Ethcoin (ETHC)

Whitepaper

Proof-of-Participation Mining on Ethereum

v1.0 -- March 2026

Ethcoin brings the simplicity and scarcity model of Bitcoin mining to Ethereum as a smart contract. By leveraging EIP-4788 beacon roots for verifiable randomness and a halving emission schedule, it provides a fair, permissionless, and gas-only mining experience for any Ethereum user.

1. Abstract

Ethcoin is an ERC-20 token on Ethereum that reintroduces proof-of-participation mining to the post-Merge ecosystem. Users mine by submitting on-chain transactions, and a single winner is selected per block using verifiable randomness from the EIP-4788 beacon chain. With a hard cap of 21 million ETHC and a halving schedule, Ethcoin creates a Bitcoin-like scarcity model natively on Ethereum.

2. Problem

Since Ethereum's transition to proof-of-stake, there is no longer a way for everyday users to "mine" and earn tokens through direct participation. Ethcoin fills this gap with a simple, permissionless mining mechanism that anyone with an Ethereum wallet can join.

3. Mechanism

3.1 Mining

Anyone can call mine(mineCount) on the Ethcoin contract. Each call records the caller as a mining participant for the next Ethcoin block. A user may submit up to 200 mine entries per transaction -- more entries means a higher probability of being selected as the block winner.

Mining is free. There is no cost beyond the Ethereum gas fee for the transaction itself.

3.2 Block Production

Ethcoin maintains its own block counter, independent of Ethereum's. A new Ethcoin block is concluded every 1 minute. When a block concludes:

- The block number advances.
- All mining entries from the previous block are sealed.
- A winner is selected from the sealed block.

3.3 Winner Selection (Randomness)

A single miner is selected per block using on-chain randomness. The primary source is the EIP-4788 beacon root -- the beacon chain block root at the first slot after the Ethcoin block was concluded. This value is:

- Unknown at commit time -- miners cannot predict or influence it when submitting entries.
- Deterministic at reveal time -- the same winner is selected regardless of when settlement occurs.

If the beacon root is unavailable (missed slot or buffer expiry), the contract falls back to prevrandao combined with blockhash.

The winning index is calculated as randomNumber mod totalMineCount, and the miner who owns that index receives the block reward.

4. Reward & Supply

Parameter	Value
Max Supply	21,000,000 ETHC
Initial Block Reward	200 ETHC
Halving Interval	~1 week (10,080 blocks)
Block Time	1 minute

After each halving, the reward is cut in half and the interval until the next halving doubles -- mirroring Bitcoin's disinflationary curve. Once total supply reaches 21 million, no further tokens are minted.

4.1 Halving Schedule

Era	Reward	Interval (blocks)	Cumulative Blocks
1	200 ETHC	10,080	10,080
2	100 ETHC	20,160	30,240
3	50 ETHC	40,320	70,560
4	25 ETHC	80,640	151,200
5	12.5 ETHC	161,280	312,480
...	...	...	...

5. Architecture

The Ethcoin system consists of three contracts deployed on Ethereum mainnet:

- Ethcoin (UUPS Proxy) -- The core ERC-20 token with mining logic, upgradeable via OpenZeppelin's UUPS proxy pattern.
- EthcoinStorage -- A separated storage contract ensuring upgrade safety and clean storage layout across implementation versions.
- EthcoinLens -- A read-only helper contract exposing network stats (mining reward, block number, total supply, next halving) and user balances for frontend applications.

6. Properties

- Permissionless -- No staking, no whitelist. Anyone can mine.
- Fair -- Winner selection uses beacon chain randomness, not miner-controllable values.
- Simple -- One function call to participate. No off-chain computation or specialized hardware.
- Scarce -- Hard-capped at 21M with a halving schedule that progressively reduces emission.

7. Conclusion

Ethcoin brings the simplicity and scarcity model of Bitcoin mining to Ethereum as a smart contract. By leveraging EIP-4788 beacon roots for verifiable randomness and a halving emission schedule, it provides a fair, permissionless, and gas-only mining experience for any Ethereum user.

The protocol requires no oracles, no off-chain infrastructure, and no governance. It is fully on-chain, fully autonomous, and open to everyone.