misakas

Post-Quantum, PQ-only Kaspa-family BlockDAG Network

量子耐性・PQ-only Kaspa 系 BlockDAG ネットワーク

Technical Whitepaper / 技術ホワイトペーパー

Draft v0.1 based on the uploaded repository snapshot

作成日: 2026-06-05 | Generated for bilingual publication review

Status note: this paper describes the design intent and repository state observed in the provided source package. It is not an investment document, legal opinion, audit report, or launch approval.

注意: 本書は提供されたソースパッケージに基づく技術ドラフトであり、投資資料・法務意見・監査報告・本番ローンチ承認ではありません。

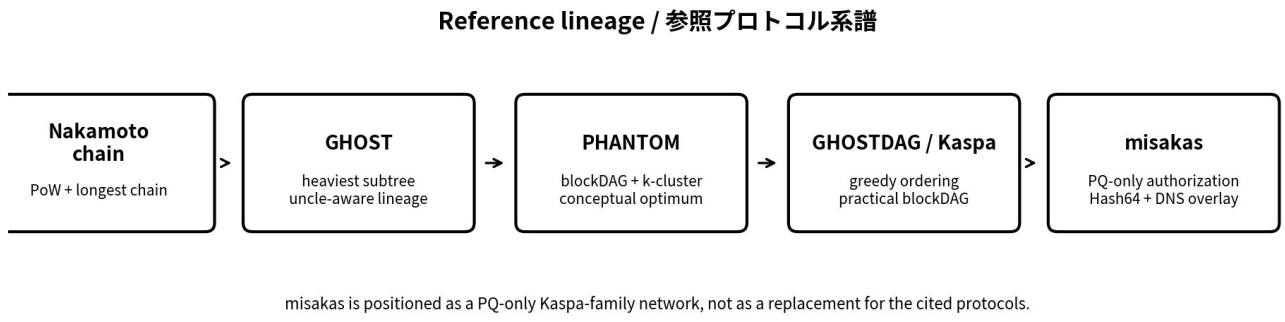

Figure 1 / 図 1: Reference lineage from Nakamoto consensus to GHOSTDAG and misakas.

0. 文書の読み方 / How to read this paper

本書は、misakas の公開用ホワイトペーパー草案として、日本語と英語を同じ構成で併記する。前半は日本語、後半は English version である。図表・用語・参照文献は両言語で再利用できるように記述した。

This document is written as a bilingual draft whitepaper for misakas. The first half is Japanese and the second half is English. The two parts intentionally mirror each other so that technical review can proceed in either language.

主要な情報源 / Primary sources

- 提供された `misakas-main` ソーススナップショット: README, `docs/kaspa-pq-design-mldsa87.md`, `docs/kaspa-pq-spec.md`, ADR-0007〜0019, consensus parameter code.
- PHANTOM and GHOSTDAG: A Scalable Generalization of Nakamoto Consensus, IACR ePrint 2018/104.
- GHOST: Secure High-Rate Transaction Processing in Bitcoin.
- NIST FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA).
- Kaspa Wiki / project material on PHANTOM GHOSTDAG and blockDAG positioning.

目次 / Contents

日本語版

1. エグゼクティブサマリー / Executive summary

misakas は、rusty-kaspa を基盤にした、PQ-only の独立ネットワークである。目的は、Kaspa 系の blockDAG / GHOSTDAG 実装が持つ高頻度ブロック生成と低レイテンシの方向性を維持しつつ、トランザクション認証を ML-DSA-87 に統一し、secp256k1/Schnorr/ECDSA、legacy address、P2SH などの非 PQ 経路を consensus・mempool・wallet/API の各層で使用不能にすることである。

本書では、misakas を「GHOSTDAG をそのまま説明する文書」ではなく、「PHANTOM/GHOSTDAG の blockDAG 研究系譜を参照し、その上に PQ-only トランザクション層、64-byte consensus identity、DNS finality overlay を重ねる Kaspa 系ネットワーク」として位置付ける。

提供された README では、現時点の運用ネットワークは experimental devnet であり、mainnet parameter set は定義されているが本番ネットワークとしてローンチまたは推奨されていない、と明記されている。このため、本書のローンチ・経済設計・finality に関する記述は「仕様草案および実装状態の説明」であり、公開時には最新コード・監査結果・ネットワーク方針で再確認する必要がある。

領域	misakas の方向性
Ledger structure	PoW blockDAG; GHOSTDAG/Kaspa 系の並列ブロック許容と ordering を参照。
Transaction authorization	ML-DSA-87 のみ。公開鍵 2592 B、署名 4627 B、署名要素 4628 B。
Address / script	PubKeyHashMlDsa87 のみ。payload は keyed BLAKE2b-512 による 64 B。P2SH は launch scope 外。
Consensus identity	block hash / txid / merkle / UTXO commitment などを Hash64 / BLAKE2b-512 domain に拡張する設計。
Finality overlay	PoW/GHOSTDAG を基礎とし、stake bond と attestation による DNS-style overlay を追加。mainnet/testnet は WorkScore と StakeScore の二次元 gate を意図。
Network status	devnet experimental。mainnet parameter set は定義済みだが、提供 README 上は live/production として扱わない。

2. 背景: DAG, GHOST, PHANTOM, GHOSTDAG / Background

Bitcoin 型の線形チェーンは、単純で監査しやすい一方、高頻度にブロックを生成するとネットワーク伝播遅延により孤立ブロックが増え、セキュリティとスループットのトレードオフが顕在化する。GHOST は、この問題に対して subtree の重みを利用する方向性を示し、高レート環境での chain selection を改善する研究として登場した。

PHANTOM は、Nakamoto consensus を blockDAG に一般化する。並列に生成されたブロックを単純に捨てるのではなく DAG 内に残し、honest な同時生成ブロックと adversarial な非協調ブロックを区別して、全順序を与えることを目指す。ただし PHANTOM の理想形は NP-hard な最適化問題を含むため、実装可能性に課題がある。

GHOSTDAG は PHANTOM の性質を実装可能な greedy algorithm として近似する。Kaspa はこの PHANTOM GHOSTDAG 系の PoW blockDAG を採用し、並列ブロックを孤立させずに consensus order に取り込むことを特徴とする。misakas はこの Kaspa 系譜を参照しつつ、量子耐性トランザクション認証と Hash64 化をネットワークの genesis から強制する。

概念	要点	misakas での扱い
DAG / blockDAG	循環のない有向グラフ。ブロックが複数親を参照し、同時生成ブロックを構造に残せる。	ledger topology の基礎概念。

概念	要点	misakas での扱い
GHOST	heaviest subtree の考え方で高レート PoW の孤立ブロック問題に対処。	GHOSTDAG 命名・系譜の前段として参照。
PHANTOM	blockDAG 上で honest cluster を見つけ、合意可能な全順序を作る設計。	理論的参照点。NP-hard 問題を含むため直接実装ではない。
GHOSTDAG	PHANTOM の greedy approximation。Kaspa 実装の中核。	PoW/GHOSTDAG base として継承・参照。

3. 設計目標と非目標 / Design goals and non-goals

設計目標 / Goals

- PQ-only: トランザクション認証を ML-DSA-87 に統一し、legacy signature opcode、legacy address、P2SH を PQ network で使用不能にする。
- Genesis isolation: mainline Kaspa や過去の kaspa-pq chain state / UTXO / address と互換性を持たない独立ネットワークにする。
- BlockDAG scalability: Kaspa 系 GHOSTDAG の高頻度ブロック生成と ordering の利点を活かす。
- Hash64 consensus identity: consensus-critical な識別子を 64-byte domain に寄せ、量子計算時代の preimage margin を明確化する。
- Operational safety: validator key の hot-node 露出を抑えるため、remote signer / software signer daemon を選択可能にする。

非目標 / Non-goals

- mainline Kaspa との wallet/RPC/P2P/address 互換性を維持すること。
- 既存 secp256k1 UTXO の移行や legacy address の PQ 化を主張すること。
- transport-layer confidentiality を PQ と主張すること。ML-KEM hybrid 等が有効でない限り transport は PQ claim の外に置く。
- 初期 launch scope で ML-DSA multisig/P2SH/smart contracts を標準化すること。
- DNS overlay を BFT hard finality と表現すること。

4. システム概要 / System overview

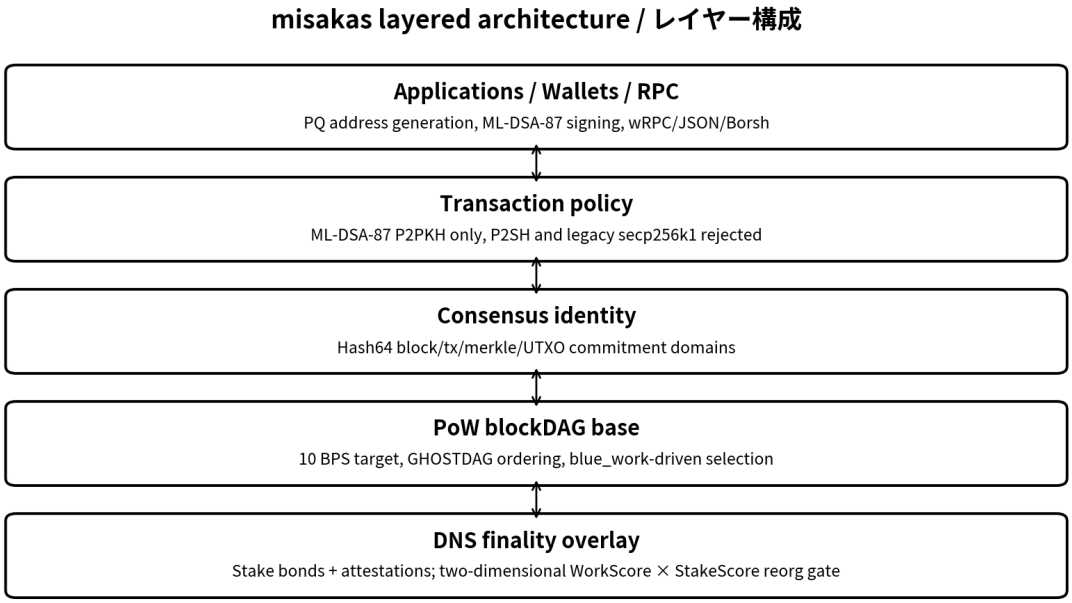

Figure 2 / 図 2: misakas のレイヤー構成。PoW/GHOSTDAG を基礎に、PQ-only transaction policy と DNS overlay を重ねる。

misakas の設計は、単一の暗号アルゴリズム差し替えに留まらない。署名方式、address payload、script policy、sighash、wallet/API、mempool standardness、consensus validation、genesis、UTXO commitment、node tooling を一貫して PQ-only にする必要がある。

提供された設計書では、重要な判断として「PQ 制約は mempool だけではなく consensus validation と script engine に置く」とされている。これにより、miner が mempool を迂回して legacy output を block に直投入する経路や、P2SH redeem 経由で legacy opcode を復活させる経路を塞ぐ。

コンポーネント	役割
kaspad	フルノード。binary 名は上流と同じだが、misakas network として PQ-only params を持つ。
kaspa-pq-miner	devnet 等で ML-DSA-87 address に採掘報酬を送る miner tooling。
kaspa-pq-validator	stake bond を持つ validator sidecar。canonical-ready epoch に attestation を発行する。
kaspa-pq-signer	validator key を validator process 外に保持する software signer daemon。strict policy では equivocation guard を signer 側に移す。
wallet / CLI / WASM	ML-DSA-87 key generation, PQ address, PQ signing, legacy path gating。

5. コンセンサス層: PoW blockDAG + GHOSTDAG / Consensus layer

misakas は、ブロック生成と tip selection の基礎を PoW/GHOSTDAG に置く。Kaspa 系 blockDAG では、同時に生成されたブロックを単純な orphan として破棄するのではなく、DAG に取り込み、GHOSTDAG によって ordering を与える。

提供コードの BPS 関連定数では 10 BPS が標準型として扱われ、target_time_per_block は 100 ms となる。10 BPS に対する GHOSTDAG K は 124 と定義されている。max block parents は performance と参照数の観点から上限 16 に抑えられている。

PoW 部分では、Layered PoW と 512-bit comparison domain が設計に含まれる。ここで重要なのは、PoW/GHOSTDAG が block production と selected-chain ordering の基礎であり、DNS overlay はそれを置き換えるものではないという点である。

6. PQ-only トランザクション認証 / PQ-only transaction authorization

misakas の中核は、トランザクション署名を ML-DSA-87 に統一することである。NIST FIPS 204 は ML-DSA をデジタル署名標準として定義しており、提供 README では ML-DSA-87 を NIST category 5 として採用している。

ML-DSA-87 は署名と公開鍵が大きい。公開鍵は 2592 bytes、署名は 4627 bytes、signature script 上の署名要素は sighash type 1 byte を加え 4628 bytes となる。このため、script element size と signature script length の上限を引き上げ、mass_per_sig_op を 10,000 に再校正している。

署名 transcript では、Schnorr 用の sighash を流用せず、`calc_mldsa87_signature_hash` による 64-byte Hash64 と、`kaspa-pq-v2/sighash/mldsa87` domain tag を使う。署名 context は `kaspa-pq-v2/tx/mldsa87` であり、scheme と network の取り違えを防ぐ domain separation が設計意図である。

項目	値
Signature algorithm	ML-DSA-87 / FIPS 204 / libcrux-ml-dsa = 0.0.9 exact pin
Public key	2592 bytes
Signature	4627 bytes
Signature item	4628 bytes = signature || sighash_type
Tx context	kaspa-pq-v2/tx/mldsa87
Sighash domain	kaspa-pq-v2/sighash/mldsa87
Legacy signatures	secp256k1/Schnorr/ECDSA disabled in PQ consensus mode

7. Hash64, アドレス, UTXO commitment / Hash64, address, UTXO commitment

misakas の address は `PubKeyHashMlDsa87` のみであり、payload は ML-DSA-87 verification key を keyed BLAKE2b-512 で 64-byte 化した値である。標準 scriptPubKey は `OP_DUP OP_BLAKE2B_512 OP_DATA64 <64B> OP_EQUALVERIFY OP_CHECKSIG_MLDSA87` であり、P2SH は launch scope から外される。

Consensus identity は 64-byte BLAKE2b-512 domain に寄せられる。設計文書の主張規律では、「512-bit commitment domain」「256-bit quantum preimage margin」「high-margin quantum collision resistance」は許容される一方、「全体として 256-bit post-quantum security」や「256-bit quantum collision」は禁止されている。

UTXO commitment は Hash64 として扱われる。これは block header、genesis、DB serialization、RPC/WASM DTO、fixtures など広い範囲に影響するため、mainline Kaspa 互換性ではなく新 genesis の独立ネットワークとして扱う必要がある。

領域	仕様上のポイント
Address version	PubKeyHashMlDsa87 only
Address payload	keyed BLAKE2b-512("kaspa-pq-v2/address/mldsa87", verification key) -> 64 B
Standard script	ML-DSA-87 P2PKH only; 69-byte output script
P2SH	disabled / launch scope 外

領域	仕様上のポイント
UTXO commitment	Hash64
Script caps	MAX_SCRIPT_ELEMENT_SIZE = 8192; MAX_SCRIPTS_SIZE / max_signature_script_len = 16,384

8. DNS finality overlay / DNS finality overlay

DNS overlay は、PoW/GHOSTDAG を置き換える finality gadget ではない。PoW が block production と tip selection を担い、PoS validator が selected-chain anchor に対して attestation を行い、on-chain shard として集約された StakeScore が deep reorg gate に使われる。

現行コードコメントでは、mainnet/testnet の production params は 20M KAS の minimum active stake / minimum bond amount、14-day evidence window、14-day unbonding + reorg horizon を採用し、required_work_depth と required_stake_depth の両方で DNS confirmation を gate する意図が示されている。一方、devnet/simnet は fast testing のため required_work_depth = 0 とし、stake-only confirmation に近い挙動を許す。

重要なのは、DNS を BFT hard finality と呼ばないことである。候補 fork が DNS-confirmed prefix を離脱する場合、WorkScore と StakeScore の両方で canonical chain を明示的 margin 以上に上回る必要がある、という non-substitutability が主張の中心である。PoW だけ、または stake だけでは confirmed history を書き換えられない、という説明に留めるべきである。

要素	説明
StakeBondPayload	validator key と stake を結び付ける bond。unbonding/evidence window により長距離攻撃の余地を制限。
StakeAttestation	validator が epoch と selected-chain anchor に署名。
Attestation shard	大きな certificate tx を避けるため、8-16 attestations 程度を shard として on-chain 化。
Slashing evidence	同一 validator が同 epoch で incompatible history に署名した証拠を提出し、bond を slash。
Reorg gate	confirmed prefix を離脱する fork は WorkScore と StakeScore の両方で dominance margin を満たす必要。

9. ノード構成と運用モデル / Node and operation model

misakas の node binary は `kaspad` のままだが、network、address prefix、project branding は misakas として扱われる。devnet では `--devnet --enable-unsynced-mining --utxoindex` などを用い、wallet/validator が必要とする borsh wRPC port を有効にする。

validator は `kaspa-pq-validator` sidecar として動作し、bond が active な間、canonical-ready epoch に対して attestation を発行する。README によれば、すべての misakas network は 10 BPS であり、attestation_epoch_length_blue_score = 100 は約 10 秒に相当する。default の attest poll interval 3 秒は単一 validator を追随させるための値として説明されている。

remote signer は運用上の重要な安全機構である。`kaspa-pq-signer` は validator key を validator process の外に保持し、Unix domain socket 経由で signing request に応答する。strict policy では anti-equivocation guard と crash-consistent store、hash-chained audit log を signer 側で持つため、validator host が侵害されても private key の直接流出や二重署名を抑制できる。

10. セキュリティモデルと主張規律 / Security model and claim discipline

misakas の security claim は、強く言うべき点と、言ってはいけない点を明確に分ける必要がある。提供設計書は、transport layer を PQ claim の外に置くこと、BFT hard finality と表現しないこと、量子 collision resistance を過大に主張しないことを明示している。

許容される表現	避けるべき表現
Tx authorization uses ML-DSA-87.	All cryptography is post-quantum.
secp256k1 signing is disabled in PQ consensus mode.	Legacy Kaspa addresses are quantum-resistant.
64-byte BLAKE2b-512 consensus identity.	256-bit post-quantum security across the board.
Transport is out of PQ scope unless ML-KEM hybrid is enabled.	Transport is PQ-secure by default.
PoW-ledger + PoS probabilistic finality overlay.	BFT hard finality / irreversible checkpoint.

脅威モデル上、ML-DSA-87 はトランザクション署名の量子耐性を高めるが、DoS、実装脆弱性、supply-chain、key custody、network eclipse、low validator decentralization、economic attack などのリスクを消すものではない。特に ML-DSA は署名が大きいため、mass policy と verification cost の継続的なベンチマークが必要である。

11. ロードマップとリスク / Roadmap and risks

提供リポジトリには、ML-DSA-87 migration、PQ-only gating、remote signer、validator overlay、reward/economics ADR などが含まれている。一方で、mainnet launch 前には、公開監査、parameter calibration、multi-operator validator set、network monitoring、wallet UX、release signing、reproducible builds、incident response runbook などを整える必要がある。

- 監査: cryptographic implementation、sighash domain separation、script policy、mempool/consensus consistency、Hash64 serialization、genesis and premine handling。
- 性能: ML-DSA-87 verify cost、script size、block mass、attestation shard mass、10 BPS sustained sync、IBD、pruning。
- 運用: validator key custody、remote signer hardening、slashing evidence handling、unbonding window、backup/restore、checkpoint distribution。
- ガバナンス: mainnet parameter set を live とみなす条件、premine custody、validator minimums、DNS claim language、release process。

結論として、misakas は「量子耐性署名を追加しただけの Kaspa fork」ではなく、legacy cryptography を consensus layer から取り除き、blockDAG/GHOSTDAG 系の high-throughput PoW を PQ-only transaction layer と結合しようとする実験的ネットワークである。公開ホワイトペーパーとしては、強い技術的方向性を示しつつ、現時点の devnet status と未監査リスクを明示する姿勢が最も重要である。

English Version

1. Executive summary / Executive summary

misakas is an independent, PQ-only network built from the rusty-kaspa codebase. Its core purpose is to preserve the high-rate blockDAG direction of the Kaspa/GHOSTDAG family while replacing classical transaction authorization with ML-DSA-87 and making non-PQ paths - secp256k1, Schnorr, ECDSA, legacy addresses, and P2SH - unavailable at the consensus, mempool, and wallet/API layers.

The paper positions misakas as a Kaspa-family blockDAG network informed by the GHOST, PHANTOM, and GHOSTDAG line of research, not as a new proof of those protocols. The distinctive misakas contribution described here is the combination of PQ-only transaction authorization, 64-byte consensus identity, and a DNS-style finality overlay on top of a PoW/GHOSTDAG ledger base.

The supplied repository describes the current live posture as experimental devnet. A mainnet parameter set exists in code, but the README states that it is not a launched or production-endorsed network. Therefore, launch, token, validator, and finality statements in this draft must be re-checked against current code, audit status, and governance decisions before publication.

Area	misakas direction
Ledger structure	PoW blockDAG inspired by the GHOSTDAG/Kaspa lineage; parallel blocks are incorporated rather than simply orphaned.
Transaction authorization	ML-DSA-87 only. Public key 2592 B, signature 4627 B, signature item 4628 B.
Address / script	PubKeyHashMlDsa87 only. Payload is a 64 B keyed BLAKE2b-512 digest. P2SH is outside launch scope.
Consensus identity	Hash64 / BLAKE2b-512 domains for consensus-critical identifiers and UTXO commitments.
Finality overlay	PoW/GHOSTDAG remains the base; stake bonds and attestations add a DNS-style WorkScore x StakeScore reorg gate.
Network status	Experimental devnet. Mainnet parameters are defined but should not be treated as live production without an explicit launch decision.

2. Background: DAG, GHOST, PHANTOM, GHOSTDAG / Background

A linear Nakamoto chain is simple and auditable, but high block rates increase the impact of propagation delay and stale/orphan blocks. The GHOST rule addressed this scaling pressure by using subtree weight in chain selection, reducing the penalty of blocks that were created honestly but arrived outside the single main chain.

PHANTOM generalizes Nakamoto consensus from a chain into a blockDAG. Instead of discarding concurrent blocks, it keeps them in a directed acyclic graph and seeks a robust total order by distinguishing well-connected honest blocks from adversarial or non-cooperating blocks. The conceptual PHANTOM formulation, however, includes an NP-hard optimization problem.

GHOSTDAG is the practical greedy approximation designed to capture the essential PHANTOM behavior. Kaspa implements the PHANTOM GHOSTDAG protocol and uses this blockDAG ordering to support high block rates. misakas inherits this design lineage while changing the authorization and consensus-identity surfaces from genesis.

Concept	Key idea	Role in misakas
DAG / blockDAG	A directed acyclic graph where blocks may reference multiple parents and concurrent blocks remain in the structure.	The ledger topology.
GHOST	A heaviest-subtree approach to mitigate stale-block penalties at high block rates.	The historical predecessor of GHOSTDAG.
PHANTOM	A blockDAG protocol using a k-cluster idea to derive consensus ordering.	A theoretical reference point; not implemented directly.
GHOSTDAG	A greedy, implementable approximation of PHANTOM used in Kaspa.	The blockDAG ordering family on which misakas is based.

3. Design goals and non-goals / Design goals and non-goals

Goals

- PQ-only authorization: accept ML-DSA-87 transaction authorization and reject legacy signature opcodes, legacy addresses, and P2SH in PQ consensus mode.
- Genesis isolation: run as a new network with its own genesis, address prefixes, network IDs, and UTXO state rather than as a compatibility layer for mainline Kaspa.
- BlockDAG scalability: preserve the high-rate PoW/GHOSTDAG direction of the Kaspa family.
- Hash64 consensus identity: use 64-byte domains for consensus-critical hashes and commitments, with precise quantum-security language.
- Operational key safety: support a remote signer path so validator signing keys can live outside the validator process.

Non-goals

- Maintaining wallet, RPC, P2P, or address compatibility with mainline Kaspa.
- Migrating secp256k1 UTXOs or claiming that legacy Kaspa addresses are quantum-resistant.
- Claiming post-quantum transport security unless an ML-KEM hybrid or equivalent transport design is explicitly enabled.
- Standardizing ML-DSA multisig, P2SH, or smart contracts in the initial launch scope.
- Describing DNS overlay behavior as BFT hard finality.

4. System overview / System overview

The architecture is not a one-line replacement of a signature algorithm. A coherent PQ-only network must align signature scheme, address payload, script policy, sighash, wallet/API, mempool standardness, consensus validation, genesis, UTXO commitments, and operator tooling.

The design documents make a critical enforcement decision: PQ restrictions must live in consensus validation and the script engine, not only in mempool policy. This prevents a miner from bypassing the mempool and placing legacy outputs directly into blocks, and prevents P2SH redeem paths from reintroducing legacy signature opcodes.

Component	Role
kaspad	Full node. The binary name remains upstream-compatible, but network parameters and branding are misakas.
kaspa-pq-miner	Mining tool that pays to ML-DSA-87 misakas addresses in devnet and test environments.
kaspa-pq-validator	Validator sidecar that bonds stake and attests selected-chain anchors.

Component	Role
kaspa-pq-signer	Software signer daemon that holds validator keys outside the validator process and can enforce strict anti-equivocation policy.
wallet / CLI / WASM	PQ key generation, address creation, transaction signing, and legacy path gating.

5. Consensus layer: PoW blockDAG + GHOSTDAG / Consensus layer

misakas keeps PoW/GHOSTDAG as the base layer for block production and tip selection. In a Kaspa-family blockDAG, concurrently mined blocks are not simply discarded as orphans; they remain in the DAG and receive consensus ordering through GHOSTDAG.

The repository parameters treat 10 BPS as the standard block rate, yielding a 100 ms target time per block. The BPS table defines GHOSTDAG K = 124 for 10 BPS, while max direct parents are capped at 16 for processing and reference-growth reasons.

The PoW design also includes Layered PoW and a 512-bit comparison domain. The key architectural point is that DNS is an overlay: PoW/GHOSTDAG remains responsible for block production and ordering, while the stake layer adds a separate signal for deep-reorg resistance.

6. PQ-only transaction authorization / PQ-only transaction authorization

The central cryptographic move is to standardize transaction authorization on ML-DSA-87. NIST FIPS 204 specifies ML-DSA as a module-lattice-based digital signature standard, and the supplied README adopts ML-DSA-87 as the category-5 parameter set for misakas transaction authorization.

ML-DSA-87 is large compared with classical signatures: the public key is 2592 bytes, the signature is 4627 bytes, and the signature script item is 4628 bytes after appending the sighash type. This size changes the script limits, transaction mass policy, fee estimation, dust policy, and DoS model. The repository recalibrates mass_per_sig_op to 10,000 based on the measured ML-DSA-87 verification cost.

The ML-DSA signing transcript must not reuse the Schnorr sighash. misakas uses `calc_mldsa87_signature_hash`, a 64-byte Hash64 transcript domain-tagged as `kaspa-pq-v2/sighash/mldsa87`, and signs with the context `kaspa-pq-v2/tx/mldsa87`. This domain separation is the boundary between schemes, networks, and message purposes.

Item	Value
Signature algorithm	ML-DSA-87 / FIPS 204 / libcrux-ml-dsa = 0.0.9 exact pin
Public key	2592 bytes
Signature	4627 bytes
Signature item	4628 bytes = signature || sighash_type
Tx context	kaspa-pq-v2/tx/mldsa87
Sighash domain	kaspa-pq-v2/sighash/mldsa87
Legacy signatures	secp256k1/Schnorr/ECDSA disabled in PQ consensus mode

7. Hash64, address, and UTXO commitment / Hash64, address, UTXO commitment

The standard address type is `PubKeyHashMlDsa87` only. The payload is a 64-byte keyed BLAKE2b-512 digest of the ML-DSA-87 verification key. The standard output script is `OP_DUP OP_BLAKE2B_512 OP_DATA64 <64B> OP_EQUALVERIFY OP_CHECKSIG_MLDSA87`, and P2SH is excluded from the launch scope.

Consensus identity moves toward 64-byte BLAKE2b-512 domains. The correct public language is narrow: a 512-bit commitment domain, a 256-bit quantum preimage margin under Grover-style reasoning, and high-margin quantum collision resistance. The document should not claim 256-bit quantum collision resistance or blanket 256-bit post-quantum security for every subsystem.

The UTXO commitment is treated as Hash64. Because this affects block headers, genesis, database serialization, RPC/WASM DTOs, and fixtures, misakas must be understood as a new-genesis network rather than a mainline Kaspa compatibility layer.

Area	Specification point
Address version	PubKeyHashMlDsa87 only
Address payload	keyed BLAKE2b-512("kaspa-pq-v2/address/mldsa87", verification key) -> 64 B
Standard script	ML-DSA-87 P2PKH only; 69-byte output script
P2SH	disabled / outside launch scope
UTXO commitment	Hash64
Script caps	MAX_SCRIPT_ELEMENT_SIZE = 8192; MAX_SCRIPTS_SIZE / max_signature_script_len = 16,384

8. DNS finality overlay / DNS finality overlay

The DNS overlay is not a replacement for PoW/GHOSTDAG and should not be described as a BFT finality gadget. PoW remains the block-production and tip-selection mechanism. Validators bond stake, attest selected-chain anchors, and contribute on-chain StakeScore through bounded attestation shards.

The current production parameter comments describe mainnet/testnet as using a 20M KAS minimum active stake and minimum bond, a 14-day evidence window, a 14-day unbonding period plus reorg horizon, and both required_work_depth and required_stake_depth as confirmation gates. Devnet/simnet keep required_work_depth at zero for fast testing, so their behavior is closer to stake-only confirmation.

The core public claim is non-substitutability. A candidate fork that exits a DNS-confirmed prefix must beat the canonical chain in both WorkScore and StakeScore by explicit margins. A PoW-only surplus cannot compensate for a stake deficit, and a stake-only surplus cannot compensate for insufficient work.

Element	Description
StakeBondPayload	Locks stake to a validator key and keeps it slashable through the unbonding/evidence window.
StakeAttestation	A validator signature over an epoch and selected-chain anchor.
Attestation shard	A bounded on-chain shard carrying several attestations to avoid huge certificate transactions.
Slashing evidence	Two incompatible attestations by the same validator for the same epoch can slash the bond.
Reorg gate	A fork exiting a confirmed prefix must satisfy both WorkScore and StakeScore dominance margins.

9. Node and operation model / Node and operation model

The node binary remains `kaspad`, but the network, address prefixes, and project branding are misakas. A devnet node is run with flags such as `--devnet`, `--enable-unsynced-mining`, and `--utxoindex`, and wallet/validator tooling requires the Borsh wRPC port.

The validator sidecar bonds stake and attests one canonical-ready epoch per round. The README states that every misakas network runs at 10 BPS, so an attestation epoch length of 100 blue score is roughly ten seconds at low DAG parallelism. The default three-second attestation polling interval is intended to keep a single validator caught up.

`kaspa-pq-signer` is an important operational control. It keeps the ML-DSA-87 validator key outside the validator process and answers signing requests over a local Unix domain socket. In strict policy mode, the signer owns the anti-equivocation record and hash-chained audit log, reducing the impact of a compromised validator process.

10. Security model and claim discipline / Security model and claim discipline

The security message must be precise. ML-DSA-87 improves transaction authorization against quantum-capable adversaries, but it does not by itself solve denial-of-service, implementation vulnerabilities, supply-chain risk, validator centralization, network eclipse attacks, or key-custody failures.

Acceptable language	Avoid
Tx authorization uses ML-DSA-87.	All cryptography is post-quantum.
secp256k1 signing is disabled in PQ consensus mode.	Legacy Kaspa addresses are quantum-resistant.
64-byte BLAKE2b-512 consensus identity.	256-bit post-quantum security across the board.
Transport is out of PQ scope unless ML-KEM hybrid is enabled.	Transport is PQ-secure by default.
PoW-ledger plus PoS probabilistic finality overlay.	BFT hard finality or irreversible checkpoint.

Because ML-DSA signatures are large and verification is heavier than classical signatures, mass policy and fee estimation are part of the security model. The network must treat large scripts, attestation shards, signature cache keys, and verification cost as consensus-adjacent DoS surfaces that require ongoing benchmarks.

11. Roadmap and risks / Roadmap and risks

The repository contains design and implementation work for ML-DSA-87 migration, PQ-only gating, remote signing, the validator overlay, reward/economic ADRs, and 10 BPS operation. Before a production mainnet launch, the project should complete external audits, parameter calibration, multi-operator validator readiness, monitoring, wallet UX, release signing, reproducible builds, and incident response procedures.

- Audit focus: cryptographic implementation, domain separation, script policy, mempool/consensus consistency, Hash64 serialization, genesis and premine handling.
- Performance focus: ML-DSA-87 verification, script size, block mass, attestation shard mass, sustained 10 BPS sync, initial block download, and pruning.
- Operational focus: validator key custody, remote signer hardening, slashing evidence, unbonding, backup/restore, and checkpoint distribution.
- Governance focus: explicit mainnet launch conditions, premine custody, validator minimums, DNS claim language, and release process.

In conclusion, misakas should be presented as an experimental PQ-only Kaspa-family network: it combines a PoW/GHOSTDAG blockDAG base with strict ML-DSA-87 transaction authorization and a future-facing DNS-style finality overlay. Its strongest public posture is precise technical ambition plus honest status disclosure.

Appendices / 付録

A. 主要パラメーター一覧 / Key parameter table

Parameter	Repository snapshot value / description
Network family	misakas; independent PQ-only Kaspa-family network
Current live status	Experimental devnet only according to the supplied README
Block rate	10 BPS; target_time_per_block = 100 ms
GHOSTDAG K for 10 BPS	124
Max direct parents	16 cap in BPS helper
Signature	ML-DSA-87, NIST FIPS 204 category 5
ML-DSA public key / signature	2592 B / 4627 B
Tx context	kaspa-pq-v2/tx/mldsa87
Sighash	calc_mldsa87_signature_hash -> 64-byte Hash64; domain kaspa-pq-v2/sighash/mldsa87
Address payload	64 B keyed BLAKE2b-512 over verification key
Standard script	ML-DSA-87 P2PKH only
P2SH	Disabled in PQ mode / outside launch scope
Script caps	MAX_SCRIPT_ELEMENT_SIZE 8192; signature script 16,384
mass_per_sig_op	10,000 in params comments after ML-DSA-87 recalibration
DNS overlay	Stake bonds + attestations + WorkScore x StakeScore reorg gate
Production DNS minimum	20M KAS minimum stake/bond in current production params comments
Production unbond/evidence window	14 days at 10 BPS plus reorg-horizon details in params comments
Remote signer	kaspa-pq-signer software signer daemon; hardware HSM deferred

B. 用語集 / Glossary

Term	Meaning
blockDAG	A directed acyclic graph of blocks, allowing concurrent blocks to be retained and ordered.
GHOSTDAG	A greedy protocol for ordering a blockDAG, used by Kaspa.
ML-DSA	Module-Lattice-Based Digital Signature Algorithm standardized in NIST FIPS 204.
PQ-only	A mode where post-quantum transaction authorization is the only accepted path.
Hash64	A 64-byte consensus hash/commitment identity used in misakas design.
DNS overlay	A stake-attestation overlay adding a second dimension for deep-reorg resistance; not BFT hard finality.
StakeScore	Deterministic score accumulated from valid on-chain validator attestations.
WorkScore / blue_work	PoW/GHOSTDAG work dimension used for ordering and reorg evaluation.

C. 参照文献 / References

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf

[2] Yonatan Sompolinsky and Aviv Zohar, Secure High-Rate Transaction Processing in Bitcoin, Financial Cryptography and Data Security, 2015; ePrint 2013/881. https://eprint.iacr.org/2013/881.pdf

[3] Yonatan Sompolinsky, Shai Wyborski, and Aviv Zohar, PHANTOM and GHOSTDAG: A Scalable Generalization of Nakamoto Consensus, IACR ePrint 2018/104. https://eprint.iacr.org/2018/104

[4] Kaspa Wiki, overview of Kaspa as a proof-of-work cryptocurrency implementing PHANTOM GHOSTDAG. https://wiki.kaspa.org/en/home

[5] NIST FIPS 204, Module-Lattice-Based Digital Signature Standard, August 13, 2024. https://csrc.nist.gov/pubs/fips/204/final

[6] MISAKA-BTC / misakas repository snapshot supplied by user: README, docs/kaspa-pq-design-mldsa87.md, docs/kaspa-pq-spec.md, ADR-0007..0019, and consensus parameter source. https://github.com/MISAKA-BTC/misakas

Publication note: Before external publication, replace repository-snapshot references with tagged releases and audited commit hashes, and update this document if any consensus parameter or claim language changes.