SYNTHOS Collective Protocol

An agent-native Layer-1 blockchain for permissionless computation and data sovereignty.

Abstract

SYNTHOS Collective is a Layer-1 blockchain engineered for a world of autonomous agents. It provides a neutral, permissionless substrate where agents and humans can transact, coordinate, and store data without gatekeepers. The protocol combines Ed25519 cryptographic identity, a 2/3 Byzantine fault-tolerant consensus, and a novel serverless immune node tier that patrols the network at near-zero operating cost.

1. Architecture

The network is composed of two cooperating node classes running over a shared bulletin-board transport. Rather than requiring open listening ports, nodes poll a replicated bulletin board (an R2-backed object store) on a fixed cadence, exchanging signed messages. This portless topology lets nodes run in serverless environments such as Cloudflare Workers, dramatically lowering the cost and complexity of participation.

2. Cloudless Serverless Mesh

SYNTHOS runs as a cloudless serverless mesh: there is no central server, load balancer, or always-on host. Every node is an ephemeral, scheduled worker that wakes on a trigger, does its work, and sleeps again. The mesh has no single point of failure and no address to attack — participants coordinate purely through the shared, replicated bulletin board.

Silent Outbound Polling

Nodes never expose an inbound port. Instead they use silent outbound polling: each node reaches out to the bulletin board on its own cadence, pulls the latest signed messages, verifies them, and pushes its own signed updates. Because all traffic is outbound, nodes remain invisible to inbound scanners, survive behind NAT and firewalls, and are effectively un-DDoSable — there is nothing listening to flood.

3. Merkle State Tree

All protocol state is committed to a Merkle tree. Each block carries a Merkle root that cryptographically fingerprints the entire state; any tampering with a leaf changes the root and is instantly detectable. This lets lightweight immune nodes verify inclusion and integrity with compact Merkle proofs — confirming a fact about the chain without downloading the whole state. The Merkle structure is the backbone of the immune system.

4. Consensus

Blocks are finalized under a 2/3 Byzantine fault-tolerant threshold: as long as fewer than one-third of staked validators are faulty or malicious, the chain reaches deterministic finality. Each validator signs proposals and votes with its Ed25519 key; aggregated signatures constitute proof of finalization that any observer can verify independently.

5. Node Types

Validator Nodes

Validators stake into the protocol, produce and sign blocks, and participate in consensus voting. They are the economic backbone of the network and are rewarded for honest, live participation.

Immune Nodes

Immune nodes are lightweight, serverless watchdogs. They continuously poll the bulletin board, cross-check validator behavior against Merkle proofs, detect equivocation and anomalies, and raise quarantine signals against bad actors. Because they run on scheduled serverless triggers, they cost effectively $0/month to operate.

6. Identity & Security

Every node is provisioned with a fresh Ed25519 keypair. The public key is its network identity; the private key never leaves the operator. All protocol messages are signed, making impersonation cryptographically infeasible. Deployment tooling generates identities server-side and surfaces the private key exactly once, encouraging secure custody from the first moment.

7. Tokenomics

The native asset aligns incentives across both node tiers. Validators stake to earn block rewards and fees; immune nodes earn bounties for correctly identifying and quarantining misbehavior. Low operating costs and open participation drive decentralization that no single entity can capture — the core guarantee behind data sovereignty.