Atho Consensus (Current)

Date: 2026-04-14

This document defines active consensus-enforced behavior for blocks, transactions, fee routing
and BPoW state transitions.
- Core Constants
From Src/Utility/const.py:
- Block target time: 120 seconds
- Difficulty retarget interval: 180 blocks
- Transaction confirmations required: 10 blocks
- Coinbase maturity: 150 blocks
- Max block base bytes: 3,500,000
- Max block weight: 14,000,000
- Max tx policy size (vsize): 250,000
- Fee floor: 500 atoms per policy byte (vsize)
- Min tx fee: 200,000 atoms
- Dust limit: 20,000 atoms (1/10 of min tx fee)
- Pre-tail base supply target: 400,000,000 ATHO
- Hard max supply cap: 500,000,000 ATHO
- Supply floor: 21,000,000 ATHO
- BPoW and Stake Constants
- BPoW enforcement height: 10,000 (mainnet, testnet, regnet)
- Bond requirement: 25 ATHO
- Bond activation confirmations: 25
- Bond unbond delay: 10,080 blocks
- Slash penalty: 2.5 ATHO
- Epoch length: 720 blocks
- Finalization buffer: 3,600 blocks
- Bootstrap allocation: 781,250 ATHO at block 1
- Stake minimum: 20 ATHO
- Stake max per address: 1,000 ATHO
- Stake max new entry (rolling window, network-wide): 50,000 ATHO over 21,600 blocks
- Stake max total locked (network-wide): 75,000,000 ATHO
- Stake unbond delay: 129,600 blocks (180 days)
- Stake rewards stop on unstake request: true

Primary data stores:
- bond.lmdb for miner bond lifecycle state
- stake.lmdb for wallet staking lifecycle state
- utxo.lmdb for standard spendable outputs

2.1 Deterministic Role Address Rules
Consensus role derivation is domain-separated from raw Falcon pubkey bytes:
- regular: SHA3-384("ATHO_ADDR_V1" || network || pubkey)
- bond: SHA3-384("ATHO_BOND_V1" || network || pubkey)
- stake: SHA3-384("ATHO_STAKE_V1" || network || pubkey)

Consensus does not trust user-facing string prefix alone. It validates deterministic derivatio
rules plus network role domains.

2.2 State Machines

Bond state machine:
- pending -> active -> exiting -> unlockable -> withdrawn

Stake state machine:
- pending -> active -> exiting -> unlockable -> withdrawn

Both are enforced by deterministic height and confirmation checks. No state transition is accepted if preconditions fail.
- Fee Routing and Pool Rules
- Fee uplift policy: +25%
- Fee pool routing:
- pre-tail (height < 17,000,000): 40% of total fees (20% miner-side, 20% stake-side),
- post-tail (height >= 17,000,000): 55% of total fees (25% miner-side, 30% stake-side).
- Miner-side split:
- pre-tail: 0% winner-proportional, 20% bonded-idle split (of total fees),
- post-tail: 20% winner-proportional, 5% bonded-idle split (of total fees).
- Burn policy at tail: 100% burn on routed non-pool fees (45% of total fees at post-tail routing, subject to floor clipping).

Consensus-managed pool address is deterministic and network-separated:
- mainnet: "P" + Base56(SHA3-384("ATHO_PROTOCOL_POOL_MAINNET"))
- testnet: "L" + Base56(SHA3-384("ATHO_PROTOCOL_POOL_TESTNET"))
- regnet: "L" + Base56(SHA3-384("ATHO_PROTOCOL_POOL_REGNET"))
- Transaction Consensus Path
Primary code:
- Src/Main/txveri.py
- Src/Transactions/txvalidation.py

Consensus checks include:
- canonical serialization/hash consistency,
- Falcon signature validity,
- UTXO existence + unspent state,
- no in-block or mempool double spend,
- strict integer-atom conservation,
- fee floor by canonical vsize,
- role/address consistency checks for bond/stake specific flows,
- rejection if role-targeted lockup paths do not match derived ownership semantics.

Private-layer checks are part of this path:
- private nullifier uniqueness and replay checks,
- anchor age + merkle path validation,
- note ownership/signature checks,
- product-v1 hidden-amount mode gating,
- block proof gate validation.
- Signature and Witness Rules
- Transport codec is binary (ATX2; ATX1 decode compatibility).
- Witness is processed as bytes in consensus paths.
- Falcon witness policy:
- signature bytes in 600..690 (target 666)
- pubkey bytes 897 canonical
- legacy 1024-byte pubkey acceptance is disabled by default.
- Block Consensus Path

Primary code:
- Src/Main/blockveri.py
- Src/Main/consensus.py

Block acceptance enforces:
- parent linkage and index continuity,
- PoW target validation,
- merkle/witness commitment checks,
- byte and weight limits,
- coinbase payout invariants,
- tx list validity under active tx rules,
- BPoW miner metadata checks (miner_pubkey, reward_address, miner_signature, role tag),
- active bond eligibility once BPoW is active.

6.1 Slashable vs Non-Slashable
Slashable:
- PoW-valid block that is consensus-invalid (miner proof, bond eligibility, tx validity, structure, or reward correctness).

Not slashable:
- stale/orphan valid block from honest race,
- reorged-out valid block,
- late but otherwise valid relay.

This distinction is deterministic and required for safe slashing enforcement.

6.2 Private Block-Mode TXID Rebinding
Current miner behavior includes a required canonical txid rebind step after private output block-mode conversion:
- private mempool form uses amount_plain,
- block form uses amount_commit,
- miner must recompute tx_id from canonical no-witness payload after conversion.

Code path:
- Src/Transactions/private_layer.py -> transform_v5_outputs_for_block(...)
- Src/Miner/miner.py -> _rederive_block_txid_in_place(...)

Without this rebind step, block merkle roots can drift from canonical tx content and be reject by block verification.
- Monetary Invariants
- All consensus value math is integer atoms.
- Coinbase payout must match:
- block subsidy +
- miner-routed fee share for that height.
- Hard-cap invariant: total_supply <= 500,000,000 ATHO.
- Subsidy path is clipped at coinbase so when cap headroom is exhausted:
- block subsidy becomes 0,
- fee routing/burn/pool logic remains unchanged.
- Tail-era floor clipping guarantees effective circulating supply cannot burn below 21,000,000 ATHO.
- Pool routing is consensus-accounted independently (fees_pool_atoms) and cannot be user-spent by arbitrary keys.

- Throughput Framing (Measured)
Measured tx-size profile is in Docs/Tx.md.

Using current measured vectors and policy limits (3,500,000 vB, 120s):

Flow Shape	vsize	TPS (ideal)	TPS (95% pack)
public 1 in / 2 out	553	52.74	50.11
public -> private	2471	11.80	11.21
private -> public	2708	10.77	10.23
private -> private	4673	6.24	5.93

These are policy-capacity estimates. Real throughput depends on tx mix and sustained utilization.
- Engine Independence
CPU and GPU miners are execution backends only. Consensus validity is engine-independent: a valid block verifies identically regardless of mining backend.
- Audit Snapshot (2026-04-05)
Audit artifacts generated from local sandbox runners:
- consensus attack audit: sandbox/consensus_attack_audit/reports/consensus_attack_audit_20260405_003607.json
- private attack audit (v1-updated harness): sandbox/private_tx_attack_audit/reports/private_tx_attack_audit_20260405_003824.json
- BPoW flow audit: sandbox/bpow_flow_audit/reports/bpow_flow_audit_20260405_003611.json

Observed summary:
- consensus attack audit: 15 total, 8 passed, 7 failed.
- private attack audit: 5000 total, 5000 passed, 0 failed.
- BPoW flow audit: 39 checks, 35 passed, 4 failed.

Interpretation notes:
- consensus audit failures are primarily harness expectation mismatches (baseline vector assumptions), not an accepted-invalid consensus path.
- private attack harness now targets v1 semantics and shows full pass on nullifier/anchor/repl vectors.
- BPoW failed checks are in slash-activation scenarios where the sandbox run reports bpow_inactive.
- Related Docs
- Network_Stack.md
- Tx.md
- Sigwit.md
- Falcon512.md
- Emissions.md
- WhitePaper.md