Aethercoin: A Peer-to-Peer Electronic Cash System

Aethercoin Network
www.aether-coin.asia

Abstract. *Aethercoin (AEC) is a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution. Aethercoin adapts the proof-of-work, timestamp-chain approach first described for Bitcoin to solve the double-spending problem without a trusted third party. The network timestamps transactions by hashing them into an ongoing chain of SHA-256 proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain serves both as proof of the sequence of events witnessed and as proof that it came from the largest pool of CPU power on the network. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, honest nodes will generate the longest chain and outpace attackers. Aethercoin further extends this model with a fixed 21,000,000 AEC supply, a fair, no-pre-mine genesis, and a native liquidity bridge that allows AEC to be represented as a wrapped token on EVM-compatible smart-contract platforms for use in decentralized finance.*

1. Introduction

Commerce on the internet relies almost exclusively on financial institutions and custodial exchanges serving as trusted third parties to process electronic payments. This model works well enough for everyday transactions, but it inherits the structural weaknesses of any trust-based system: transactions can be reversed, mediation raises costs, and small, casual, or cross-border payments become impractical. Users must trust an intermediary not to freeze funds, censor transactions, or become a single point of failure.

Aethercoin proposes an electronic payment system based on cryptographic proof instead of institutional trust, allowing any two willing parties to transact directly with one another. Building on the timestamp-server and proof-of-work design that Bitcoin introduced in 2008, Aethercoin uses a peer-to-peer network to generate computational proof of the chronological order of transactions. The resulting ledger is secure as long as honest nodes collectively control more hashing power than any cooperating group of attackers.

2. Transactions

An Aethercoin coin is defined, as in the Bitcoin design, as a chain of digital signatures. Each owner transfers a coin to the next owner by digitally signing a hash of the previous transaction together with the public key of the next owner, and appending this signature to the coin. A payee can verify the chain of ownership by checking the signatures back to the coin's origin.

To prevent an owner from signing away the same coin to two different recipients (double-spending) without relying on a central mint, the network must have a single agreed-upon record of which transaction was received first. Aethercoin transactions are broadcast publicly, and the peer-to-peer network reaches consensus on their ordering through the block-chain and proof-of-work mechanism described in the sections below.

3. Timestamp Server

Aethercoin implements a distributed timestamp server: each block contains a hash of the block of transactions being timestamped together with the hash of the previous block, forming an ongoing chain. Each additional block reinforces every block that came before it, so that altering a past transaction would require recomputing every block after it.

4. Proof-of-Work (SHA-256)

Aethercoin uses SHA-256 as its proof-of-work hashing function, the same function used by Bitcoin. Miners repeatedly vary a nonce in a candidate block until the resulting SHA-256 hash begins with a network-defined number of leading zero bits. Verifying a completed proof-of-work requires a single hash computation, while producing one requires, on average, an amount of work that grows exponentially with the required number of zero bits.

Proof-of-work resolves the question of how to weight participation in majority decision-making across an open, permissionless network: rather than one-IP-address, one-vote — which can be subverted by anyone able to allocate many addresses — Aethercoin is effectively one-CPU-cycle, one-vote. The chain with the greatest cumulative proof-of-work is treated by all nodes as the valid history. To rewrite a past block, an attacker would need to redo the proof-of-work for that block and every block after it, and then overtake the combined hash rate of the honest network — a task whose probability of success falls off exponentially with each additional confirmation, as shown in Section 11 of the original Bitcoin analysis, which applies unchanged to Aethercoin's identical consensus mechanics.

To keep block production stable as network hash rate changes over time, Aethercoin retargets proof-of-work difficulty on a rolling basis to hold the average block interval at approximately 10 minutes.

5. Network

- New transactions are broadcast to all nodes on the network.
- Each node collects pending transactions into a candidate block.
- Each node works on finding a valid proof-of-work for its candidate block.
- When a node finds a valid proof-of-work, it broadcasts the block to the network.
- Nodes accept a block only if every transaction in it is valid and unspent.
- Nodes signal acceptance by beginning work on the next block, using the accepted block's hash as the new previous-hash.

Nodes always treat the longest valid chain as authoritative and continue extending it. If two blocks are broadcast at nearly the same time, nodes work on whichever they received first while retaining the other branch; the fork is resolved once a subsequent block extends one branch further, at which point nodes converge on the longer chain. Transaction and block propagation are both best-effort and tolerant of dropped messages, and nodes that fall behind simply request missing blocks upon rejoining.

6. Incentive and Monetary Policy

By convention, the first transaction in each Aethercoin block is a special coinbase transaction that mints new AEC to the address of the block's finder. This is the sole mechanism by which new coins enter circulation — Aethercoin has no pre-mine and no founder or developer allocation. Every unit in circulation is understood to have been earned through proof-of-work, consistent with the project's fair-launch design.

Aethercoin's total supply is capped at 21,000,000 AEC. As with Bitcoin, the per-block coinbase reward is halved at fixed intervals (every 210,000 blocks, or roughly four years at the 10-minute target block time) until the full supply has been issued, after which miner incentives transition entirely to transaction fees. This fixed, disinflationary issuance schedule is a policy choice intended to make long-term supply predictable and resistant to arbitrary expansion.

The incentive structure is also designed to keep rational miners honest: a miner controlling a majority of network hash power stands to gain more by collecting block rewards and fees under the existing rules than by attempting to defraud the network and undermine confidence in the asset it is simultaneously mining.

7. Mining Accessibility

A stated design goal of Aethercoin is to keep block production accessible to consumer-grade CPU and GPU hardware rather than concentrated in specialized ASIC hardware, so that mining — and therefore initial coin distribution — remains broadly decentralized. Operators should note that this goal is a policy and tuning objective rather than an inherent property of the SHA-256 function itself, since SHA-256 is the same algorithm used by Bitcoin's ASIC-dominated mining industry; maintaining practical ASIC resistance typically requires either a different memory-hard hash function or an explicit, published difficulty/algorithm adjustment strategy, which the Aethercoin project intends to document in an accompanying technical specification.

8. Reclaiming Disk Space

Once a transaction is buried under enough confirmations, the spent transactions preceding it can be discarded to save storage. Aethercoin blocks hash their transactions into a Merkle tree, with only the root included in the block header, so that old transaction data can be pruned without invalidating the block's hash. A network of lightweight, header-only nodes can therefore participate in verification without storing the full transaction history.

9. Simplified Payment Verification

A wallet does not need to run a full node to verify payments. By retaining only block headers of the longest proof-of-work chain and requesting the Merkle branch linking a given transaction to the block that contains it, a lightweight client can confirm that a network node accepted the transaction, with each subsequent block adding further confirmation. This method is reliable as long as honest nodes control the network, but merchants processing frequent or high-value payments are encouraged to run a full Aethercoin node for stronger, independent verification.

10. Privacy

As with Bitcoin, Aethercoin's transaction graph is public by design — every node can see that a given amount moved from one address to another — but privacy is preserved by keeping public keys unlinked to real-world identity. Users are encouraged to generate a new address for each incoming transaction to limit the ability of outside observers to link payments to a single owner, keeping in mind that multi-input transactions necessarily reveal common ownership of their inputs.

11. EVM Liquidity Bridge

To support use within existing decentralized finance ecosystems, Aethercoin includes a bridge mechanism through which native AEC can be locked on the Aethercoin chain in exchange for minting a corresponding wrapped representation on EVM-compatible smart-contract platforms, and burned on those platforms to unlock native AEC in return. This allows AEC liquidity to be used in external smart-contract applications while the underlying supply continues to be secured by Aethercoin's own proof-of-work chain. Bridge custody, validator set, and unlock conditions are implementation details that should be fully specified and independently audited in a companion technical document before the bridge is relied upon for meaningful value.

12. Conclusion

Aethercoin applies the peer-to-peer, proof-of-work timestamp chain first demonstrated by Bitcoin to a fixed-supply, fairly-launched digital currency with an added bridge to EVM-based decentralized finance. Nodes require no coordination beyond the protocol itself: transactions and blocks are broadcast on a best-effort basis, and any node can leave and rejoin the network, catching up simply by accepting the longest valid proof-of-work chain as the record of what took place in its absence. Participants express their agreement with the rules by extending valid blocks and rejecting invalid ones, and this consensus mechanism is sufficient to enforce Aethercoin's supply schedule and transaction rules without a central authority.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. The consensus design in this paper is directly adapted from Nakamoto's original proposal.

[2] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[3] A. Back, "Hashcash – a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[4] R.C. Merkle, "Protocols for public key cryptosystems," Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, 1980.