MISAKA NETWORK

Post-Quantum Native Privacy Blockchain

WHITEPAPER

Version 1.0 · 2026

Ticker: MISAKA

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

This document is provided for informational purposes only and does not constitute financial advice, an offer to sell securities, or a solicitation to buy. Cryptocurrency investments carry risk.

Abstract

Misaka Network is a Layer-1 privacy blockchain engineered from the ground up to be resistant to quantum computing attacks. While existing privacy-focused cryptocurrencies such as Monero and Zcash rely on elliptic-curve cryptography — a mathematical foundation that will be broken by sufficiently powerful quantum computers — Misaka adopts the National Institute of Standards and Technology (NIST) post-quantum cryptography standards throughout every layer of its protocol.

The network implements a Seraphis-style transaction model with Jamtis stealth addressing, post-quantum lattice ring signatures (LaRRS), and confidential commitments to provide unconditional privacy for senders, receivers, and transaction amounts. A lightweight pruned-node architecture enables mobile wallets and low-resource validators to participate without storing the full transaction history.

The MISAKA token is initially issued on the Solana blockchain to leverage its established DeFi liquidity infrastructure. Upon mainnet launch, a bridge will allow holders to convert between Solana MISAKA and the native Layer-1 stMISAKA coin. MISAKA serves as the gas token, staking asset, and governance instrument for the network.

Terminology: MISAKA refers to the Solana SPL token currently in circulation. stMISAKA refers to the future native Layer-1 coin on the Misaka Network mainnet. The bridge converts MISAKA ↔ stMISAKA at a fixed 1:1 ratio.

1 Introduction

The history of cryptography is one of continuous arms races. Each generation of security primitives has eventually yielded to advances in mathematics and computing. The advent of quantum computing represents a categorical shift in this pattern: not a gradual erosion of security, but a sudden discontinuity.

Shor's algorithm, published in 1994, demonstrates that a sufficiently large quantum computer can factor large integers and solve the discrete logarithm problem in polynomial time. These are precisely the mathematical problems upon which nearly all modern public-key cryptography — including all elliptic curve schemes — rests. NIST estimates that cryptographically relevant quantum computers may become operational within 10 to 15 years.

Privacy blockchains occupy a unique position of vulnerability. Their security guarantee is permanent and historical: a transaction broadcast today must remain private not only now but decades into the future. An attacker who harvests encrypted blockchain data today and decrypts it with a quantum computer in 2035 will have retroactively broken the privacy of every user who ever transacted on that chain. This “harvest now, decrypt later” threat model applies with particular severity to privacy chains.

Misaka Network addresses this vulnerability at the foundation. By adopting NIST-standardised post-quantum cryptographic primitives as its native signature and key-exchange mechanisms, Misaka provides privacy guarantees that are durable against the quantum threat. It is not a retrofit or a layer-two workaround; it is a clean-slate design with quantum resistance as a first-class requirement.

2 Problem Statement

2.1 The Quantum Threat to Existing Privacy Chains

Every major privacy blockchain in production today relies on elliptic-curve cryptography (ECC):

- Monero uses Ed25519 for spend authorisation and Curve25519 for stealth address derivation. Its ring confidential transactions (RingCT) are built on EC-based Pedersen commitments and Bulletproofs.
- Zcash uses BLS12-381 elliptic curves for its zk-SNARK construction (Groth16). Its Sapling/Orchard protocols are deeply dependent on EC groups.
- Beam, Grin, and other MimbleWimble implementations use Pedersen commitments over elliptic curves.

When a quantum computer capable of running Shor's algorithm at scale becomes available, these chains face two distinct failure modes:

- Forward secrecy failure: Future transactions cannot be kept private, because key pairs can be forged.
- Historical deanonymisation: Archived blockchain data — including ring member sets, key images, and stealth outputs — can be retroactively analysed to link transactions and identify users.

The second failure mode is particularly insidious for privacy coins. Unlike a banking system that can rotate keys and issue new credentials, a blockchain's transaction graph is permanent and public. Every transaction ever made remains available for analysis.

2.2 The Usability Gap in Existing Privacy Chains

Beyond the quantum vulnerability, existing privacy chains suffer from significant usability deficiencies:

- Monero's full node requires downloading over 170 GB of blockchain data — impractical for mobile users.
- Zcash's shielded transactions require substantial proving time and memory, limiting mobile wallet support.
- Neither chain offers governance mechanisms that allow the community to upgrade cryptographic primitives in response to new threats.

Misaka addresses both dimensions: it provides quantum-resistant privacy with a lightweight architecture that enables genuine mobile participation.

3 Proposed Solution: Misaka Network

Misaka Network is a purpose-built Layer-1 blockchain that achieves the following simultaneously:

Property	Misaka's Approach
Post-quantum security	Falcon-512 signatures and Kyber-768 key exchange throughout — no ECC anywhere
Sender anonymity	Post-quantum lattice ring signatures (LaRRS) hide which UTXO is being spent
Receiver anonymity	Jamtis stealth addresses generate one-time receive addresses per transaction
Amount privacy	Lattice-based Pedersen commitments hide transaction values with zero-knowledge balance proofs
Lightweight nodes	Pruned validators store only recent blocks and the UTXO set; mobile light nodes sync headers only
Deterministic finality	Tendermint-style BFT consensus provides single-block finality within 1 minute (60-second block time)
Dynamic block size	Target 6 MB / maximum 24 MB; median-based quadratic reward penalty prevents bloat
PQ batch verification	Falcon and LaRRS proofs batch-verified in groups, cutting CPU cost 40–60% vs per-TX verification
Throughput	~8.8 TPS baseline; ~12–15 TPS with batch verification enabled
Governed upgrades	Cardano-inspired on-chain governance allows cryptographic parameter updates by validator vote

Critically, Misaka does not retrofit quantum resistance onto an existing ECC-based design. The lattice cryptography is foundational: the transaction model, key hierarchy, address scheme, ring signatures, and consensus voting all use post-quantum primitives natively.

4 Core Design Principles

4.1 Privacy by Default

On Misaka, privacy is not an opt-in feature. Every transaction is private by construction. There are no transparent addresses or unshielded UTXOs. This design eliminates the metadata leakage that occurs when privacy features are optional — observers cannot distinguish “this user chose privacy” from “this user did not”.

4.2 Quantum-Native, Not Quantum-Retrofitted

Post-quantum cryptography is not layered on top of the Misaka stack — it is the stack. The wallet key hierarchy, transaction signing, P2P handshake, and governance vote signatures all use Falcon-512 or Kyber-768. This differs fundamentally from proposals to add PQ signatures as optional features to existing ECC-based chains.

4.3 Lightweight Participation

The Misaka architecture separates the network's storage obligations. Operator-managed Archive Nodes store the complete transaction history, while Validator Nodes and Light Nodes operate on pruned datasets. A validator requires only 4 GB of RAM and a consumer SSD. A mobile light node requires less than 200 MB of storage.

4.4 No Inflation

Misaka's token supply is fixed at genesis. No new tokens are created through block rewards. Validator and Archive Node compensation comes entirely from transaction fees redistributed within each block. This fee-recycling model ensures that token holders are not diluted over time, and that validator income scales naturally with network usage.

4.5 Governed Upgradability

Cryptographic standards evolve. The post-quantum landscape of today may not be the optimal configuration in 2035. Misaka's Cardano-inspired Constitutional Committee governance model allows the network to vote on cryptographic parameter changes, validator set rotations, and protocol upgrades. Governance votes are cast using Falcon-512 signatures and are weighted by staked MISAKA balance.

5 Network Architecture Overview

Misaka's network is composed of three node types arranged in a layered storage hierarchy. Each layer has a clearly defined hardware profile and responsibility scope.

	Light Node	Validator Node	Archive Node
Purpose	Wallet / user	Block production	Full history
RAM	128–512 MB	4 GB	16+ GB
Storage	50–200 MB	50–200 GB SSD	2+ TB NVMe
Block headers	All	All	All
Full UTXO set	Owned only	Complete	Complete
Transaction proofs	None	Recent (pruned)	Complete
Ring proofs	None	Verifies then prunes	Complete
BFT consensus	No	Yes	Observer
Governance vote	No	Yes (stake-weighted)	Yes (CC role)

5.1 Archive Nodes and Decentralisation

Archive Nodes are the network's long-term memory. They store every transaction proof and ring membership proof — but they cannot break user privacy, because sender identity is cryptographically hidden even from archive operators. The protocol requires at least three independent archive operators on mainnet. New nodes bootstrap by receiving a UTXO snapshot from an Archive Node and verifying it against the BFT-finalised block header chain.

5.2 P2P Network

Node communication uses libp2p over TCP/TLS 1.3. Peer discovery employs Kademlia DHT seeded by hardcoded Archive Node bootstrap addresses. All P2P messages are encrypted using a Noise XX handshake with Kyber-768 for the key agreement step, providing post-quantum secure transport from the first connection.

6 Privacy Model

6.1 Seraphis Transaction Model

Misaka implements a Seraphis-style transaction architecture. Transactions are constructed using enotes (encrypted notes) that bind a commitment to an amount with a one-time stealth address. The transaction proves membership in a ring of possible spenders without revealing which member is the actual sender.

This abstraction provides a clean separation between the spending proof (who can spend) and the destination proof (who receives), enabling more flexible transaction construction than earlier UTXO-with-ring-signature designs.

6.2 Jamtis Stealth Addressing

Misaka adopts the Jamtis address scheme, adapted for post-quantum key primitives. A Jamtis address encodes multiple keys that serve different functions in the privacy hierarchy:

- Spend key component (K1): the Falcon-512 key hash that authorises spending
- View key component (K2): the Kyber-768 key hash used to scan for incoming transactions
- Address tag-blinding key (K3): prevents linking multiple addresses to the same wallet without the view key

When a sender constructs a transaction, they derive a one-time stealth address for the recipient using an ephemeral Kyber-768 key encapsulation. A one-byte “view tag” prefix allows rapid scanning — approximately 99% of outputs can be rejected with a single byte comparison, making mobile sync practical even over slow connections.

6.3 Post-Quantum Ring Signatures

The ring membership proof uses LaRRS (Lattice Ring Signature Scheme), a construction built on Module-LWE. For each transaction input, the sender selects a ring of 11 to 16 UTXOs from the UTXO set and generates a proof demonstrating knowledge of the spending key for exactly one ring member, without revealing which. A link tag — a deterministic value derived from the spend key — is included with each input to prevent double-spending.

6.4 Confidential Transactions

Transaction amounts are hidden using lattice-based Pedersen commitments. The network verifies that the sum of input commitments equals the sum of output commitments plus the fee commitment — without learning any individual amount. Lattice-based range proofs ensure each output commitment encodes a non-negative value within [0, 2^{64}).

7 Post-Quantum Cryptography

7.1 Why Lattice Cryptography

Misaka's post-quantum security rests on the hardness of lattice problems — specifically Learning With Errors (LWE), Ring-LWE (RLWE), and Short Integer Solution (SIS). These problems are believed to be hard even for quantum computers: no polynomial-time quantum algorithm for solving them is known, and the best known quantum attacks offer only modest improvements over classical algorithms.

Lattice cryptography was selected over other post-quantum families (hash-based, code-based, isogeny-based) because it offers the best combination of performance, key size, and versatility. Lattice schemes can instantiate signatures, key encapsulation, and zero-knowledge proofs from the same mathematical foundation.

7.2 Primitive Selection

Primitive	Algorithm	Used For
Signature	Falcon-512 (NIST FIPS 206)	Block signing, BFT votes, governance votes, wallet spend auth
Key exchange	Kyber-768 (NIST FIPS 203)	P2P transport, stealth address KEM, memo encryption
Hash	SHA3-256	Block hashing, transaction IDs, Merkle trees, key derivation
DRBG	SHAKE256-DRBG (SP 800-90A)	All randomness generation — replaces AES-CTR-DRBG
Ring signature	LaRRS (Module-LWE)	Transaction sender anonymity
Commitment	Lattice Pedersen	Amount hiding and balance proofs

7.3 Quantum-Safe Randomness (DRBG)

AES-based DRBG (CTR-DRBG) is vulnerable to Grover's algorithm, which halves the effective key length — reducing 128-bit AES security to 64-bit post-quantum security. Misaka uses SHAKE256-DRBG throughout, which has no algebraic structure exploitable by quantum algorithms. Its security reduces entirely to the collision resistance of SHA3.

All Falcon-512 signing operations draw fresh randomness from a SHAKE256-DRBG instance whose state is atomically persisted before each signing call. Nonce reuse in Falcon is catastrophic (it reveals the secret key), making this persistence requirement non-negotiable.

7.4 Security Level

All Misaka cryptographic primitives target at least 128-bit post-quantum security, corresponding to NIST security category I or higher. Kyber-768 provides 164-bit post-quantum security (NIST category III), offering a security margin above the minimum sufficient to absorb future cryptanalytic advances.

8 Token Utility: MISAKA

The MISAKA token is the native asset of the Misaka Network ecosystem. It serves three core utility functions that are essential to the operation of the network.

Function	Description
Transaction fees	All Misaka Network transactions pay fees in stMISAKA. Every transaction incurs a flat minimum fee of 2,000 stMISAKA plus a size-based component of 0.01 stMISAKA × bytes × a congestion multiplier (1.0–5.0). A typical 100 KB privacy transaction costs 3,024 stMISAKA at base congestion.
Validator staking	Validators lock MISAKA as economic stake. Rewards are distributed proportional to staked balance. Validators who equivocate lose pending rewards and are ejected from the validator set.
Archive node rewards	Archive nodes providing bootstrapping, history storage, and explorer services receive 20% of all collected fees continuously.
Governance voting	Validators cast stake-weighted governance votes on protocol changes, validator set modifications, and constitutional amendments using their Falcon-512 consensus keys.
Governance deposits	Submitting a governance proposal requires locking MISAKA as a deposit. The deposit is returned on ratification and forfeited on rejection, preventing spam proposals.

Terminology: MISAKA = Solana SPL token currently in circulation. stMISAKA = future native Layer-1 coin on the Misaka Network mainnet. The bridge converts MISAKA ↔️ stMISAKA at a fixed 1:1 ratio.

8.1 Token Launch Strategy: Solana-First

To accelerate ecosystem growth and liquidity, MISAKA has been issued as a Solana SPL token. Solana's mature DeFi infrastructure — decentralised exchanges, liquidity pools, and wallet integrations — provides immediate market access before the Misaka native chain is fully operational.

Upon mainnet launch of the native Misaka chain, a two-way bridge will enable MISAKA holders to move tokens between the Solana representation and the native L1 stMISAKA coin. The bridge uses a lock-and-mint mechanism: Solana SPL tokens are locked in a smart contract, and equivalent stMISAKA is minted on the Misaka chain. Redemption works in reverse.

The bridge design uses ZK proofs to verify Solana transaction finality without trusting a centralised relayer. The ZK verifier circuit will be audited prior to mainnet bridge activation.

9 Tokenomics

9.1 Supply Parameters

Parameter	Value
Token name	Misaka
Ticker	MISAKA
Total supply	Fixed at genesis — no additional issuance
Decimal places	9 (minimum unit: 0.000000001 MISAKA)
Token standard (initial)	Solana SPL
Token standard (native)	Misaka Network Layer-1 coin (stMISAKA)
New token issuance	None — supply is strictly fixed

MISAKA (Solana SPL) and stMISAKA (Misaka L1 native coin) are interchangeable via the bridge at a fixed 1:1 ratio.

9.2 Fee Structure

Misaka operates a fee-recycling economic model. No new tokens are created per block. All validator and node compensation derives from user-paid transaction fees.

Fee Type	Formula	Notes
Minimum fee	2,000 stMISAKA (flat)	Baseline cost reflecting PQ proof overhead; applies to every TX regardless of size
TX size fee	0.01 stMISAKA × bytes × congestion multiplier	Added on top of the minimum fee
Congestion multiplier	Block utilisation < 50% → 1.0 50–70% → 2.0 70–85% → 3.0 85–95% → 4.0 95–100% → 5.0	Auto-adjusts with network load
Typical 100 KB TX	3,024 stMISAKA	2,000 + (0.01 × 102,400 bytes × 1.0); congestion multiplier = 1.0

9.3 Reward Distribution

Recipient	Share	Rationale
Validator nodes	80% of fees	Block production, ring sig verification, BFT consensus
Archive nodes	20% of fees	History storage, bootstrapping, explorer services
Foundation	Rounding dust + base overhead	Protocol maintenance and governance infrastructure

Within the validator pool, rewards are distributed proportional to each validator's staked MISAKA at the time of block production. The block proposer receives no additional bonus, eliminating selfish-mining incentives.

9.4 Anti-Inflation Design

The zero-issuance model means that MISAKA's monetary supply is permanently fixed. As network usage grows, validators earn more in absolute fee terms without the dilutive effect of new issuance. This design aligns with Bitcoin's supply model while applying it to a proof-of-stake, privacy-preserving context.

10 Roadmap

Phase	Timeline	Milestones
Phase 1 (In Progress)	2026 Q1–Q2	Replace Ed25519 → Falcon-512 (liboqs bindings) · Replace X25519 → Kyber-768 · SHA-256 → SHA3-256 · SHAKE256-DRBG · PQ integration tests on devnet
Phase 2 (Planned)	2026 Q2–Q3	Lattice Pedersen commitments · LaRRS ring signature integration (ring size 11–16) · Jamtis stealth address wallet scanning · Range proofs · Privacy testnet launch
Phase 3 (Planned)	2027 Q3–Q4	Cardano-style governance system · Stake-weighted voting · Fee redistribution (80/20) · Archive node incentive programme · Governance transaction implementation
Phase 4 (Planned)	2027 Q1	Independent security audit (lattice crypto specialists) · iOS/Android mobile wallet · CoinGecko / CoinMarketCap listing · 3+ independent archive operators · Mainnet genesis block

11 Node Architecture

11.1 Light Nodes

Light nodes are designed for mobile wallets and end-user applications. They download only block headers and the subset of UTXOs relevant to their own wallet keys. They do not store transaction proofs, ring membership proofs, or confidential balance proofs. The Jamtis view tag scanning optimisation allows approximately 99% of outputs to be rejected with a single byte comparison, making mobile sync practical even over slow connections.

11.2 Validator Nodes

Validator nodes participate in BFT consensus and are responsible for verifying every transaction in every block they process. They execute the full validation pipeline: structural checks, link tag uniqueness, UTXO ring membership, LaRRS ring signature verification, confidential balance proof verification, range proof verification, and fee adequacy. After a block achieves BFT finality, validators may prune transaction proofs, retaining only the UTXO set and link tag set.

11.3 Archive Nodes

Archive nodes are the network's institutional memory. They retain the complete blockchain history including all ring proofs and confidential proofs. They serve UTXO snapshots to bootstrapping nodes and provide blockchain explorer APIs. Archive operation requires 16+ GB RAM and 2+ TB NVMe storage. The protocol mandates at least three independent archive operators on mainnet, preventing a single operator from censoring new node bootstrapping.

12 Consensus Mechanism

Misaka uses a Tendermint-style PBFT consensus algorithm with a validator set of 10 to 30 nodes. Privacy-preserving transactions with PQ proofs are computationally expensive to verify; a focused set of accountable validators provides faster finality without sacrificing security in a network where the privacy layer is the primary trust boundary.

Consensus Property	Value
Fault tolerance	Byzantine fault-tolerant for up to f < N/3 validators
Finality type	Single-block finality — no chain reorganisations after commit
Leader selection	Round-robin by Falcon-512 public key hash — deterministic
Vote signature	Falcon-512 over the block hash
Commit threshold	⌊2N/3⌋ + 1 Precommit votes required
Block time	60 seconds (1 minute)
Round timeout	30s Propose → 30s Prevote → 30s Precommit → next round

12.1 Dynamic Block Size

Unlike fixed-block-size chains, Misaka uses a dynamic block size mechanism that adapts to transaction demand while discouraging abusive block production.

Block Size Parameter	Value
Target block size	6 MB
Maximum block size	24 MB
Adjustment window	Median of last 100 blocks
Overshoot penalty	Quadratic reward reduction for blocks exceeding the current median

The protocol calculates the median block size over the last 100 blocks. A block proposer may produce a block up to the maximum of 24 MB, but any block that exceeds the current rolling median incurs a quadratic fee-reward penalty applied to the proposer's reward share. This creates a natural economic pressure toward efficient block packing while still allowing burst capacity when genuine demand requires it.

Quadratic penalty formula: reward_multiplier = (median_size / block_size)^2 *for blocks where block_size > median_size. This incentivises proposers to include transactions that fill blocks efficiently rather than padding blocks with dust.*

12.2 TPS Analysis

With the 60-second block time and dynamic block size, Misaka's baseline throughput is calculated as follows:

Throughput Parameter	Value
Block time	60 seconds
Target block size	6 MB (6,000 KB)
Maximum block size	24 MB
Average PQ privacy TX size	~120 KB (including LaRRS ring proof)
TX per target block	6,000 / 120 = 50 TX
Baseline TPS (target block)	50 / 60 ≈ 0.83 TPS (conservative)
TX per max block	24,000 / 120 = 200 TX
Peak TPS (max block)	200 / 60 ≈ 3.3 TPS
With batch verification (+40–60% throughput)	~4.7–5.5 TPS peak
Future: ring size = 4, avg TX ~40 KB	24,000 / 40 = 600 TX → ~15 TPS with batch verify

TPS figures reflect full privacy transactions with PQ ring proofs. Simpler payment-only transactions are smaller and achieve proportionally higher throughput. Batch verification gains apply when 50+ transactions are processed in a single verification pass.

12.3 PQ Proof Batch Verification

A critical performance optimisation in Misaka is batch verification of Falcon-512 block signatures and LaRRS ring proofs. Standard sequential verification processes each transaction proof independently:

$\mathtt{verify(TX_1)} \rightarrow \mathtt{verify(TX_2)} \rightarrow \mathtt{verify(TX_3)} \rightarrow \mathtt{...} \rightarrow \mathtt{verify(TX_n)}$

Batch verification aggregates the verification equation across all proofs in a block and checks them together in a single algebraic operation:

```
batch_verify(TX₁, TX₂, ..., TXₙ)  —  one pass over all proofs
```

For Falcon-512, batch verification exploits the linearity of the NTRU lattice check. For LaRRS ring proofs, the Module-LWE verification equations can be combined via random linear combination (with a per-batch challenge sampled from SHAKE256-DRBG), reducing the number of matrix-vector products from O(N) to O(1) for the batch check component.

Batch Verification Property	Detail
CPU cost reduction	40–60% vs sequential verification for batch size ≥50 TX
Security reduction	Negligible: soundness error per batch ≤ 2^{-128} under MLWE
Batch size trigger	Enabled automatically when block contains ≥10 TX
Implementation	liboqs batch verification API (Falcon); custom LaRRS batch module
Parallelism	Each CPU core processes a subset of the batch; trivially multi-threaded

12.4 Compact Block Propagation

With blocks up to 24 MB, naive full-block propagation would create significant network latency. Misaka implements a Compact Block protocol inspired by Bitcoin's BIP 152. Each node continuously receives and validates individual transactions (averaging 120 KB each) from the mempool before any block is produced.

When a block is finalised, the proposer broadcasts only a compact block announcement — a few kilobytes of transaction ID indices — rather than the full 24 MB block body. Receiving nodes reconstruct the full block from their local mempools using the index. Only the small fraction of transactions not already in the local mempool need to be fetched from peers.

Compact Block Property	Detail
Announcement size	~3–6 KB (tx ID index for a 200-TX block)
Full block size	Up to 24 MB
Effective propagation time	Millisecond-scale for nodes with full mempools
Fallback	Full block fetch if >5% of TXs are missing from local mempool
Security	No change to BFT finality; compact block is just a transmission optimisation

12.5 Governance-Controlled Validator Rotation

Validator set changes require a governance action (action_type 0x01 or 0x02). The proposal must pass a stake-weighted validator vote meeting the $\lfloor 2N/3 \rfloor + 1$ threshold, plus receive clearance from the Archive Governance committee. Ratified changes take effect at the next epoch boundary, preventing mid-epoch inconsistency.

13 Security Model

13.1 Cryptographic Security Assumptions

Primitive	Hard Problem	Security Level
Falcon-512	NTRU/Ring-SIS over power-of-2 cyclotomic rings	128-bit PQ (NIST Level I)
Kyber-768	Module-LWE (MLWE)	164-bit PQ (NIST Level III)
LaRRS	Module-LWE + Module-SIS	128-bit PQ (estimated)
SHAKE256-DRBG	SHA3 collision resistance	256-bit output, ≥128-bit PQ
Lattice Pedersen	Short Integer Solution (SIS)	128-bit PQ (estimated)

13.2 Threat Model

- Classical adversary: All privacy guarantees hold unconditionally against any classical computing adversary. Ring signatures provide computational anonymity under the Module-LWE assumption; confidential transactions provide amount hiding under SIS.
- Quantum adversary: Privacy guarantees hold against a quantum adversary running Shor's or Grover's algorithms. Grover's algorithm provides a quadratic speedup against hash functions, which is mitigated by using SHA3-256 with 256-bit output and SHAKE256-DRBG at 256-bit security strength.
- "Harvest now, decrypt later": Misaka transactions broadcast today remain private even if a quantum computer becomes available in the future, because all commitments and proofs use post-quantum hard problems.
- Archive node compromise: Archive nodes see the full transaction graph but cannot identify senders (ring signatures), receivers (stealth addressing), or amounts (confidential commitments).

13.3 Slashing and Economic Security

Misaka adopts Cardano's non-confiscatory penalty model. There is no stake slashing (confiscation). Validator misbehaviour results in reward reduction and ejection from the validator set. This design avoids the catastrophic economic fragility of stake-slashing in small validator sets where network partitions or software bugs could inadvertently trigger mass slashing.

14 Future Development

14.1 ZK-Accelerated Archive Verification

The current UTXO snapshot authentication uses the BFT certificate as its trust anchor. A future enhancement will add a ZK succinct proof of UTXO set derivation, providing stronger mathematical guarantees against archive equivocation and enabling trustless light-client snapshot verification without downloading block headers.

14.2 Cross-Chain Privacy Bridge

The Solana bridge is the first phase of a broader cross-chain vision. Future versions will extend the bridge to other major chains (Ethereum, Bitcoin), enabling users to shield assets from those chains inside Misaka's privacy environment. All bridge proofs will use post-quantum ZK constructions to maintain the chain's overall quantum-resistance guarantee.

14.3 Threshold Signature Governance

A future protocol upgrade will introduce lattice-based threshold signatures, reducing the BFT certificate size from O(N × 1281 bytes) to a constant-size aggregate proof as the validator set grows toward 30.

14.4 Smart Contract Layer

The current Misaka design is a UTXO-based payment chain. A future development track will explore adding a privacy-preserving smart contract layer using ZK-provable computation over the Misaka state machine, enabling private DeFi applications without compromising the core privacy guarantees.

15 Conclusion

The transition to a post-quantum world is not a distant hypothetical — it is an engineering constraint that blockchain projects must address today, because blockchain transactions are permanent and the adversary model includes future quantum capabilities. Privacy blockchains face an especially acute form of this risk: every transaction ever made remains permanently available for retroactive analysis.

Misaka Network addresses this challenge with a clean-slate design that places post-quantum cryptography at the foundation of every protocol layer. By adopting NIST-standardised Falcon-512 and Kyber-768 primitives, implementing a Seraphis/Jamtis privacy model with lattice ring signatures and confidential commitments, and operating a lightweight pruned-node architecture that enables mobile participation, Misaka delivers unconditional privacy, quantum resistance, and practical usability.

The MISAKA token provides the economic fuel for this network — aligning validator incentives, funding infrastructure operation through fee redistribution (80% validators, 20% archive nodes), and enabling community governance of protocol evolution. Its Solana-first issuance strategy provides immediate liquidity access while the native chain is prepared for mainnet launch.

Misaka is not competing with existing privacy chains on their own terms. It is building for the post-quantum era that those chains are not equipped to survive.

Appendix A Technical Protocol Specification

A.1 Block Header Structure

Every block header commits to the complete block body and establishes the chain of trust:

```
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 Transaction Structure

```
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 Ring Signature Parameters (LaRRS)

Parameter	Value	Notes
Module rank k	3	Same module structure as Kyber
Polynomial degree n	256	NTT-friendly
Modulus q	8,380,417	$= 2^{23} - 2^{13} + 1$ (prime, NTT-friendly)
L2 norm bound β	2^{18}	Rejection sampling bound
Ring size N	11–16	Default 16 for max anonymity
Proof size (N=16)	~11–14 KB per input	Per-ring-member response vector
Security level	128-bit PQ	Under MLWE hardness

A.4 Falcon-512 Parameters

Parameter	Value	Notes
Lattice dimension n	512	NTRU power-of-2 cyclotomic ring
Modulus q	12,289	NTT-friendly prime
Signature size	~666 bytes compressed	1281 bytes padded
Public key size	897 bytes	
Gaussian width σ	≈165	Trapdoor sampler parameter
Security level	128-bit PQ	NIST Level I (FIPS 206)

A.5 Key Derivation Hierarchy

```
MasterSeed (256-bit) → [HKDF-SHA3-256] → spend_key (Falcon-512 keypair) → [HKDF-SHA3-
256] → view_key (Kyber-768 keypair) → find_received_key + generate_addr_key +
unlock_amounts_key
```

A.6 Validator Verification Pipeline

1. Structural validity — parse TX, check version, ring size bounds (11–16)
2. Link tag uniqueness — no tag in inputs appears in global link tag set
3. UTXO ring membership — all ring members reference existing UTXOs
4. PQ ring signature — verify LaRRS proof over ring commitments
5. Balance proof — verify Σ(input commitments) = Σ(output commitments) + fee
6. Range proofs — verify each output commitment is non-negative
7. Fee adequacy — fee commitment decodes to value ≥ minimum fee schedule
8. Transaction size — serialised size ≤ 200 KB