

WIZM Chain

A Post-Quantum Privacy Blockchain:
Formal Specification of State Transition, Consensus and Cryptography
Production edition: five-validator PoA mainnet

WIZM Protocol Engineering

14 October 2026

Verified against `wizm-chain` at commit `0195ec2`; measurements from the live five-validator mainnet.

Abstract

This paper specifies WIZM as a deterministic replicated state machine running proof-of-authority among five validators on ten-second slots. We define the protocol instance and world state σ , the transaction-level transition $\Upsilon(\sigma, T)$ and block-level transition $\Omega(B, \sigma)$ with validity predicates for five transaction layouts; post-quantum cryptography (Falcon-512, ML-KEM-768, BLAKE3, transparent Flock proofs, stealth derivation) as formal schemes with correctness equations; PoA slot mathematics with seal-suppression gates (mesh-settle, blind, behind, flap, first-seen, syncing) and a deterministic same-height convergence rule; a gap-buffered mempool formalised as a transition system with floors, jumps, parking, re-grounding and reaping; pipelined catch-up with a stall-independent trigger; fee conservation and the closed-form emission schedule; network timing with a derived capacity theorem; and measured throughput reconciled from chain data.

Contents

1	System and state model	3
1.1	Nomenclature caveat	3
2	Cryptographic schemes	3
3	Addresses, stealth and notes	4
4	Flock transparent proofs	4
5	Transactions	5
6	State transition	5
7	Consensus mathematics	5
8	Mempool as a transition system	6
9	Network bounds and node operation	7
10	Supply function and genesis	7
11	Wallet backup envelope	7
12	Measured performance	7
A	Constant table	8

B	RPC reference	8
C	Code-comment errata	8
D	Verification matrix	8

1 System and state model

Definition 1.1 (Protocol instance). A WIZM instance is a tuple

$$\mathcal{W} = (N, T_{\text{blk}}, B_{\text{max}}, \mathcal{V}, H_0) \quad (1)$$

with committee size N , block interval $T_{\text{blk}} = 10$ s, proposal cap $B_{\text{max}} = 1200$, validator set $\mathcal{V} = \{0, \dots, N-1\}$ and genesis hash H_0 . Launch configuration: $N = 5$ on five regions.

Definition 1.2 (World state). The world state is a tuple

$$\sigma = (A, \mathcal{N}, C, I, K, R, T, \rho) \in \Sigma, \quad (2)$$

where $A : \{0, 1\}^{160} \rightarrow \mathbb{N} \times \mathbb{N}$ maps addresses to (balance, nonce), $\mathcal{N} \subset \{0, 1\}^{256}$ is the spent-nullifier set, $C \in (\{0, 1\}^{256})^*$ the commitment sequence with index I , $K \subset \{0, 1\}^{256}$ the spent key-image set, $R \in (\{0, 1\}^{256})^{\leq 64}$ the recent-roots window, T the depth-22 shielded Merkle tree, and $\rho \in \{0, 1\}^{256}$ the running hash-chain accumulator.

Definition 1.3 (Encoding). Integers are unsigned little-endian; $\parallel$ is concatenation; $H : \{0, 1\}^* \rightarrow \{0, 1\}^{256}$ is BLAKE3-256, modelled as a random oracle when domain-separated. Addresses derive as

$$\text{addr}(pk) = H(pk)[0..20], \quad 1 \text{ token} = 10^8. \quad (3)$$

1.1 Nomenclature caveat

Code comments predate primitive selection and say “ML-DSA” where the linked scheme is Falcon-512 (standardised as FN-DSA, FIPS 206), and “ML-KEM” where the linked code paths are pre-standardisation Kyber with the 768-bit set deployed for committee/mempool use. Older prose in this repository says “four validators”, “5 s slots”, “depth 20” and “Bullshark”; the normative values are this paper’s (five validators, 10 s slots, depth 22, PoA). Appendix C lists every stale label.

2 Cryptographic schemes

Definition 2.1 (Signature scheme). $\Pi_{\text{sig}} = (\text{Gen}, \text{Sign}, \text{Verify})$ is Falcon-512 over $\mathcal{PK} = \{0, 1\}^{7176}$, $\mathcal{SK} = \{0, 1\}^{10248}$, variable compressed signatures in $[512, 690]$ bytes (897-byte public keys, 1281-byte secret keys). Correctness:

$$\Pr \left[\begin{array}{l} (pk, sk) \leftarrow \text{Gen}() \\ \text{Verify}(pk, m, \text{Sign}(sk, m)) = 1 \end{array} \right] = 1 - \text{negl}. \quad (4)$$

Verification rejects $|pk| \neq 897$, $|\sigma| \notin [512, 690]$, and empty inputs. Signing is deterministic; admission verifies transparent signatures before pool entry and caches the verdict so execution skips redundant checks.

Definition 2.2 (KEM). $\Pi_{\text{kem}} = (\text{Gen}, \text{Encaps}, \text{Decaps})$ is ML-KEM-768 ($|pk| = 1184$, $|ct| = 1088$, $|ss| = 256$ bits) for the encrypted mempool and committee shares, with

$$\text{Decaps}(sk, \text{Encaps}(pk)) = ss \quad \text{except with negligible failure.} \quad (5)$$

The shared secret feeds AES-256-GCM for entry bodies; sender and nonce metadata stay in plaintext headers for gap-buffered draining without decrypting. Threshold key support holds validator shares.

Definition 2.3 (Hash domains). Let $H_D(x) = H(D \parallel x)$. Deployed domains include `wizm-flock-v1` (proof transcript), `wizm-commitment-v1`, `wizm-nullifier-v1`, `wizm-blake3-pair-v1` (Merkle), `wizm-shielded-note`, `wizm-mempool-aes-256-gcm`, `wizm-pq-transport-v1`, `wizm-stealth-amount`, and the genesis seed `wizm_genesis`. AES-256-GCM secures notes, amounts and pool payloads; ChaCha20-Poly1305 secures only gossip transport with nonce $H(ss \parallel |ct|_{\text{le64}})[0..12]$.

3 Addresses, stealth and notes

Definition 3.1 (Stealth derivation). Recipient meta-address $M = (pk_s, pk_v)$. Sender samples $r \xleftarrow{\$} \{0, 1\}^{256}$ and publishes

$$s = H(r), \quad t = s[0], \quad A = H(pk_s \parallel s)[0..20], \quad (A, r, t). \quad (6)$$

Detection recomputes $s = H(r)$, rejects unless $s[0] = t$ (fast path, 255/256 rejection), and accepts iff $H(pk_s \parallel s)[0..20] = A$. Double spends are excluded by key images $k = H(r \parallel A)$ with the rule $k \notin K$ pre-apply, $K \leftarrow K \cup \{k\}$ post-apply. Amounts hide as $\text{AEAD}_K(v_{\text{le64}})$ under $K = \text{KDF}(\text{wizm-stealth-amount}, H(r))$.

Definition 3.2 (Notes, commitments, nullifiers). A note is $(v, b, s) \in \mathbb{N} \times \{0, 1\}^{256} \times \{0, 1\}^{256}$ sealed as (ct_{768}, t, c_{88}) totaling 857 bytes. Commitments and nullifiers

$$cm = H_{\text{wizm-commitment-v1}}(v_{\text{le64}} \parallel b), \quad (7)$$

$$nf = H_{\text{wizm-nullifier-v1}}(sk \parallel \ell_{\text{le64}}), \quad (8)$$

with deposits fixing $\ell = 0$, $secret = H(sender \parallel n_{\text{le64}})$. The shielded tree is binary of depth $d = 22$ (capacity $2^{22} = 4,194,304$) with pair hash $H_{\text{wizm-blake3-pair-v1}}$; proofs verify against the tip root or any of the 64 retained roots:

$$\text{VerifyRoot}(r) \iff r = \text{tip} \vee r \in R. \quad (9)$$

4 Flock transparent proofs

Definition 4.1 (Scheme). $\Pi_{\text{flock}} = (\text{Setup}, \text{Prove}, \text{Verify})$ over relation $\mathcal{R}$ with statement $x = (nf, cm, root)$ and witness $w = (v, b, sk, \ell, P)$, $|P| = 22$:

$$\mathcal{R}(x, w) \iff \begin{cases} cm = H_{\text{cmt}}(v_{\text{le64}} \parallel b), & v \neq 0, \\ nf = H_{\text{nf}}(sk \parallel \ell_{\text{le64}}), \\ root = \text{Fold}(cm, P), \end{cases} \quad (10)$$

where Fold hashes up the path with direction bit ($\ell \gg k$) & 1 at level k . Setup outputs public parameters only (no secrets, no ceremony).

Definition 4.2 (Proof equations). With domain $D = \text{wizm-flock-v1}$ and $\pi \in \{0, 1\}^{1792}$ (224 bytes),

$$C = H(D \parallel \text{commit} \parallel v \parallel b \parallel sk \parallel \ell \parallel P), \quad (11)$$

$$ch = H(D \parallel \text{challenge} \parallel C \parallel x), \quad (12)$$

$$E = \text{Expand}(ch, 128) = 128\text{-byte iterated-hash chain}, \quad (13)$$

$$F = H(D \parallel \text{final} \parallel \pi[0..192] \parallel x). \quad (14)$$

$\text{Verify}(x, \pi)$ recomputes ch, E, F and accepts iff all three equalities hold and $|x| = 3 \times 256$ bits.

Proposition 4.1 (Completeness and transparency). *Honest proofs verify: $\mathcal{R}(x, w) \Rightarrow \text{Verify}(x, \text{Prove}(x, w)) = 1$. Soundness rests on BLAKE3 preimage/binding resistance (post-quantum); the “PCS opening” is an expansion check rather than a low-degree test, so no succinctness beyond the fixed 224 bytes is claimed. Groth16/BN254/ Poseidon and all ceremony artifacts were removed.*

5 Transactions

Definition 5.1 (Transaction). $T = (\tau, \delta)$ with type $\tau \in \{T, S, Z_1, Z_2, D\}$ and body δ :

$$\begin{aligned} T : & \quad [from:20][to:20][v:8][n:8] \parallel pk \parallel \sigma \quad (1465-1705 B), \\ S : & \quad [snd:20][A:20][r:32][t:1][\bar{v}:32][k:32] \parallel pk \parallel \sigma \quad (1546-1786), \\ Z_1 : & \quad [nf:32][cm:32][r:32][f:20] \parallel \pi_{224} \quad (340), \\ Z_2 : & \quad header_{116} \parallel note_{857} \parallel cm_{out,32} \parallel \pi_{224} \quad (1229), \\ D : & \quad [snd:20][n:8][v:8] \parallel 857 \parallel 32 \parallel \pi \parallel pk \parallel \sigma \quad (2558-2798). \end{aligned} \tag{15}$$

$txid(T) = H(\delta)$. Admission classifies by exact length (Falcon signatures vary); the T/S overlap $[1546..1705]$ breaks by $H(pk)[0..20] \stackrel{?}{=} \delta[0..20]$.

Definition 5.2 (Validity predicate). $\text{Valid}(\sigma, T)$ holds iff type lengths are exact and:

$$\begin{aligned} T : & \quad \text{Verify}(pk, \delta[0..56], \sigma) \wedge n = A[from].nonce \wedge A[from].bal \geq v + F, \\ S : & \quad \text{Verify}(pk, \delta[0..137], \sigma) \wedge k \notin K \wedge A[snd].bal \geq v + F, \\ Z : & \quad \Pi_{\text{flock}}. \text{Verify}([nf, cm, r], \pi) \wedge nf \notin \mathcal{N} \wedge \text{VerifyRoot}(r) \wedge A[f].bal \geq F, \\ D : & \quad \text{Verify}(pk, \delta[0..925], \sigma) \wedge n = A[snd].nonce \wedge nf_0 \notin \mathcal{N} \wedge A[snd].bal \geq v + F, \end{aligned} \tag{16}$$

with uniform fee $F = 10\,000$ base units for all types.

6 State transition

Definition 6.1 (Transaction application). For $\text{Valid}(\sigma, T)$ define $\Upsilon(\sigma, T) = \sigma'$ by type. Let $(b, n) = A[a]$ and write $A[a \mapsto (b', n')]$ for the point update. With fee F :

$$\begin{aligned} T : & \quad A' = A[from \mapsto (b-v-F, n+1)][to \mapsto (b_{to}+v, n_{to})], \\ & \quad \text{failure still consumes the nonce (by design);} \\ S : & \quad A' = A[snd \mapsto (b-v-F, n)][A \mapsto (b_A+v, n_A)], \quad K' = K \cup \{k\}; \\ Z : & \quad A' = A[f \mapsto (b-F, n)], \quad \mathcal{N}' = \mathcal{N} \cup \{nf\}, \quad C' = C \parallel [cm_{out}]; \\ D : & \quad A' = A[snd \mapsto (b-v-F, n+1)], \\ & \quad \mathcal{N}' = \mathcal{N} \cup \{nf_0\}, \quad C' = C \parallel [cm_{out}]. \end{aligned} \tag{17}$$

For $\neg \text{Valid}(\sigma, T)$, Υ skips T (fee and reward paths excepted). Rewards credit every committee address and the running hash absorbs $(tag, data)$ per mutation.

Definition 6.2 (Block application). For block $B = (H, [T_1, \dots, T_k])$,

$$\Omega(B, \sigma) = \Upsilon(\sigma, T_k) \circ \dots \circ \Upsilon(\sigma, T_1), \tag{18}$$

after parallel signature/proof verification and deterministic nonce-order sorting of transparent/deposit transactions. Fees accumulate $f(B) = \sum_i \phi(T_i)$ into the burned total; while emission is active all fees burn, afterwards they split per-validator with only the remainder burned.

Proposition 6.1 (Fee conservation). *Let $S(\sigma)$ be the sum of account balances. For valid T , $S(\Upsilon(\sigma, T)) = S(\sigma) - F$ exactly (value moves, the fee leaves supply); rewards add the scheduled per-validator amount and nothing else. Invalid T move no value.*

7 Consensus mathematics

Definition 7.1 (Slot schedule). Wall time maps to slots of $T_{\text{blk}} = 10\text{s}$ with 4s grace. Height h seals no earlier than its parent's sealed timestamp plus T_{blk} (chain-time pacing: catch-up bursts cannot compress history). Fallback attempts fire on wall-clock delay (60s), so a slow mesh never triggers competing versions by itself. Epochs span 360 heights with ratified seat snapshots.

Definition 7.2 (Producer function). For height h , attempt a and committee $\mathcal{C}$, $\text{producer}(h, a, \mathcal{C}) \in \mathcal{V}$ rotates deterministically (attempt 0 round-robins the five seats; higher attempts rotate on delay). A validator seals h iff it is entitled at an attempt due by wall clock and its slot is open, unfilled, and unsuppressed below.

Definition 7.3 (Seal-suppression gates). Let m be the best mesh height sampled (with arrival time), c the last mesh contact time, u the uptime and t our tip. With staleness bound $S = 300\text{s}$, contact window $C = 900\text{s}$, settle 150s and blind cap 600s , seals wait while any holds: $u < 150$ (mesh settle); $m = \perp \wedge u < 600 \wedge t > 0$ (blind boot); $m > t + 1$ with fresh m (behind); $m > t + 1$ with stale m but c within C (flap: heard the chain, keep following, never mint stale); a fresh buffered proposal for $t + 1$ exists (first-seen, 120s); unexecuted buffers sit above t (syncing). A lagging node with recent contact therefore suppresses rather than forks; a truly-solo node seals via the blind bound.

Theorem 7.1 (Same-height convergence). *Competing versions of one height resolve by earlier seal (lower-hash tiebreak) with a one-height unwind onto the winner. The rule is strictly improving in (seal time, hash), so versions converge with no oscillation; fork evidence (a competing tip version in hand while the mesh sealed beyond) unwinds onto the mesh version, including on the sync-response path, so followers never extend forks.*

Definition 7.4 (Finality and checkpoints). Finality fast-forwards to $\text{tip} - 128$ at boot, then advances the contiguous-majority vote watermark lockstep behind the tip. Light checkpoints every 100 heights carry header ancestry only; recovery never trusts more than one checkpoint of unverified history. Snapshots export full rest-state every 2,000 heights; the rewind journal (32 depths, persisted per commit) bounds operator recovery.

Definition 7.5 (Pipelined catch-up). While the mesh leads by more than 8 heights, a node requests up to three forward 100-height windows in parallel, draining strictly in order. Windows fire on the 60s stall clock *and* whenever the lead exceeds 32 heights even without a stall (parity followers never trip the stall clock yet must still converge).

8 Mempool as a transition system

Definition 8.1 (Pool and floors). The pool holds entries $e = (s, n?, t_0)$ with sender s , optional nonce n and admission time t_0 , indexed by random IDs and mirrored in per-sender ordered sets, capped at 500 MB / 200,000 entries with 5,400s TTL. The floor map $F : \{0, 1\}^{160} \rightarrow \mathbb{N}$ stores next-expected nonces, advanced by commits (max-merge), reseeded from durable state at boot and resynced from live executor truth.

Definition 8.2 (Drain function). $\text{Drain}(M, F, k)$ scans at most $\min(16k, 4|M|)$ entries with alternating-deque fairness, threading expectation e_s per sender from $F(s)$. For nonce-bearing n vs e :

$$\left\{ \begin{array}{ll} n < e : & \text{drop (settled),} \\ n > e, \text{ stale}_{300}(e) \wedge [e, n) \cap M_s = \emptyset : & F(s) \leftarrow \min(n, \min(M_s \cap [e, \infty))), \text{ re-evaluate (jump),} \\ n > e : & \text{purge iff pressured}_{\geq 80\%} \wedge \text{trailless, else park,} \\ n = e : & \text{emit, } e \leftarrow e + 1. \end{array} \right. \quad (19)$$

Parked lanes leave the scan path (staying indexed) and unpark when F reaches their head; stale parked heads jump without rescanning. Jump-marked lanes hold until commit-grounded floors advance past the mark (live-truth overlay lets arriving refills emit head-first). At capacity, an entry with $F(s) < n \leq \max M_s$ displaces the sender's tail. Untracked entries always emit. An emptied marked lane re-grounds floor and mark on its next tracked arrival, so restart-from-truth resubmits flow; TTL-expired parked entries reap on a 60s timer without any pressure gate.

Proposition 8.1 (Drain invariants). *(i) Every purge or jump target is trailless-or-absent: no live successor is ever stranded. (ii) Each scan pops fresh entries first; held lanes cost one park per lifetime, so throughput is independent of backlog depth. (iii) With monotone odometers ($adm, rej, valve, setl, ttl, rss, tail, forf, dup, prescreen, recycled, dedup$),*

$$adm - sealed = inpool + shed, \quad (20)$$

so any silent loss is definitionally visible; live gauges expose parked entries and jump-marked lanes directly.

9 Network bounds and node operation

Definition 9.1 (Timing). Gossipsub heartbeat 1s over mesh target 4; QUIC on UDP :7778; bulk fill in 200-ID chunks over 32-height spans (8s/20s timeouts); propose tick $T_{\text{blk}} = 10$ s; sync tick 10s with 15s request cooldown; stale/view-change 15s. Proposals travel compact (header + 8-byte IDs, ≈ 9 KB per 1000 txs vs ≈ 2.5 MB full). Theoretical capacity:

$$\Theta_{\text{max}} = B_{\text{max}}/T_{\text{blk}} = 1200/10 = 120 \text{ TPS}. \quad (21)$$

Definition 9.2 (Client discipline). Submits carry Bearer API keys (writes) with a 500/s per-IP token bucket; reads are open. Validators link over TCP :7777 with per-node TLS proxies (external :8546 to local :8545) and a gRPC stub on :50051. Host firewalls pin admin faces to operators; the dashboard polls blocks every second and state every ten.

10 Supply function and genesis

Definition 10.1 (Emission). With $Y = 3\,155\,760$ blocks/year (10s slots), period length $P = 2Y$ blocks and schedule $S = (S_0, \dots, S_4)$ totalling 8 312 029 999 000 000 (22,248,474.30; 20,023,626.87; 17,020,082.84; 13,616,066.27; 10,212,049.71 WIZM), for height h let $p(h) = \min(\lfloor h/P \rfloor, 4)$. The active predicate is $h < 5P = 31\,557\,600$; per-validator reward $r(h) = S_{p(h)}/(P \cdot N)$ while active, else 0. Cumulative emission $E(h) = \sum_{j < h} N \cdot r(j)$ and *remaining*(h) = *Supply* − $E(h)$. Fees burn during emission and distribute per-validator afterwards (remainder burned).

11 Wallet backup envelope

Definition 11.1 (Vault backup). Export seals the vault under PBKDF2-SHA256 (600,000 rounds) plus AES-256-GCM in one envelope, implemented purely in each client so backups round-trip across desktop and browser builds. Eight vectors cover the envelope including cross-implementation decryption.

12 Measured performance

Definition 12.1 (Measurement). Throughput is counted from finalized chain data only: $\Theta = \sum tx_count / \Delta t$ over consecutive blocks by their deterministic timestamps. Client timeouts count separately and never as rejects; submitted and committed rates must agree.

Proposition 12.1 (Observed liveness). *All five validators hold lockstep tips (identical hashes) through 150–200 TPS bursts absorbed as honest backlog and drained in cooldown phases; full 1,200-transaction blocks execute in 0.5–4.0 s; per-node odometers reconcile offered-against-sealed totals with chain-true rejects at zero across day-scale envelopes and client timeouts held in a separate counter.*

Table 1: On-chain seal rates, October 2026 five-validator mainnet (observed ranges + derived ceiling).

Regime	Observed	TPS
Full blocks	1,200 txs sealing $\approx$ every 10 s	$\approx$ 120 (ceiling)
Sustained soak	submitted $\approx$ committed, 60–95	60–95
Single run volume	$\approx$ 4.0M committed	—
Bursts 150–200	absorbed as backlog, drained in cools	peak 150–200
Chain-true rejects	zero at $\leq$ 150 levels	0

A Constant table

Chain: $N=5$, $T_{\text{blk}}=10\text{s}$, grace 4 s, $B_{\text{max}}=1200$, epochs 360, fallback 60 s, pool 500 MB/200 k/TTL 5400 s, shed 100 k, staleness 300 s, refill 500, sweep 60 s, settle 150 s, blind 600 s, sample-stale 300 s, contact 900 s, journal 32, checkpoints 100, snapshots 2000, finality 128, bodies 4000, headers 200 k, pipeline 3×100 past lead 8, catch-up gap 32, watchdog 600 s + lead 12, purge 300 s, per-address 500 k (+500 k/30 s burst), scan $\min(16k, 4|M|)$. Crypto: Falcon 897/1281B keys, 512–690B sigs; ML-KEM-768 1184/1088/32; Flock 224B; Merkle depth 22, 64-root window. Ports 7777/7778/8545/8546/50051. Fees 10 000 uniform; supply 8 312 029 999 000 000. Tolerances: rate 500/s per IP; tombstone cap 10^5 .

B RPC reference

Tip, block, sealed header, balance, nonce, mempool stats (pending, bytes, ten shed odometers, parked/marked gauges, floor lag), tokenomics, shielded commitments/notes, chain ID, committee KEM key, gRPC raw submit, operator rewind. Reads reflect live executor truth; writes require Bearer keys.

C Code-comment errata

Stale “ML-DSA-44”/“Dilithium” labels mark Falcon-512 call sites; “ML-KEM” labels mark pre-FIPS Kyber paths (768-bit set deployed for committee/mempool); the committee KEM is N -of- N XOR despite “T-of-N” wording; isolated byte-size comments predate variable-length Falcon signatures; any “four validator”/“5 s”/ “depth 20”/“Bullshark” prose predates the production PoA. Normative values are this paper’s.

D Verification matrix

Nightly `rustfmt` clean; strict Clippy (warnings, pedantic, nursery denied) zero; 460+ unit/protocol tests including per-rule mempool, gate-matrix and pipeline regressions; live ten-day clever-random soaks (spike/drain cools, watchdog refills, freeze pauses) with odometer reconciliation and zero chain-true rejects.