

POP CHAIN

A Decentralized Layer-1 Blockchain Powered by Hybrid Proof-of-Participation (PoP), Byzantine Fault Tolerance, and Smartphone Node Democracy.

Solving the blockchain trilemma through high-speed BFT block finality combined with permissionless, zero-battery mobile Proof-of-Participation mining.

Core Consensus Architecture

Tri-Consensus Paradigm: Delegated Proof-of-Stake (PoS) + 2/3+ Supermajority BFT Finality Gadget + Mobile Proof-of-Participation (PoP) Layer.

Chain ID	Total Supply Cap	Target Block Time	Publication Date
7070 (EVM Compatible)	10,000,000,000 POP	3.0 Seconds	October 2026

1. Executive Summary & Vision

Since the inception of Bitcoin in 2008, public distributed ledger technology has struggled with the fundamental **Blockchain Trilemma**: achieving decentralization, security, and scalability simultaneously without making severe compromises.

- **Proof-of-Work (PoW)**: Relies on brute-force thermodynamic computation. While secure, it requires gigawatts of electricity, demands expensive specialized ASIC hardware, and has concentrated hashrate into a handful of centralized mining pools.
- **Proof-of-Stake (PoS)**: Solves the energy dilemma but frequently leads to *wealth concentration* (*plutocracy*). Only wealthy token holders who can afford tens of thousands of dollars in staking capital or high-availability server racks can participate as validators.
- **Mobile Nodes (The Untapped Frontier)**: Over 6.5 billion people worldwide own smartphones. Until now, mobile devices have been relegated to passive wallet viewers because running a full node on a smartphone drains battery, exhausts RAM, and overheats processors within hours.

POP Chain solves this by architecting a **Hybrid Tri-Consensus Layer-1** blockchain. High-availability validators provide high-throughput block production and EVM state execution with instant 3-second BFT finality, while millions of smartphones participate directly in network consensus through **Proof-of-Participation (PoP)**—earning token rewards without consuming excessive battery or processing power.

2. Technical Architecture & Workspace Components

POP Chain is engineered as an asynchronous, highly modular Rust workspace running on the Tokio runtime. Each protocol layer is separated into isolated crates to ensure fault isolation, formal verifiability, and extreme execution performance.

Crate Module	Responsibility	Implementation Details
<code>pop-state</code>	State Ledger	Account balances, nonces, code storage, and Merkle Patricia State roots.
<code>pop-crypto</code>	Cryptography	Ed25519 node identities, Keccak-256 / SHA-256 hashing, secp256k1 EVM signatures.
<code>pop-consensus</code>	Consensus Orchestrator	Coordinates PoS validator rotation, BFT rounds, and PoP proof ingestion.
<code>pop-pos</code>	Validator & Staking	Validator registry, pool delegation, slashing rules, and unbonding queues.

Crate Module	Responsibility	Implementation Details
<code>pop-pop</code>	Participation Engine	Mobile node challenges, proof verification, scoring basis points, and probation.
<code>pop-finality</code>	BFT Finality Gadget	2-phase voting (Pre-vote & Pre-commit) for deterministic single-slot finality.
<code>pop-evm</code>	Smart Contract Engine	Full EVM compatibility (Solidity/Vyper bytecode execution) with state rollbacks.
<code>pop-network</code>	P2P Networking	Libp2p gossipsub protocol, Kademlia DHT peer discovery, block syncing.
<code>pop-rpc</code>	JSON-RPC 2.0	EVM web3 endpoints (<code>eth_*</code>) and proprietary PoP methods (<code>pop_*</code>).

3. The Hybrid Tri-Consensus Protocol

POP Chain decouples **Block Production & Finality** from **Decentralized Network Participation**. This separation allows the network to process high volumes of transactions with sub-second responsiveness without compromising the democratic distribution of rewards.

3.1. Layer 1: Block Production (PoS + BFT)

Validators stake POP tokens (or accept delegated Node Fractions) to enter the active validator pool. Blocks are produced every **3.0 seconds** using a deterministic round-robin leader election weighted by effective stake.

- **BFT Finality Gadget:** Proposed blocks undergo two rounds of voting:
 1. **Pre-Vote:** Validators broadcast pre-votes once block validity and state transitions are verified.
 2. **Pre-Commit:** Once a validator collects $>\frac{2}{3}$ pre-votes, it issues a pre-commit vote.
- **Zero Reorganizations:** A block with $>\frac{2}{3}$ pre-commit signatures achieves immediate deterministic finality. Forking is mathematically impossible under honest supermajority assumptions.

3.2. Layer 2: Proof-of-Participation (PoP) for Mobile Nodes

Mobile nodes participate by submitting cryptographic proofs that verify node identity, network uptime, and protocol compliance. Instead of continuous heavy computation, nodes respond to **Heartbeat V1** challenges derived deterministically from the latest finalized block hash.

The Inactivity Boundary

An epoch spans **1,200 blocks (~1 hour)**. If a mobile node does not submit a proof for greater than 3,600 seconds, its status transitions to **Inactive**. Upon submitting a new proof, its status immediately recovers to **Active** and mining resumes.

3.3. Mobile Node Hardware & Energy Profile (Zero-Battery Design)

Traditional cryptocurrency mining (such as Bitcoin SHA-256 or Monero RandomX) executes unconstrained hashing loops that pin device CPU/GPU utilization at 100%. On a mobile device, this results in rapid thermal runaway, severe CPU throttling, battery degradation, and complete battery depletion within 1 to 2 hours.

POP Chain replaces brute-force computation with **event-driven Proof-of-Participation**:

- **Micro-Execution Duty Cycle:** The mobile node sleeps for 300 seconds (5 minutes). Upon waking, it executes a single SHA-256 challenge hash and Ed25519 signature verification taking **< 5 milliseconds** of CPU time before returning to deep sleep. The active duty cycle is less than **0.002%**.

- **Negligible Battery Consumption:** Benchmarks across mid-tier and flagship Android devices demonstrate total 24-hour battery consumption of **less than 0.2%** of standard 4,000–5,000 mAh battery capacity.
- **Zero Thermal Emission:** The smartphone operates strictly at ambient temperature with 0°C thermal delta, completely preserving lithium-ion battery health and lifespan.
- **Minimal Bandwidth Footprint:** Each participation proof is an HTTP JSON-RPC payload of approximately 180 bytes. Running continuously for 24 hours (288 heartbeats) consumes only **~50 KB of data per day**, ensuring complete compatibility with low-bandwidth mobile cellular networks.
- **Android Foreground DataSync Resiliency:** Implemented via `NodeForegroundService` with `FOREGROUND_SERVICE_TYPE_DATA_SYNC` and `BOOT_COMPLETED` intent receivers, ensuring reliable continuous execution without being terminated by Android 14+ Doze Mode or aggressive OEM battery optimizers.

3.4. Uptime Policy & Zero-Penalty Offline Fault Tolerance

A fundamental distinction in POP Chain is the operational separation between **Server Validators** and **Mobile Edge Nodes**:

Attribute	Core Server Validators (AWS / Cloud)	Mobile Light Nodes (Android App)
24/7 Uptime Requirement	Strictly Mandatory (99.9%+ SLA)	Optional & Flexible (Participate at will)
Offline Consequence	Slashing penalties, probation, jailed validator status	Zero Penalties / Zero Slashing
Wallet Balance Impact	Potential stake forfeiture for double-signing/downtime	100% Protected (Earned funds never deducted)
Mining State on Disconnect	Loss of active block proposal slots	Mining gracefully pauses; resumes instantly on reconnect
Optimal Incentive	Maintain continuous block finality	Earn up to 1.00 POP/day & achieve 100.0 PoP Score

Mobile nodes are never penalized for going offline, entering airplane mode, experiencing battery depletion, or losing cellular connectivity. When a node disconnects, proof submittals pause; the moment the device reconnects to Wi-Fi or cellular data, the node immediately transmits its fresh heartbeat and resumes reward accrual without probationary delay. Users who maintain 24/7 connectivity maximize their daily token accrual ($288 \text{ proofs} \times 0.0417 \text{ POP} = \sim 1.00 \text{ POP/day}$ in Genesis) and steadily build their PoP score to the maximum threshold of 100.0 (+0.5 per verified proof).

3.5. Mathematical PoP Scoring Formula

Each node maintains an integer score (from \$0.0\$ to \$100.0\$) evaluated on every epoch boundary using five orthogonal dimensions:

$$PoP\ Score = 0.30 \times A + 0.25 \times V + 0.20 \times R + 0.15 \times Q + 0.10 \times H$$

- **Availability (\$A\$):** Ratio of verified challenge responses to issued assignments.
- **Verification (\$V\$):** Successful verification of light state proofs and transaction receipts.
- **Relay (\$R\$):** P2P propagation of validated mempool transactions.
- **Quality (\$Q\$):** Protocol response timeliness and network latency metrics.
- **History (\$H\$):** Longevity and consistent active epoch count since node genesis.

4. Node Fractions: Democratic Staking Pools

Traditional validator staking requires millions of native coins, barring everyday users from earning staking yields. POP Chain introduces **Node Fractions** as an on-chain native primitive.

Fractions	POP Staked	Validator Pool Capacity Equivalent
1 Fraction	1,000 POP	0.01% (Minimum delegation unit)
10 Fractions	10,000 POP	0.10%
100 Fractions	100,000 POP	1.00%
1,000 Fractions	1,000,000 POP	10.00%
10,000 Fractions	10,000,000 POP	100.00% (Full Validator Capacity)

Supply Invariant Protection

Creating, staking, or delegating Node Fractions does **NOT** mint new POP tokens. Tokens are locked in protocol-verified staking vaults. Total circulating supply strictly respects the 10 Billion hard cap.

5. Tokenomics: 10 Billion POP Allocation & Emission Curve

The native token of POP Chain is **POP** (18 decimals). The supply is strictly hard-capped at **10,000,000,000 POP (10 Billion)** with deflationary burn mechanisms for gas fees.

5.1. Macro Economics & Maximum Supply

- **Token Name:** POP (18 Decimals)
- **Total Max Supply:** 10,000,000,000 POP (10 Billion Hard Cap)
- **Target Block Time:** 3.0 Seconds (28,800 blocks per day)
- **Max Protocol Emission:** 200 POP per block
- **Deflationary Engine:** 20% of all Gas Fees are permanently burned.

5.2. The Final 10 Billion POP Allocation

Unlike traditional blockchains that rely on smart contracts for emissions, the POP Chain allocates 70% of its total supply directly to a **Native Consensus & Mining Vault** hard-coded into the core Rust protocol. This guarantees zero smart-contract vulnerability risk and 100% Layer-1 sovereignty.

- **70% — Native Consensus & Mining Vault (7,000,000,000 POP):**
 - **98% to Mobile PoP Treasury:** Pays exactly **2 POP per day** to every active Node Fraction. Any unneeded daily allowance is dynamically "**skipped**" (**left unminted**) to permanently prevent inflation.
 - **2% to Validator Treasury:** Pays exactly **4 POP per block** to the physical server Node Operators.
- **10% — Exchange Liquidity (1,000,000,000 POP):** Locked for DEX (PancakeSwap/Uniswap) and Tier-1 CEX market making.
- **5% — Ecosystem & Grants (500,000,000 POP):** Incentives for developers to build dApps and protocols on POP Chain.
- **5% — Treasury DAO (500,000,000 POP):** Community-governed vault for future network upgrades and marketing.
- **5% — Community Airdrop (500,000,000 POP):** Testnet participant rewards and viral user acquisition campaigns.
- **3% — Core Team (300,000,000 POP):** Founders and core engineers (Subject to a 4-year linear vesting lock).
- **2% — Genesis Backers (200,000,000 POP):** Early ecosystem bootstrappers (Subject to a 3-year vesting lock).

5.3. The 3 Pillars of Absolute Scarcity

1. **The "Skip" Minting Rule:** The blockchain is not forced to print all 200 POP per block. The protocol natively counts active fractions and *only* mints what is owed (2 POP per fraction). The rest of the allowance is skipped, meaning the circulating supply only grows in lockstep with real network adoption.
2. **The Fraction Bonding Curve:** The cost to join the network starts at 1,000 POP and mathematically **doubles every 200,000 fractions**. All POP spent buying fractions is recycled natively back into the Mobile Treasury to sustain the network.
3. **The 1.03M Hard Cap:** Because of the escalating fraction cost, if every single POP token was spent buying fractions, the entire 10 Billion supply would run out at exactly **Fraction #1,031,222**. This creates a mathematical ceiling that guarantees permanent, untouchable scarcity for early adopters.

5.4. Native Protocol Integration (No Smart Contracts)

The 30% genesis allocation (Liquidity, DAO, Team, etc.) is handled entirely without smart contracts. Vesting is enforced by **Native Protocol Timelocks** at the state level (nodes natively reject transactions before unlock blocks). Governance is handled by a native `VoteTx` module, ensuring zero EVM-exploit risk and gasless state distribution.

7. Cryptographic Security & Anti-Sybil Architecture

Security on POP Chain is architected through a multi-tiered cryptographic model that balances immediate, frictionless interoperability with the broader Ethereum/EVM ecosystem against rigorous forward-looking cryptographic risk management and post-quantum preparedness.

7.1. Standardized EVM Key Derivation & Address Mechanics

All user wallets and node addresses generated within the POP Chain ecosystem strictly conform to universal Ethereum Improvement Proposals (EIPs) and Bitcoin Improvement Proposals (BIPs), guaranteeing complete plug-and-play compatibility with industry hardware and software wallets (e.g., MetaMask, Trust Wallet, Ledger, Trezor):

- **Entropy & Canonical BIP-39 Mnemonics:** Wallet creation utilizes a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) to sample 128 bits of high-entropy randomness (\$E\$). A 4-bit checksum ($\text{SHA256}(E)[0..3]$) is appended to yield a 132-bit bitstring, partitioned into 12 distinct 11-bit chunks mapped against the canonical 2,048-word English BIP-39 dictionary.
- **PBKDF2 HMAC-SHA512 Seed Generation:** The 12-word mnemonic is transformed into a 512-bit binary master seed using PBKDF2 with HMAC-SHA512 across 2,048 iterative rounds and salt `"mnemonic" + passphrase`.
- **BIP-32 / BIP-44 Hierarchical Deterministic Derivation:** Key derivation strictly follows the canonical Ethereum BIP-44 derivation path:

$$m / 44' / 60' / o' / o / o$$

This guarantees that any 12-word recovery phrase generated inside the POP mobile node produces the exact same private key, public key, and account address across all standard EVM wallets.

- **secp256k1 Point Multiplication:** Public keys (\$Q\$) are derived via scalar point multiplication on the Koblitz curve $y^2 \equiv x^3 + 7 \pmod{p}$ with standard generator point \$G\$:

$$Q = k \times G = (Q_x, Q_y)$$

- **Keccak-256 Hashing & EIP-55 Mixed-Case Checksumming:** Addresses are derived by hashing the uncompressed 64-byte public key coordinates (Q_x, Q_y) using Keccak-256 (with FIPS-202 domain separation `0x01`) and taking the final 20 bytes. Addresses are formatted with EIP-55 mixed-case capitalisation to prevent catastrophic typographical transmission errors:

$$\text{Address} = \text{EIP55}(\text{Keccak256}(Q_x \parallel Q_y)[12..31])$$

7.2. Anti-Sybil Proof-of-Participation Freshness & Dual-Key Isolation

- **Dual Key Separation:** Node Identity Keys (responsible for signing PoP heartbeats and lightweight computational proofs) are mathematically and physically decoupled from EVM Wallet Custody Private Keys (responsible for holding and signing balance transfers). Even in the unlikely event of an Android application sandbox or memory inspection breach, node identity telemetry cannot authorize token transactions or deplete wallet funds.
- **Block-Bound Challenge Freshness:** Proof challenges require the cryptographic hash of the immediately preceding finalized Layer 1 block:

$$\text{Challenge} = \text{SHA256}(\text{"POP-CHALLENGE-V1"} \parallel \text{ChainID} \parallel \text{Epoch} \parallel \text{NodeID} \parallel \text{PrevFinalizedHash})$$

Because PrevFinalizedHash is randomized and unknown until finalized by the BFT validator set, automated botnets and cloud farms are strictly prevented from pre-computing PoP proofs in advance.

- **Defensive Crash Boundaries:** Android client runtime routines isolate background coroutines, network RPC polls, and embedded AdMob SDK views within self-healing fault boundaries, eliminating unhandled exceptions and sustaining continuous, high-uptime background telemetry.

7.3. Quantum Threat Assessment & Post-Quantum Cryptography (PQC) Roadmap

A critical consideration for any Layer 1 blockchain designed for multi-decade persistence is resilience against quantum computation. POP Chain's security architecture differentiates between components vulnerable to quantum acceleration and those possessing intrinsic quantum resistance.

The Quantum Threat Reality

Quantum computing introduces two primary algorithmic threats to modern cryptography: **Shor's Algorithm** (which threatens asymmetric public-key cryptography) and **Grover's Algorithm** (which optimizes unstructured brute-force search over symmetric keys and hash preimages).

Cryptographic Primitive	Underlying Math / Standard	Quantum Threat Profile	Effective Quantum Security
secp256k1 (ECDSA)	Elliptic Curve Discrete Log	Vulnerable to Shor's Algorithm ($\mathcal{O}((\log N)^3)$ polynomial time)	0 bits (Broken once Public Key is exposed)
Keccak-256 / SHA-256	Sponge Permutation / Merkle-Damgård	Quantum-Resistant (Grover's Algorithm quadratic speedup only)	$\mathbf{128 \text{ bits}}$ (Computationally infeasible for billions of years)
PBKDF2 HMAC-SHA512	Iterative Hash MAC (2048 rounds)	Quantum-Resistant	$\mathbf{256 \text{ bits}}$

Cryptographic Primitive	Underlying Math / Standard	Quantum Threat Profile	Effective Quantum Security
Unspent Addresses	Public key hidden behind Keccak-256	Temporarily Protected (Public key obscured)	$\mathbf{128\text{ bits}}$ until first outgoing transaction

7.3.1. The Keccak-256 Hashing Shield

Because POP Chain addresses are derived as $\text{Keccak-256}(Q[12..31])$, an address that has only *received* funds and has never broadcast an outgoing transaction reveals **zero public key data** to the network. An adversary operating a Cryptanalytically Relevant Quantum Computer (CRQC) cannot apply Shor's algorithm directly to an address because the underlying public key coordinates are obscured behind a one-way preimage resistant hash. Only when an account signs and broadcasts its first transaction are its uncompressed public coordinates exposed via the (r, s, v) ECDSA signature tuple.

7.3.2. NIST Standardized Post-Quantum Migration Strategy

In August 2024, the National Institute of Standards and Technology (NIST) finalized its premier Post-Quantum Cryptography standards: **FIPS 203 (ML-KEM)**, **FIPS 204 (ML-DSA / CRYSTALS-Dilithium)**, and **FIPS 205 (SLH-DSA / SPHINCS+)**. POP Chain has established a three-phase transition framework to ensure perpetual quantum immunity without sacrificing immediate EVM usability:

- Phase 1: Ecosystem Parity & Classical Security (Current Testnet & Mainnet Launch)**
 Utilization of canonical `secp256k1`, BIP-39, and BIP-44 to ensure full compatibility with the existing multi-billion-dollar EVM wallet, dev tooling, and smart contract ecosystem.
- Phase 2: ERC-4337 Account Abstraction Quantum Safe Accounts**
 Through ERC-4337 Smart Contract Accounts, mobile and institutional users on POP Chain can deploy accounts that verify lattice-based digital signatures (such as **ML-DSA / Dilithium** or **Falcon**) directly at the contract verification level, achieving post-quantum protection today without requiring protocol-wide hard forks.
- Phase 3: Native L1 Consensus Hard Fork & Precompile Upgrade**
 As quantum hardware approaches the cryptanalytically relevant threshold (projected by NIST and leading quantum physicists to be 10–20+ years away), POP Chain governance will trigger a scheduled Layer 1 hard fork introducing:
 - A native post-quantum signature verification precompile (`PQC_VERIFY` at address `0x00...0b`).
 - A cryptographic grace period allowing classical `secp256k1` accounts to sign a one-time migration proof binding their balances to an ML-DSA or SLH-DSA post-quantum public key.
 - Deprecation of legacy ECDSA signatures for exposed accounts, permanently neutralizing Shor's algorithm across the entire POP ledger.

8. Official Network Specifications & Resources

Network Parameter	Specification / Live Resource
Network Name	POP Chain Testnet
EVM Chain ID	7070
Currency Symbol	POP (18 Decimals)
Public JSON-RPC Endpoint	http://3.108.40.44:7070
Block Explorer (PopScan)	http://3.108.40.44:8080/
Android Node APK (v0.2.1)	http://3.108.40.44:8080/downloads/pop-node-v0.2.1.apk
Testnet Faucet	Integrated in PopScan & RPC (pop_claimFaucet)