Botho: Privacy-Preserving Cryptocurrency

Executive Summary

Overview

Botho is a privacy-preserving cryptocurrency that combines post-quantum cryptography with efficient transaction privacy, achieving strong security guarantees with practical performance.

Key innovation: Hybrid post-quantum architecture applies quantum-resistant cryptography selectively—protecting permanent data (recipient identities) while using efficient classical cryptography for ephemeral privacy (sender anonymity).

Core Features

Feature	**Description**
Privacy	All transactions private by default. Ring signatures (CLSAG) hide sender among 20 decoys. Stealth addresses hide recipients. Confidential transactions hide amounts.
Post-Quantum	ML-KEM-768 protects recipient identity against future quantum attacks. On-chain data remains secure even if quantum computers break classical cryptography.
Fast Finality	Hybrid PoW+SCP consensus achieves deterministic finality in ∼5 seconds. Unlike Bitcoin, finalized blocks cannot be reverted.
Fair Economics	Progressive fees based on coin ancestry (not identity) create Sybil-resistant pressure against wealth concentration. Fees are 80% redistributed via lottery, 20% burned.

Technical Parameters

Parameter	**Value**	**Notes**
Ring size	20	Sender hidden among 20 possibilities
Transaction size	∼4 KB	Practical for mobile wallets
Block time	5–40s	Dynamic based on network load
Finality	∼5s	Deterministic (not probabilistic)
Tail emission	0.3 BTH/block	Perpetual ∼2% inflation

Cryptographic Primitives

- **Recipient privacy**: ML-KEM-768 (post-quantum KEM, NIST FIPS 203)
- **Sender privacy**: CLSAG ring signatures (classical, efficient)
- **Amount privacy**: Pedersen commitments + Bulletproofs range proofs
- **Minting signatures**: ML-DSA-65 (post-quantum signatures, NIST FIPS 204)
- **Key derivation**: BIP39 mnemonic → SLIP-10 → subaddresses

Consensus Mechanism

Hybrid PoW + SCP: Proof-of-work provides permissionless block proposal (anyone can mine). Stellar Consensus Protocol provides fast Byzantine-fault-tolerant finalization.

Why hybrid?

- PoW alone: Slow probabilistic finality, reorg vulnerability
- BFT alone: Requires known validator set, not permissionless
- PoW+SCP: Permissionless *and* fast deterministic finality

Economic Design

Progressive fees: Transaction fees scale with sender's cluster wealth percentile (1× for bottom 50%, up to 6× for top 1%). Based on coin *ancestry*, not current ownership—preserves privacy.

Fee distribution:

- 80% redistributed via lottery to random UTXO (favors small holders statistically)
- 20% burned (creates deflationary pressure proportional to usage)

Tail emission: Perpetual 0.3 BTH per block ensures long-term security funding. Asymptotic inflation: ∼2%.

Security Model

Threat	Protection	Security Level
Sender identification	CLSAG ring signatures	128-bit classical
Recipient identification	ML-KEM-768 stealth addresses	192-bit post-quantum
Amount discovery	Pedersen + Bulletproofs	128-bit classical
Double-spending	Key images + SCP finality	Information-theoretic
51% attack	SCP quorum intersection	Byzantine fault tolerant

Comparison

	Botho	**Monero**	**Zcash**	**Bitcoin**
Privacy	Full	Full	Optional	Pseudonymous
Post-quantum	Partial	No	No	No
Finality	5s deterministic	10+ min prob.	10+ min prob.	60+ min prob.
Tx size	4 KB	2 KB	2 KB (shielded)	0.3 KB
Fair distribution	Yes	No	No	No

Resources

- **Full whitepaper**: `botho-whitepaper.pdf` (127 pages)
- **Website**: `https://botho.org`
- **Source code**: `https://github.com/botho/botho`

"Motho ke motho ka batho" — A person is a person through other people.