CivicNet (CIVIC) — Whitepaper
The Decentralized Community Grid

Version 1.0 — July 2026

Abstract

CivicNet is an open-source, Proof-of-Work cryptocurrency built on the Bitcoin/Litecoin Core codebase, designed around one core principle: **mining and network participation should stay accessible to ordinary people on ordinary hardware.** No ASIC farms. No GPU rigs. No minimum capital to participate in securing or earning from the network.

This document describes CivicNet's current architecture (civiclight v2, a memory-hard ASIC-resistant algorithm), its tokenomics, and its roadmap toward a Hybrid Proof-of-Work + Proof-of-Stake consensus model.

---

1. Introduction

1.1 The Problem

Most Proof-of-Work cryptocurrencies, however fairly launched, eventually converge toward mining centralization: specialized ASIC hardware or large GPU farms come to dominate block production, pushing out the individual participant with a regular computer. This undermines the original promise of decentralized, permissionless participation.

1.2 The CivicNet Approach

CivicNet takes a CPU-first stance from the ground up:

- A custom, memory-hard mining algorithm designed to resist ASIC/GPU optimization.
- No pre-sale, no ICO, no venture allocation — fair launch, with a fully disclosed 1% developer allocation.
- A roadmap toward Hybrid PoW+PoS that keeps staking open to any holder, with no minimum balance requirement.

—

2. Network Parameters

Parameter	Value
Ticker	CIVIC
Consensus	Proof of Work (Hybrid PoW+PoS planned)
Algorithm	civiclight v2 (ASIC-resistant)
Block time	1 minute
Block reward	77 CIVIC
Halving interval	2,100,000 blocks (~4 years)
Maximum supply	~315,000,000 CIVIC
Coinbase maturity	50 confirmations
Address format	Bech32 (civc1...)
P2P port	9333
RPC port	9332
License	MIT

—

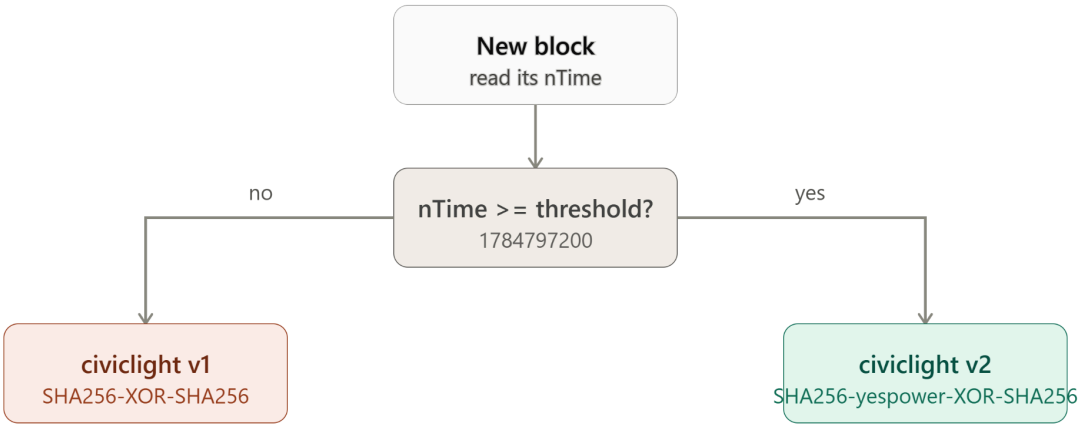
3. Mining Algorithm: civiclight

3.1 civiclight v1 (Original)

At launch, CivicNet used civiclight v1: a lightweight hashing pipeline (SHA256d → SHA256 → XOR → SHA256), chosen for being CPU-friendly in practice — no ASIC or GPU miners existed for it at launch. However, this was openly acknowledged as not cryptographically ASIC-resistant: the underlying construction was not memory-hard, meaning specialized hardware could, in principle, eventually be built for it.

3.2 civiclight v2 (Current)

To close this gap, CivicNet underwent a hard fork upgrading the algorithm to civiclight v2: SHA256 → yespower → XOR → SHA256, incorporating yespower, a proven, memory-hard hashing core, into the pipeline. This makes specialized ASIC/FPGA hardware fundamentally inefficient compared to ordinary CPUs.

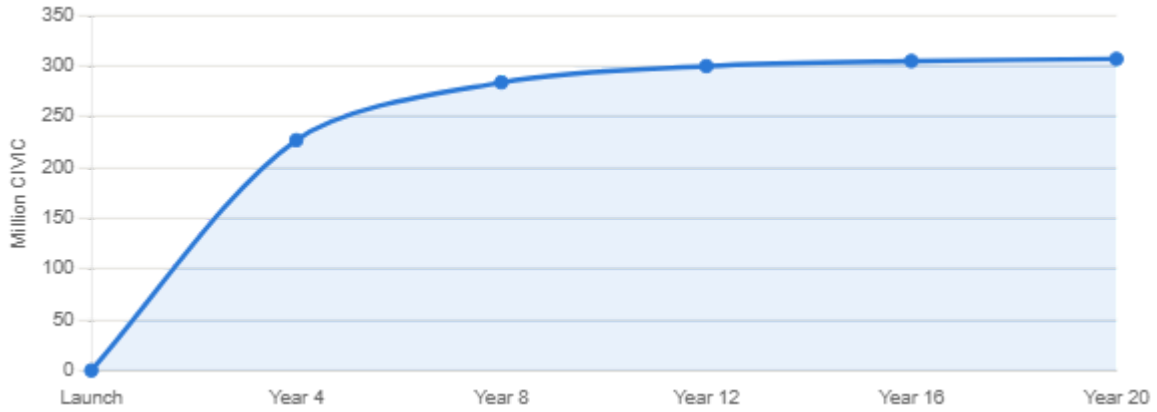


Design notes:
- The algorithm name exposed to miners and pools remains "civiclight" — yespower is an internal component, not a user-facing rename. Mining commands and pool configuration are unaffected by the algorithm upgrade.
- **Fork activation is time-based, not block-height-based.** Each block's validity is determined by its own timestamp (`nTime`): blocks with `nTime` before the activation threshold are validated under civiclight v1; blocks at or after the threshold are validated under civiclight v2. This logic was tested on testnet prior to mainnet activation, confirming correct automatic switching with no chain-split risk.
- civiclight v2 activated on mainnet **July 23, 2026, 09:00 UTC**.

---

4. Tokenomics

- **Maximum supply:** ~315,000,000 CIVIC
- **Block reward:** 77 CIVIC, halving every 2,100,000 blocks (~4 years)
- **Developer allocation:** 1% (3,150,000 CIVIC), created at block 1, publicly disclosed, reserved for core development, infrastructure (seed nodes, explorer, pool), security improvements, and community bounties.
- **No ICO, no private sale, no venture capital allocation, no hidden founder rewards, no stealth mining.** Beyond the disclosed 1% allocation, all CIVIC enters circulation through mining (and, in the future, staking rewards under the hybrid model).

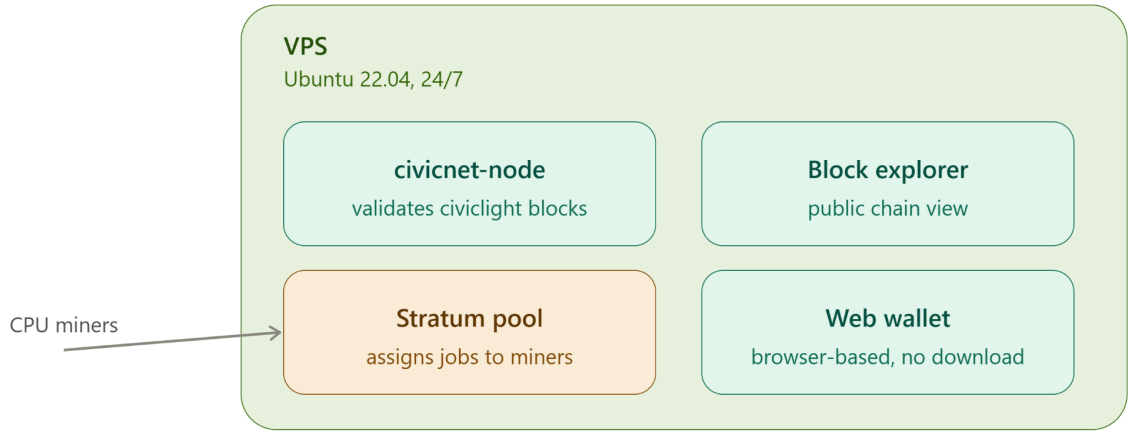


---

5. Network Infrastructure (Current State)

- **Full node / wallet:** Bitcoin/Litecoin Core-based, with Linux and Windows binaries, including a Windows GUI wallet.
- **Web wallet:** Browser-based, no download required.
- **Official mining pool:** CPU-mineable, low fee, automatic payouts.
- **Block explorer:** Public, full transaction and block history.
- **DNS seed:** Automatic peer discovery for new nodes.

All infrastructure is open source.



—

6. Roadmap: Hybrid Proof-of-Work + Proof-of-Stake

6.1 Motivation

CivicNet's long-term security model layers Proof-of-Stake on top of Proof-of-Work, rather than transitioning away from mining. This section outlines the current design direction. **As of this document's writing, this is a finalized design specification, not yet implemented in code.**

6.2 Design Philosophy

Two earlier design directions were explicitly considered and set aside:

- **A fixed 80/20 PoW/staking split with a 10 CIVIC minimum balance** (the original project blueprint) was set aside because determining staking eligibility for every wallet above the minimum would require scanning the full UTXO set in real time at the consensus layer — computationally impractical at scale.
- **Masternodes** (large fixed-collateral validator nodes) were explicitly rejected as inconsistent with CivicNet's inclusive, no-barrier-to-entry philosophy.

The chosen model is inspired by Blackcoin's Proof-of-Stake design, with CivicNet-specific improvisations.

6.3 Core Staking Rules

- **No coin age.** Only a wallet's current balance counts toward staking eligibility — coin age (rewarding coins for sitting idle longer) is deliberately excluded to prevent "accumulate, then dump" behavior.
- **No minimum balance.** Any balance, however small, is eligible to attempt staking.
- **Wallet must be online and unlocked to stake.** Staking is an active process, not passive/delegated (in this initial design).

6.4 Improvisations Beyond the Blackcoin Model

(a) Non-linear (square-root) staking odds. Rather than weighting staking probability linearly with balance (the standard approach, which tends toward staking power concentrating with large holders), CivicNet weights odds by the square root of balance:staking_weight(wallet) = sqrt(balance) A wallet with 10,000 CIVIC receives roughly 10x the staking odds of a wallet with 100 CIVIC — not the ~100x that linear weighting would give. This keeps staking meaningfully accessible to small holders.

(b) Anti-clustering rule. A minimum number of PoW blocks (N) is required between any two PoS blocks, guaranteeing PoW miners a consistent share of block production even during high staking

participation. The value of N is mathematically constrained by the PoS ratio ceiling (§6.5): N must satisfy 1/(N+1) > ceiling, so N = 2 was chosen (max sustainable PoS share ≈ 33%, above the 30% ceiling).

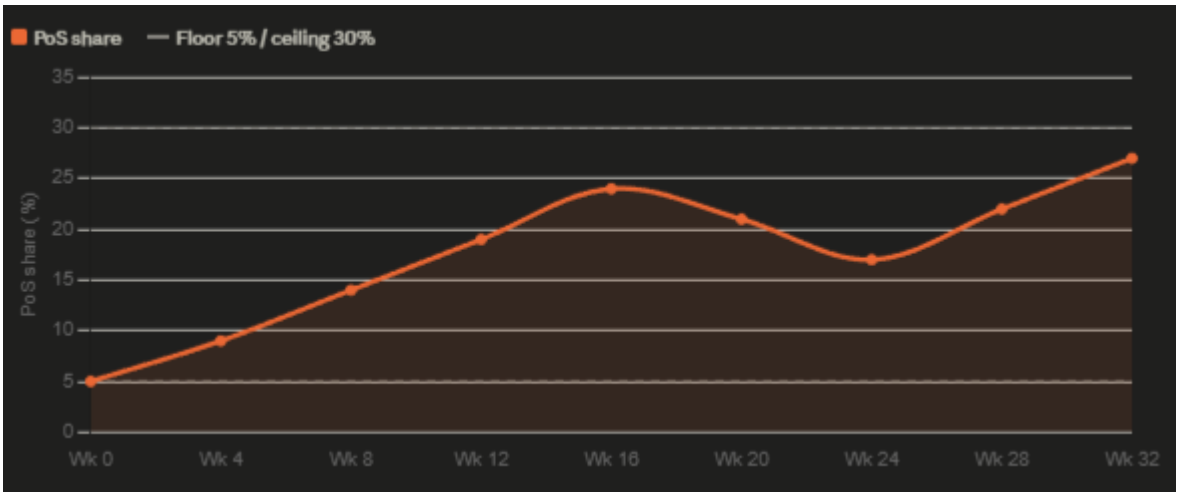
(c) Per-address stake-share caps were considered as an additional anti-centralization measure and explicitly not adopted at this stage — the square-root weighting in (a) already substantially addresses whale dominance without the added consensus-layer complexity of tracking per-address share network-wide.

6.5 Dynamic PoW/PoS Ratio

Rather than a fixed ratio or a schedule tied to halving events (both considered and set aside as too rigid), the PoW/PoS block ratio adjusts dynamically based on actual network participation:

Parameter	Value
Starting ratio	95% PoW / 5% PoS
Evaluation window	~10,080 blocks (~1 week)
Adjustment step	±1–2 percentage points per window
Floor	5% PoS (never lower than launch)
Ceiling	30% PoS (PoW never drops below 70%)

Each window, the network compares the number of PoS blocks actually found against the number targeted by the current ratio. Over-delivery shifts the ratio toward more PoS; under-delivery shifts it back toward PoW. This ties network security composition to real participation rather than an arbitrary timeline.



6.6 Reward Distribution

The full block reward for a given block goes entirely to whichever consensus type produced it: a PoW block's reward goes entirely to the mining miner; a PoS block's reward goes entirely to the staker. There is no per-block split between the two. Total emission continues to follow the existing halving curve unchanged — only the recipient alternates by block type, keeping the reward mechanism simple.

6.7 Consensus Specification (Technical Summary)

Kernel hash (staking win condition):hash(kernel) < target × sqrt(balance)

kernel = Hash(stakeModifier, txPrev.blockTime, txPrev.offset, txPrev.vout.n, nTimeTx)
nTimeTx (the PoS analog to a PoW nonce) must be greater than the current time and a multiple of a fixed timestamp mask (e.g. 8 seconds), bounding the search space similarly to Peercoin's approach, scaled to CivicNet's 1-minute block time.

Block type marking: a dedicated `nVersion` bit flags a block as Proof-of-Stake, in addition to (and validated against) a mandatory coinstake transaction structure — the flag alone is not trusted without a matching valid transaction.

Coinstake transaction structure (always the second transaction in a PoS block):
- `vin[0]`: the staker's UTXO (kernel input)
- `vout[0]`: empty (value 0, empty script) — mandatory coinstake marker
- `vout[1]`: the staker's original balance plus block reward
- `vout[2]` (optional): stake splitting, dividing large outputs to prevent unbounded UTXO growth on a single address

Stake modifier (prevents grinding attacks): recomputed every H blocks (H = 120, ≈2 hours) using a fully deterministic rule — no candidate "selection," pure arithmetic on chain state, so all fully-validating nodes independently compute an identical value:
reference_height = current_boundary_height − k (k = 30 blocks, ≈30 min)
reference_hash = hash of the block at reference_height
new_modifier = SHA256(previous_modifier || reference_hash || reference_height)

The initial (genesis) stake modifier is derived from the genesis block itself (hash of genesis block hash + genesis time), rather than a manually hardcoded constant, so testnet and mainnet automatically receive distinct, independently-verifiable initial values.

6.8 Open Items

The following remain undecided pending further design work and are explicitly flagged as such:
- Exact reward-split mechanics interaction with stake splitting (§6.7).
- Full testnet rollout timeline.
- Whether delegated/pooled staking for offline wallets is ever introduced (out of scope for the initial design).

This is a consensus-changing hard fork and will not be deployed to mainnet until extensively validated on a public testnet.

---

7. Security Considerations

- The dynamic PoW/PoS ratio (§6.5) introduces more consensus-layer complexity than a fixed schedule would; this trade-off was made deliberately in favor of responsiveness to real participation, and should be weighed carefully during implementation and audit.
- Stake modifier and kernel hash design follow patterns proven in Peercoin and Blackcoin; CivicNet's implementation should be built by directly studying and adapting their audited approaches rather than designing grinding-resistance mechanisms from scratch.
- As with the civiclight v2 hard fork, any consensus change of this scope requires public testnet validation, with the network given advance notice, before any fork activation height or time is set.

---

8. Conclusion

CivicNet's design consistently prioritizes accessibility over exclusivity — from a memory-hard, ASIC-resistant mining algorithm, to a transparent fair-launch token model, to a staking design with no minimum balance and whale-resistant weighting. The project's next major milestone, Hybrid PoW+PoS, extends this philosophy into network security itself, aiming to keep both mining and staking meaningfully open to any participant with ordinary hardware and any amount of CIVIC.

Disclaimer

This document describes CivicNet's current implementation (Section 3–5) and a finalized design direction not yet implemented in code (Section 6). It is not financial advice and makes no guarantee of future value, adoption, or exchange availability. CivicNet is experimental software provided as-is.