrypt later）」脅威モデルは、プライバシーチェーンに対して特別な深刻度をもって適用されます。

Misaka Network はこの脆弱性を根底から解決します。NISBT が標準化したポスト量子暗号プリミティブをネイティブの署名・鍵交換メカニズムとして採用することで、Misaka は量子の脅威に対して耐久性のあるプライバシー保証を提供します。これは後付けや第 2 層の回避策ではありません。量子耐性を第一級の要件として設計されたクリーンスレートな設計です。

2 問題提起

2.1 既存プライバシーチェーンへの量子の脅威

現在運用中のすべての主要プライバシーブロックチェーンは楕円曲線暗号（ECC）に依存しています。

- Monero: 支払い認証に Ed25519、ステルスアドレス導出に Curve25519 を使用。リング秘匿トランザクション（RingCT）は EC ベースの Pedersen コミットメントと Bulletproofs で構築されています。
- Zcash: zk-SNARK 構造（Groth16）に BLS12-381 楕円曲線を使用。Sapling および Orchard プロトコルは EC グループに深く依存しています。
- Beam、Grin、その他の MimbleWimble 実装: 楕円曲線上の Pedersen コミットメントを使用。

Shor のアルゴリズムを大規模に実行できる量子コンピュータが利用可能になると、これらのチェーンは 2 つの異なる障害モードに直面します。

- 前方秘匿性の喪失: 鍵ペアを偽造できるため、将来のトランザクションをプライベートに保つことができません。
- 歴史的な匿名性解除: アーカイブされたブロックチェーンデータ（リングメンバーセット、キーイメージ、ステルス出力を含む）を遡及的に分析してトランザクションを連結し、ユーザーを特定できます。

第 2 の障害モードはプライバシーコインにとって特に深刻です。鍵をローテーションして新しい認証情報を発行できる銀行システムとは異なり、ブロックチェーンのトランザクショングラフは永続的かつ公開されています。これまでに行われたすべてのトランザクションが分析のために永続的に利用可能なまま残ります。

2.2 既存プライバシーチェーンのユーザビリティのギャップ

量子の脆弱性を超えて、既存のプライバシーチェーンは重大なユーザビリティの欠陥を抱えています。

- Monero のフルノードは 170 GB 以上のブロックチェーンデータのダウンロードが必要で、モバイルユーザーには現実的ではありません。
- Zcash のシールドトランザクションは相当な証明時間とメモリを要求し、モバイルウォレットのサポートを制限しています。
- どちらのチェーンも、新しい脅威への対応として暗号プリミティブをアップグレードできるガバナンスメカニズムを提供していません。

Misaka はこの両面に対処します。格子暗号リング署名と秘匿コミットメントによる量子耐性プライバシーと、真のモバイル参加を可能にする軽量アーキテクチャを同時に実現します。

3 提案するソリューション：Misaka Network

Misaka Network は、以下のすべてを同時に達成する目的で構築された Layer-1 ブロックチェーンです。

特性	Misaka のアプローチ
ポスト量子セキュリティ	Falcon-512 署名と Kyber-768 鍵交換をプロトコル全体で採用—ECC はどこにも存在しない
送信者の匿名性	ポスト量子格子リング署名（LaRRS）がどの UTXO が使用されているかを隠す
受信者の匿名性	Jamtis ステルスアドレスがトランザクションごとに使い捨て受信アドレスを生成
金額のプライバシー	格子ベースの Pedersen コミットメントがゼロ知識残高証明で取引金額を秘匿
軽量ノード	プルーニングされたバリデータは最近のブロックと UTXO セットのみを保存; モバイルライトノードはヘッダーのみを同期
確定的ファイナリティ	Tendermint-style BFT コンセンサスが 1 分以内（60 秒ブロック時間）のシングルブロックファイナリティを提供
動的ブロックサイズ	ターゲット 6 MB / 最大 24 MB；中央値ベースの二乗報酬ペナルティでブロック肥大化を抑制
PQ バッチ検証	Falcon および LaRRS 証明をまとめてバッチ検証し、逐次検証比で CPU コストを 40〜60%削減
スループット	ベースライン〜8.8 TPS；バッチ検証有効時〜12〜15 TPS
ガバナンスによるアップグレード	Cardano にインスパイアされたオンチェーンガバナンスにより、バリデータ投票で暗号パラメータを更新可能

重要なのは、Misaka は ECC ベースの既存設計に量子耐性を後付けしていないことです。格子暗号は基盤的なものです。トランザクションモデル、鍵階層、アドレス方式、リング署名、コンセンサス投票のすべてがポスト量子プリミティブをネイティブに使用しています。

4 コア設計原則

4.1 デフォルトでプライバシー

Misaka では、プライバシーはオプトインの機能ではありません。すべてのトランザクションは構造的にプライベートです。透明なアドレスやシールドされていない UTXO は存在しません。この設計により、プライバシー機能がオプションである場合に生じるメタデータの漏洩が排除されます。プライバシーを選択したユーザーとそうでないユーザーをオブザーバーが区別できなくなります。

4.2 量子ネイティブ（後付けではない）

ポスト量子暗号は Misaka スタックの上に重ねられているのではなく、スタックそのものです。ウォレット鍵階層、トランザクション署名メカニズム、P2P ハンドシェイク、ガバナンス投票署名のすべてが Falcon-512 または Kyber-768 を使用しています。これは、PQ 署名をオプション機能として既存の ECC ベースチェーンに追加するという提案とは根本的に異なります。

4.3 軽量な参加

Misaka アーキテクチャはネットワークのストレージ義務を分離します。オペレーター管理のアーカイブノードが完全なトランザクション履歴を保存する一方、バリデータノードとライトノードはプルーニングされたデータセットで動作します。バリデータに必要なのは 4 GB の RAM とコンシューマーSSD のみです。モバイルライトノードに必要なストレージは 200 MB 未満です。この設計により、ハードウェア要件による参加の制限を排除します。

4.4 インフレなし

Misaka のトークン供給量はジェネシス時に固定されます。ブロック報酬による新規トークンは発行されません。バリデータとアーカイブノードへの報酬は、各ブロック内で再分配されるトランザクション手数料のみから生まれます。この「手数料リサイクル」モデルにより、時間の経過とともにトークン保有者が希薄化されることがなく、バリデータの収入がネットワーク利用量と自然に比例します。

4.5 ガバナンスによるアップグレード可能性

暗号標準は進化します。2025 年のポスト量子状況が 2035 年に最適な構成であるとは限りません。

Cardano の Constitutional Committee モデルにインスパイアされたオンチェーンガバナンスシステムにより、ネットワークは暗号パラメータの変更、バリデータセットのローテーション、プロトコルアップグレードについて投票できます。ガバナンス投票は Falcon-512 署名を使用してキャストされ、ステークされた残高によって重み付けされます。

5 ネットワークアーキテクチャ概要

Misaka のネットワークは、階層化されたストレージ階層に配置された 3 つのノードタイプで構成されています。各層には明確に定義されたハードウェアプロファイルと責任範囲があります。

	ライトノード	バリデータノード	アーカイブノード
目的	ウォレット/ユーザー	ブロック生成	完全履歴
RAM	128〜512 MB	4 GB	16 GB 以上
ストレージ	50〜200 MB	50〜200 GB SSD	2 TB 以上 NVMe
ブロックヘッダー	全件	全件	全件
完全 UTXO セット	自身の出力のみ	完全	完全
トランザクション証明	なし	最近分のみ（プルーニング）	完全
リング証明	なし	検証後プルーニング	完全
BFT コンセンサス	なし	あり	オブザーバー
ガバナンス投票	なし	あり（ステーク加重）	あり（CC 役割）

5.1 アーカイブノードと分散化

アーカイブノードはネットワークの長期記憶です。すべてのトランザクション証明、リングメンバーシップ証明、秘匿残高証明を保存しますが、送信者の身元は暗号的に隠されているため、アーカイブオペレーターですらユーザーのプライバシーを侵害できません。プロトコルはメインネットで少なくとも 3 つの独立したアーカイブオペレーターを要求します。新規ノードはアーカイブノードから UTXO スナップショットを受け取り、BFT 確定済みブロックヘッダーチェーンと照合して検証することでブートストラップします。

5.2 P2P ネットワーク

ノード間通信は TCP/TLS 1.3 上の libp2p を使用します。ピア探索はハードコードされたアーカイブノードブートストラップアドレスをシードとする Kademlia DHT を採用します。すべての P2P メッセージは、鍵合意ステップに Kyber-768 を使用した Noise XX ハンドシェイクで暗号化され、最初の接続からポスト量子安全なトランスポートを提供します。

6 プライバシーモデル

6.1 Seraphis トランザクションモデル

Misaka は Seraphis スタイルのトランザクションアーキテクチャを実装しています。Seraphis モデルでは、トランザクションはコミットメントを金額に結びつけ、使い捨てステルスアドレスと組み合わせる enote（暗号化ノート）を使用して構築されます。トランザクションは、実際の送信者であるメンバーを明かすことなく、可能な支払者のリング内のメンバーシップを証明します。

この抽象化は、支払い証明（誰が使用できるか）と宛先証明（誰が受け取るか）の間に明確な分離を提供し、以前の UTXO+リング署名設計よりも柔軟なトランザクション構築を可能にします。

6.2 Jamtis ステルスアドレッシング

Misaka は Jamtis アドレス方式をポスト量子鍵プリミティブに適応したものを採用しています。Jamtis アドレスは、プライバシー階層において異なる機能を果たす複数の鍵をエンコードします。

- 使用鍵コンポーネント（K_1）：使用を認証する Falcon-512 鍵ハッシュ
- ビュー鍵コンポーネント（K_2）：受信トランザクションをスキャンするために使用する Kyber-768 鍵ハッシュ
- アドレスタグブラインディング鍵（K_3）：ビュー鍵なしに複数のアドレスを同じウォレットに結びつけることを防止

送信者がトランザクションを構築する際、エフェメラル Kyber-768 鍵カプセル化を使用して受信者の使い捨てステルスアドレスを導出します。受信者はビュー鍵を使用してブロックチェーンをスキャンします。1 バイトの「ビュータグ」プレフィックスにより高速スキャンが可能です。受信者はビュータグが一致する出力の一部分にのみ Kyber 完全復号を実行すればよく、モバイル同期が実用的になります。

6.3 ポスト量子リング署名

どの UTXO が使用されているかを隠す暗号メカニズムであるリングメンバーシップ証明は、Module-LWE 上に構築された LaRRS（格子リング署名方式）を使用します。各トランザクション入力について、送信者は UTXO セットから 11〜16 の UTXO のリングを選択し、どれかを明かすことなく、ちょうど 1 つのリングメンバーの使用鍵の知識を証明します。

二重使用を防止するために、使用鍵から決定論的に導出される値であるリンクタグが各入力に含ま

れます。これは Monero のデザインにおけるキーイメージに類似していますが、格子構造上で計算されます。

6.4 秘匿トランザクション

トランザクション金額は格子ベースの Pedersen コミットメントを使用して隠されます。コミットメント C = v·G + r·H は、格子ジェネレータ G と H を使用して、値 v をランダムブラインディング係数 r で結びつけます。ネットワークは個々の金額を学ぶことなく、入力コミットメントの合計が出力コミットメントの合計と手数料コミットメントに等しいことを検証します。格子ベースのレンジ証明により、各出力コミットメントが有効範囲[0, 2^{64})内の非負値をエンコードしていることを保証します。

7 ポスト量子暗号

7.1 なぜ格子暗号なのか

Misaka のポスト量子セキュリティは、格子問題の困難性に基づいています。具体的には、LWE（Learning With Errors）、RLWE（Ring-LWE）、SIS（Short Integer Solution）問題です。これらの問題は、量子コンピュータに対しても困難であると考えられています。なぜなら、これらを解く多項式時間の量子アルゴリズムは知られておらず、最もよく知られた量子攻撃は古典的なアルゴリズムと比べてわずかな改善しか提供しないからです。

格子暗号は、他のポスト量子ファミリー（ハッシュベース、コードベース、アイソジェニーベース）に対して、パフォーマンス、鍵サイズ、汎用性の最良の組み合わせを提供するため選択されました。格子スキームは、同じ数学的基盤から署名、鍵カプセル化、ゼロ知識証明をインスタンス化できます。

7.2 プリミティブの選択

プリミティブ	アルゴリズム	用途
署名	Falcon-512（NIST FIPS 206）	ブロック署名、BFT 投票、ガバナンス投票、ウォレット使用認証
鍵交換	Kyber-768（NIST FIPS 203）	P2P トランスポート、ステルスアドレス KEM、メモ暗号化
ハッシュ	SHA3-256	ブロックハッシュ、TX ID、マークルツリー、鍵導出
DRBG	SHAKE256-DRBG（SP 800-90A）	すべての乱数生成—AES-CTR-DRBG を置き換え
リング署名	LaRRS（Module-LWE）	トランザクション送信者の匿名性
コミットメント	格子 Pedersen	金額秘匿と残高証明

7.3 量子安全な乱数生成（DRBG）

AES ベースの DRBG（CTR-DRBG）は Grover アルゴリズムに脆弱であり、有効鍵長を半分に削減します—128 ビット AES セキュリティが 64 ビットポスト量子セキュリティに低下します。Misaka は全体を通して SHAKE256-DRBG を使用し、量子アルゴリズムが利用できる代数的構造を持ちません。そのセキュリティは SHA3 の衝突耐性に完全に還元されます。

すべての Falcon-512 署名操作は、各署名呼び出しの前に状態がアトミックに永続化される SHAKE256-DRBG インスタンスから新鮮な乱数を取得します。Falcon におけるノンスの再利用は壊滅的（秘密鍵が漏洩）であり、この永続化要件は非交渉的です。

7.4 セキュリティレベル

Misaka のすべての暗号プリミティブは少なくとも 128 ビットのポスト量子セキュリティを目標とし、NIST セキュリティカテゴリ I またはそれ以上に対応します。Kyber-768 は 164 ビットのポスト量子セキュリティ（NIST カテゴリ III）を提供し、将来の Module-LWE に対する暗号解析の進展を吸収するための最小値を大きく上回るセキュリティマージンを提供します。

8 トークンユーティリティ：MISAKA（MSK）

stMISAKA トークンは Misaka Network のネイティブ資産です。ネットワーク運営に不可欠な 3 つのコアユーティリティ機能を果たします。

機能	説明
取引手数料	Misaka Network のすべてのトランザクションはガストークンとして stMISAKA で手数料を支払います。すべての TX に 2,000 stMISAKA の固定最低手数料が課され、さらに 0.01 stMISAKA × バイト数 × 混雑係数のサイズ手数料が上乗せされます。典型的な 100 KB TX の手数料は 3,024 stMISAKA
バリデータステーキング	バリデータはネットワーク検証に参加するために Misaka を経済的ステークとしてロックします。報酬はステーク残高に比例して分配されます。
アーカイブノード報酬	ブートストラップ、履歴保存、エクスプローラーサービスを提供するアーカイブノードは、**手数料の 20%**を継続的に受け取ります。
ガバナンス投票	バリデータは Falcon-512 コンセンサス鍵を使用して、プロトコル変更、バリデータセット変更、憲法改正についてステーク加重のガバナンス投票を行います。
ガバナンスデポジット	ガバナンス提案を提出するには stMISAKA をデポジットとしてロックする必要があります。デポジットは批准されると返却され、否決されると没収され、スパム提案を防止します。

8.1 トークンローンチ戦略：Solana 優先

エコシステムの成長と流動性を加速するために、Misaka はまず Solana SPL トークンとして発行されています。Solana の DEX、流動性プール、ウォレット統合を含む成熟した DeFi インフラにより、Misaka ネットワークが完全に稼働する前から即座の市場アクセスが提供されてます。

Misaka ネットワークのメインネットローンチ後、双方向ブリッジにより Misaka 保有者は Solana と stMISAKA の間でトークンを移動できるようになります。ブリッジはロックアンドミントメカニズムを使用します。Solana SPL トークンはスマートコントラクトにロックされ、同等の Misaka(solana)が Misaka チェーン上にミントされます。償還はその逆の順序で行われます。

> *ブリッジ設計は中央集権的なリレーヤーを信頼することなく、Solana トランザクションのファイナリティを検証するために ZK 証明を使用します。ZK 検証回路はメインネットブリッジ有効化前に監査されます。*

9 トークノミクス

9.1 供給パラメータ

パラメータ	値
トークン名	Misaka
ティッカー	MISAKA
総供給量	ジェネシス時に固定—追加発行なし
小数点以下桁数	9 桁（最小単位: 0.000000001 Misaka）
トークン規格（初期）	Solana SPL
トークン規格（ネイティブ）	Misaka Network Layer-1 コイン
新規トークン発行	なし—供給量は厳密に固定

※solana 上の Misaka を MISAKA とし、将来の MISAKAnetwork トークンを stMISAKA と定義する。

9.2 手数料と報酬の構造

Misaka は手数料リサイクル経済モデルを採用しています。ブロックごとに新規トークンは作成されません。バリデータとノードへのすべての報酬はユーザーが支払うトランザクション手数料から生まれます。

手数料タイプ	計算式	備考
最低手数料	2,000 stMISAKA（固定）	すべての TX に適用されるベースコスト。PQ 証明のオーバーヘッドを反映
Tx サイズ手数料	0.01 stMISAKA × バイト数 × 混雑係数	最低手数料に加算される
混雑係数	ブロック使用量 < 50% → 1.0 50〜70% → 2.0 70〜85% → 3.0 85〜95% → 4.0 95〜100% → 5.0	ネットワーク混雑時に手数料を自動調整
典型的な 100 KB TX	3,024 stMISAKA	2,000 + (0.01 × 102,400 バイト × 1.0) ; 混雑係数=1.0

※solana 上の Misaka を MISAKA とし、将来の MISAKAnetwork トークンを stMISAKA と定義する。

9.3 報酬分配

受取先	配分	根拠
バリデータノード	手数料の 80%	ブロック生成、リング署名検証、BFT コンセンサス
アーカイブノード	手数料の 20%	履歴保存、ブートストラップ、エクスプローラー
財団	端数＋基本オーバーヘッド	プロトコル保守とガバナンスインフラ

バリデータプール内では、ブロック生成時の各バリデータのステークされた MISAKA に比例して報酬が分配されます。ブロック提案者には追加ボーナスはなく、利己的なマイニングインセンティブを排除します。

9.4 反インフレ設計

ゼロ発行モデルは MISAKA の通貨供給量が永続的に固定されることを意味します。ネットワーク利用が増えるにつれて、バリデータは新規発行の希薄化効果なしに手数料の絶対額でより多くを獲得します。この設計は Bitcoin の供給モデルをプルーフオブステーク・プライバシー保護の文脈に適用したものです。

10 ロードマップ

フェーズ	時期	マイルストーン
Phase 1（進行中）	2026 Q1–Q2	Ed25519 → Falcon-512 への置き換え（liboqs バインディング）· X25519 → Kyber-768 への移行 · SHA-256 → SHA3-256 · SHAKE256-DRBG · devnet での PQ 統合テスト
Phase 2（予定）	2026 Q1–Q2	格子 Pedersen コミットメント · LaRRS リング署名統合（リングサイズ 11〜16）· Jamtis ステルスアドレスウォレットスキャン · レンジ証明 · プライバシーtestnet ローンチ
Phase 3（予定）	2026 Q2–Q3	Cardano スタイルガバナンスシステム · ステーク加重投票 · 手数料再分配（75/25）· アーカイブノードインセンティブプログラム · ガバナンストランザクション実装
Phase 4（予定）	2026 Q3 以降	独立セキュリティ監査（格子暗号専門家）· iOS/Android モバイルウォレット · CoinGecko/CoinMarketCap リスティング · 独立アーカイブオペレーター3 社以上 · メインネットジェネシスブロック

11 ノードアーキテクチャ

11.1 ライトノード

ライトノードはモバイルウォレットとエンドユーザーアプリケーション向けに設計されています。ブロックヘッダーと自身のウォレット鍵に関連する UTXO のサブセットのみをダウンロードします。トランザクション証明、リングメンバーシップ証明、秘匿残高証明は保存しません。ライトノードの同期は Jamtis アドレス方式のビュータグスキャン最適化を使用します—出力の約 99%を 1 バイトの比較で拒否できるため、低速接続でもモバイル同期が実用的になります。

11.2 バリデータノード

バリデータノードは BFT コンセンサスに参加し、処理するすべてのブロックのすべてのトランザクションを検証します。構造チェック、リンクタグの一意性、UTXO リングメンバーシップ、LaRRS リング署名検証、秘匿残高証明検証、レンジ証明検証、手数料適切性の完全な検証パイプラインを実行します。ブロックが BFT ファイナリティを達成した後、バリデータはローカルストレージからトランザクション証明をプルーニングし、UTXO セットとリンクタグセットのみを保持できます。

11.3 アーカイブノード

アーカイブノードはネットワークの組織的な記憶です。すべてのリング証明と秘匿証明を含む完全なブロックチェーン履歴を保持します。ブートストラップするノードに UTXO スナップショットを提供し、ブロックチェーンエクスプローラーAPI を提供し、チェーン監査をサポートします。アーカイブ運用には 16 GB 以上の RAM と 2 TB 以上の NVMe ストレージが必要です。プロトコルはメインネットで少なくとも 3 つの独立したアーカイブオペレーターを義務付け、単一オペレーターが新しいノードのブートストラップを検閲することを防止します。

12 コンセンサスメカニズム

Misaka はバリデータセットとして Tendermint-style PBFT コンセンサスアルゴリズムを使用し、バリデータ数は 10〜30 台です。PQ 証明を含むプライバシー保護トランザクションの検証は計算コストが高く、少数の説明責任のあるバリデータがより速いファイナリティを提供し、プライバシー層が主要な信頼境界であるネットワークではセキュリティを損なうことなく機能します。

コンセンサス特性	値
耐障害性	バリデータ f < N/3 まで、ビザンチン耐故障性
ファイナリティタイプ	シングルブロックファイナリティ—コミット後の再編成なし
リーダー選択	Falcon-512 公開鍵ハッシュによるラウンドロビン—このスケールでは VRF 不要の決定論的
投票署名	ブロックハッシュに対する Falcon-512
コミット閾値	[2N/3] + 1 Precommit 投票が必要
ブロック時間	60 秒（1 分）
ラウンドタイムアウト	30s Propose → 30s Prevote → 30s Precommit → 次ラウンド

12.1 動的ブロックサイズ

Misaka は、トランザクション需要に適応しながら不当なブロック生成を抑制する動的ブロックサイズ機構を採用しています。

ブロックサイズパラメータ	値
ターゲットブロックサイズ	6 MB
最大ブロックサイズ	24 MB
調整ウィンドウ	直近 100 ブロックの中央値
超過ペナルティ	現在の中央値を超えるブロックに対して、提案者の報酬を二乗で減額

プロトコルは直近 100 ブロックのブロックサイズ中央値を計算します。ブロック提案者は最大 24 MB までのブロックを生成できますが、現在の中央値を超えるブロックを提案した場合、二乗ペナ

ルティが報酬シェアに適用されます。これにより、正当な需要がある際はバースト容量を活かしつつ、効率的なブロック充填に対する自然な経済的圧力が生まれます。

> *二乗ペナルティ計算式：block_size > median_size の場合、reward_multiplier = (median_size / block_size)²。提案者がダストで水増しするよりも効率的にトランザクションをパックするインセンティブが働きます。*

12.2 TPS 分析

60 秒ブロック時間と動的ブロックサイズを組み合わせた Misaka のスループット試算は以下のとおりです。

スループットパラメータ	値
ブロック時間	60 秒
ターゲットブロックサイズ	6 MB（6,000 KB）
最大ブロックサイズ	24 MB
平均 PQ プライバシーTX サイズ	～120 KB（LaRRS リング証明含む）
ターゲットブロック当たり TX 数	6,000 ÷ 120 = 50 TX
ベースライン TPS（ターゲットブロック）	50 ÷ 60 ≈ 0.83 TPS（保守的）
最大ブロック当たり TX 数	24,000 ÷ 120 = 200 TX
ピーク TPS（最大ブロック）	200 ÷ 60 ≈ 3.3 TPS
バッチ検証あり（+40～60%スループット）	～4.7～5.5 TPS（ピーク）
将来：リングサイズ=4、平均 TX ～40 KB 時	24,000 ÷ 40 = 600 TX → バッチ検証で～15 TPS

> *TPS 数値は完全な PQ リング証明付きプライバシートランザクションに基づきます。より単純な支払いのみのトランザクションは小さく、比例してスループットが向上します。バッチ検証の効果は 50TX 以上を 1 パスで処理する場合に発揮されます。*

12.3 PQ 証明バッチ検証

Misaka における重要なパフォーマンス最適化は、Falcon-512 ブロック署名と LaRRS リング証明のバッチ検証です。標準的な逐次検証ではトランザクション証明を 1 件ずつ処理します。

$$\texttt{verify}(TX_1) \rightarrow \texttt{verify}(TX_2) \rightarrow \texttt{verify}(TX_3) \rightarrow \ldots \rightarrow \texttt{verify}(TX_n)$$

バッチ検証では、ブロック内の全証明の検証式を集約し、1 回の代数演算でまとめてチェックします。

$$\texttt{batch\_verify}(TX_1, TX_2, \ldots, TX_n) \quad - \quad \text{全証明を 1 パスで処理}$$

Falcon-512 では NTRU 格子チェックの線形性を利用したバッチ検証が可能です。LaRRS リング証明では、SHAKE256-DRBG からサンプリングしたバッチごとのチャレンジを用いたランダム線形結合により Module-LWE 検証式を統合でき、行列-ベクトル積の数を O(N)から O(1)に削減します。

バッチ検証特性	詳細
CPU コスト削減	バッチサイズ≧50 TX で逐次検証比 40〜60%削減
セキュリティ劣化	無視できる水準：バッチあたりの健全性誤差 $\leq 2^{-128}$（MLWE 仮定下）
バッチサイズトリガー	ブロックに 10 TX 以上含まれる場合に自動有効化
実装	liboqs バッチ検証 API（Falcon）；カスタム LaRRS バッチモジュール
並列処理	各 CPU コアがバッチのサブセットを処理；自明にマルチスレッド対応

12.4 コンパクトブロック伝播

最大 24 MB のブロックでは、単純なフルブロック伝播は大きなネットワーク遅延を生じさせます。Misaka は Bitcoin の BIP 152 にインスパイアされたコンパクトブロックプロトコルを実装しています。各ノードはブロックが生成される前から、個別のトランザクション（平均 120 KB）をメモリプールで継続的に受信・検証しています。

ブロックがファイナライズされると、提案者は 24 MB のフルブロック本体ではなく、数 KB のコン

パクトブロックアナウンスメント（トランザクション ID インデックス）のみをブロードキャストします。受信ノードはこのインデックスを使ってローカルメモリプールからフルブロックを再構成します。ローカルメモリプールにないトランザクションの小さな割合のみをピアからフェッチすればよいため、実質的なブロック伝播時間はミリ秒単位まで短縮されます。

コンパクトブロック特性	詳細
アナウンスメントサイズ	～3～6 KB（200 TX ブロックの ID インデックス）
フルブロックサイズ	最大 24 MB
実効伝播時間	フルメモリプール保有ノード間ではミリ秒単位
フォールバック	ローカルメモリプールに 5%以上の TX が不足している場合はフルブロックフェッチ
セキュリティ	BFT ファイナリティに変更なし；コンパクトブロックは伝送最適化のみ

12.5 ガバナンス制御によるバリデータローテーション

バリデータセットの変更にはガバナンスアクション（action_type 0x01 または 0x02）が必要です。提案は[2N/3] + 1 の閾値を満たすステーク加重バリデータ投票を通過し、さらにアーカイブガバナンス委員会からの承認を受ける必要があります。批准された変更は次のエポック境界で発効し、エポック途中の不整合を防止します。

13 セキュリティモデル

13.1 暗号セキュリティ前提

プリミティブ	困難問題	セキュリティレベル
Falcon-512	NTRU/Ring-SIS（2 の冪乗次数円分環）	128 ビット PQ（NIST Level I）
Kyber-768	Module-LWE（MLWE）	164 ビット PQ（NIST Level III）
LaRRS	Module-LWE + Module-SIS	128 ビット PQ（推定）
SHAKE256-DRBG	SHA3 衝突耐性	256 ビット出力、≥128 ビット PQ
格子 Pedersen	Short Integer Solution（SIS）	128 ビット PQ（推定）

13.2 脅威モデル

- 古典的な敵対者: すべてのプライバシー保証は Module-LWE 仮定のもとでの計算上の匿名性を提供する古典的なコンピューティング敵対者に対して無条件に成立します。
- 量子の敵対者: Shor または Grover アルゴリズムを実行する量子の敵対者に対してプライバシー保証が成立します。Grover アルゴリズムはハッシュ関数に対して二次高速化を提供しますが、256 ビット出力の SHA3-256 と 256 ビットセキュリティ強度の SHAKE256-DRBG の使用によって緩和されます。
- 「今収集して後で復号する」: Misaka が今日ブロードキャストするトランザクションは、将来量子コンピュータが利用可能になった場合でもプライベートに保たれます。すべてのコミットメントと証明がポスト量子困難問題を使用しているためです。
- アーカイブノードの侵害: アーカイブノードはトランザクショングラフ全体を見ますが、送信者の身元はリング署名によって隠されているため特定できません。受信者の身元はステルスアドレッシングによって隠されます。金額は秘匿コミットメントによって隠されます。

13.3 スラッシングと経済的セキュリティ

Misaka は Cardano の没収なしペナルティモデルを採用しています。ステークスラッシング（没収）は存在しません。バリデータの不正行動は報酬減額とバリデータセットからの除名をもたらします。この設計は、ネットワーク分断やソフトウェアバグが誤って大規模スラッシングを引き起こす可能性がある小規模バリデータセットにおけるステークスラッシングの壊滅的な経済的脆弱性を回避します。

14 今後の開発

14.1 ZK 加速アーカイブ検証

現在の UTXO スナップショット認証は BFT 証明書を信頼のアンカーとして使用しています。将来の拡張として、UTXO セット導出の ZK 簡潔証明を追加し、アーカイブによる不正な代替チェーン提示への強化された数学的保証と、ブロックヘッダーをダウンロードすることなくトラストレスなライトクライアントスナップショット検証を可能にします。

14.2 クロスチェーンプライバシーブリッジ

セクション 8 で説明した Solana ブリッジは、より広範なクロスチェーンビジョンの第一段階です。将来のバージョンでは、ブリッジを他の主要チェーン（Ethereum、Bitcoin）に拡張し、ユーザーがそれらのチェーンから Misaka のプライバシー環境内に資産をシールドできるようにします。すべてのブリッジ証明はポスト量子 ZK 構造を使用し、チェーンの全体的な量子耐性保証を維持します。

14.3 閾値署名ガバナンス

バリデータセットが 16 の上限に近づくにつれて、BFT 投票のナイーブな集約（個別の Falcon-512 署名の送信）は帯域幅のボトルネックになります。将来のプロトコルアップグレードでは格子ベースの閾値署名を導入し、BFT 証明書サイズを O(N × 1281 バイト)から定数サイズの集約証明に削減します。

14.4 スマートコントラクト層

現在の Misaka の設計は UTXO ベースの支払いチェーンです。将来の開発トラックでは、プライバシー保護スマートコントラクト層の追加を検討します。Misaka ステートマシン上の ZK 証明可能な計算を使用し、コアプライバシー保証を損なうことなくプライベート DeFi アプリケーションを可能にする可能性があります。

15 結論

ポスト量子時代への移行は遠い将来の仮定ではありません—それは今日のブロックチェーンプロジェクトが対処しなければならないエンジニアリング上の制約です。なぜならブロックチェーントランザクションは永続的であり、敵対者モデルには将来の量子能力が含まれるからです。プライバシーブロックチェーンは、これまでに行われたすべてのトランザクションが遡及的な分析のために永続的に利用可能なまま残るという点で、特に深刻な形でこのリスクに直面しています。

Misaka Network は、ポスト量子暗号をすべてのプロトコル層の基盤に置くクリーンスレートな設計でこの課題に対処します。NIST 標準化された Falcon-512 と Kyber-768 プリミティブを採用し、格子リング署名と秘匿コミットメントを用いた Seraphis/Jamtis プライバシーモデルを実装し、モバイル参加を可能にする軽量プルーニングノードアーキテクチャで運用することで、Misaka は完全なパッケージを提供します。無条件のプライバシー、量子耐性、そして実用的なユーザビリティです。

MISAKA トークンはこのネットワークの経済的な燃料を提供します。バリデータのインセンティブを整合させ、手数料再分配によりインフラ運用に資金を提供し、プロトコル進化のコミュニティガバナンスを可能にします。Solana 優先の発行戦略により、ネイティブチェーンのメインネットローンチ準備中に即座の流動性アクセスが提供されます。

Misaka は既存のプライバシーチェーンと同じ条件で競争しているのではありません。それらのチェーンが生き残るための装備を持っていないポスト量子時代のために構築しています。

付録 A 技術プロトコル仕様

A.1 ブロックヘッダー構造

すべてのブロックヘッダーは完全なブロック本体にコミットし、信頼の連鎖を確立します。

```
version (u32) · height (u64) · prev_hash ([u8;32]) · timestamp (u64) · tx_merkle_root ([u8;32]) · utxo_root ([u8;32]) · link_tag_root ([u8;32]) · proposer_id ([u8;32]) · proposer_sig ([u8;1281]) · bft_sigs (Vec<BftSig>)
```

A.2 トランザクション構造

```
version (u8) · inputs (Vec<TxInput>) · outputs (Vec<TxOutput>) · ring_proof (PQRingProof) · conf_proof (BalanceProof) · link_tags (Vec<[u8;32]>) · fee_commit ([u8;32]) · tx_extra (Vec<u8>)
```

A.3 PQ リング署名パラメータ（LaRRS）

パラメータ	値	備考
モジュールランク k	3	Kyber と同じモジュール構造
多項式次数 n	256	NTT フレンドリー
法 q	8,380,417	$= 2^{23} - 2^{13} + 1$（素数、NTT フレンドリー）
L2 ノルム境界 β	2^{18}	リジェクションサンプリング境界
リングサイズ N	11〜16	デフォルト 16（最大匿名性）
証明サイズ（N=16）	約 11〜14 KB/入力	リングメンバーごとの応答ベクトル
セキュリティレベル	128 ビット PQ	MLWE 困難性のもとで

A.4 Falcon-512 パラメータ

パラメータ	値	備考
格子次元 n	512	NTRU 2 の冪乗次数円分環
法 q	12,289	NTT フレンドリー素数
署名サイズ	約 666 バイト（圧縮）	1281 バイト（パディング）
公開鍵サイズ	897 バイト	
ガウス幅 σ	≈165	トラップドアサンプラーパラメータ
セキュリティレベル	128 ビット PQ	NIST Level I（FIPS 206）

A.5 鍵導出階層

```
MasterSeed (256 ビット) → [HKDF-SHA3-256] → spend_key (Falcon-512 鍵ペア) → [HKDF-SHA3-256] → view_key (Kyber-768 鍵ペア) → find_received_key + generate_addr_key + unlock_amounts_key
```

A.6 バリデータ検証パイプライン

1. 構造的妥当性—TX 解析、バージョン確認、リングサイズ境界（11〜16）
2. リンクタグの一意性—入力内のタグがグローバルリンクタグセットに存在しないこと
3. UTXO リングメンバーシップ—すべてのリングメンバーが既存の UTXO を参照
4. PQ リング署名—リングコミットメントに対する LaRRS 証明を検証
5. 残高証明—Σ（入力コミットメント）= Σ（出力コミットメント）+ 手数料を検証
6. レンジ証明—各出力コミットメントが非負であることを検証
7. 手数料適切性—手数料コミットメントが最低手数料スケジュール以上の値をデコード
8. トランザクションサイズ—シリアライズサイズ ≤ 200 KB