

BitBorn (BTB): Whitepaper v2 Refined

The Rebirth of Bitcoin – Faster, Smarter, More Private

1. Vision and Philosophy

BitBorn was born from a frustration: Bitcoin became slow, costly, and speculative instead of being a currency for everyday use.

Monero ensures privacy but is complex for average users. BitBorn combines scarcity, privacy, and simplicity in one system.

Core value: a digital currency for people – fast, private, easy.

Vision: within 5–10 years, BitBorn will serve daily commerce, e-commerce, and remittances, becoming a standard for private digital payments worldwide.

2. Consensus and Network Design

Block time: 45 seconds. Expected orphan rate: 2–4 percent, with a maximum acceptable threshold of 10 percent.

Fast propagation: Compact Blocks and GHOST protocol to limit orphan blocks.

Mining: RandomX for ASIC resistance.

Hashing: SHA3-256 for block headers and transaction integrity.

3. Scalability and Adaptive Block Size

Block size adapts using the median of the last 100 blocks, about 75 minutes of data.

Cap: maximum 20 percent block size growth per 24 hours.

This balances responsiveness to demand with protection against uncontrolled growth.

4. Privacy Layer

Privacy defaults: Stealth Addresses and RingCT.

Minimum ring size: 11, users may opt for larger (up to 64).

View Keys: multiple can be generated, managed securely in wallets, useful for auditors or regulators.

Libraries: based on reviewed open-source code (such as Monero), with additional audits.

5. Mining and Security

RandomX mining to resist centralization, SHA3 hashing for integrity.

Audits: external security reviews before Mainnet and annually.

Bug Bounty: continuous program through platforms like Immunefi.

Emergency response: rapid patching and community alerts.

RAM monitoring: parameters adjustable if RandomX requirements grow.

Quantum readiness: plan to integrate post-quantum cryptography such as XMSS or Falcon when practical.

6. Economics and Tokenomics

Distribution: Fair Launch from block zero, no premine or ICO.

Optional early airdrop (1 percent) to expand initial distribution.

Block Reward: starts at 50 BTB, halves every 4 years.

Tail Emission: 0.1 BTB per block, around 0.12 percent annual inflation, ensuring miner incentives.

Adjustability: community may vote to reduce or stop tail emission with 80 percent supermajority.

Incentives: holding rewards, cashback for merchants, and liquidity rewards for Lightning 2.0 channels.

7. Governance and Development Fund

Governance: BBIPs (BitBorn Improvement Proposals).

Quorum: 20 percent of circulating supply must participate.

Approval thresholds: 51 percent for routine, 67 percent for major upgrades, 80 percent for fundamental changes.

Dev Fund: 1 percent of block rewards for 4 years, secured by multi-sig (7-of-10) wallet.

Transparency: quarterly public financial reports.

Extension: community may vote to continue or stop after 4 years.

Participation: simplified mobile-friendly voting UI with summaries and symbolic rewards.

8. Community and Adoption

Ambassador Program: global representatives incentivized with BTB.

Community initiatives: hackathons, content contests, educational campaigns.

Official channels: Discord, Telegram, and Twitter/X with verified moderation.

Adoption focus: micropayments, e-commerce plugins (Shopify, WooCommerce), and global remittances.

Developer ecosystem: SDKs, grants, hackathons to expand applications.

9. Layer 2 and Bridges

Lightning 2.0: internally developed, simpler UX, privacy-enhanced, compatible with Bitcoin LN for cross-network payments.

Features: automatic channel backups, recovery with seed, and user-friendly interfaces.

Liquidity: early operator incentives through lower fees and rewards.

Bridges: designed to be decentralized (e.g., ChainBridge, tBTC).

Interim multisig bridges use 7-of-10 keys from independent institutions.

Safeguards: audits, transaction caps, and insurance pool for bridge users.

10. Long-Term Security and Strategy

Scaling: prioritize Layer 2; consider Layer 1 sharding only if demand requires it.

Attack resistance: Replace-by-Fee, fee bumping, and fork option against censorship.

Censorship attacks (21 percent miners) countered by incentive misalignment and RBF.

Quantum threat: readiness to integrate post-quantum schemes.

Vision: in 10 years, BitBorn as global private payment standard, usable in coffee shops, e-commerce, and remittances.

11. Team Insights and Lessons

Challenge: building community trust proved harder than writing code.

Dream feature: integrated decentralized identity.

Biggest pride: transparency and fairness, no premine or ICO.

Advice: start with the story, not the code. The narrative inspires, the code follows.