RBTC

Reverse Bitcoin Protocol

Whitepaper v3.2 - Public Testnet Draft

Consensus v2: difficulty retarget, real Bech32 addresses, 70/20/10 fee split

Important Notice

RBTC is not production mainnet software today; it is an experimental Rust-based testnet node prototype. The correct public description is: "RBTC Node is an experimental Rust-based testnet prototype for the Reverse Bitcoin Protocol." Testnet tokens have no monetary value.

1. Summary

RBTC (Reverse Bitcoin Protocol) is an independent blockchain protocol inspired by Bitcoin's Proof-of-Work security model, but with the emission logic inverted. In Bitcoin, the block reward halves over time; in RBTC, the block reward grows as the circulating supply approaches the target ceiling (S_max). The protocol is an end-to-end Rust node implementation with its own genesis block, its own emission curve, SHA-256d-based PoW mining, a UTXO model, a P2P network, an RPC service, and a wallet/signed-transaction flow.

With v3.2, the protocol's core consensus-hardening work is complete: a real time-based difficulty retarget, BIP-173 Bech32 address encoding, and the 70/20/10 transaction fee split are now enforced in all node validation (see Sections 4 and 5).

2. Canonical Core Parameters

Project status	Experimental Rust-based testnet prototype	Not mainnet / not production-ready
Maximum supply	100,000,000 RBTC	Immutable protocol constant
Treasury premine	1,000,000 RBTC (1%)	Minted in the genesis block
Distributable mining supply	99,000,000 RBTC	Distributed over time via PoW
Consensus	Pure Proof of Work	SHA-256d hash algorithm
Hash algorithm	SHA-256d	Bit-for-bit compatible with Bitcoin's hashing model
Target block time	300 seconds (5 min)	Difficulty retarget targets this value
N_total	5,256,000 blocks	50 years x 105,120 blocks/year
lambda	5.0	Emission curve coefficient
R0	0.63887161 RBTC/block	Canonical value, 8 decimals
Fee split	70% miner / 20% treasury / 10% burn	Enforced in consensus v2
Difficulty retarget	Every 60 blocks, bounded to +/-2 bits	Enforced in consensus v2
Testnet address format	Real Bech32 (BIP-173), prefix: trbtc	Enforced in consensus v2
Testnet P2P port	28333	-
Testnet RPC port	28332	-

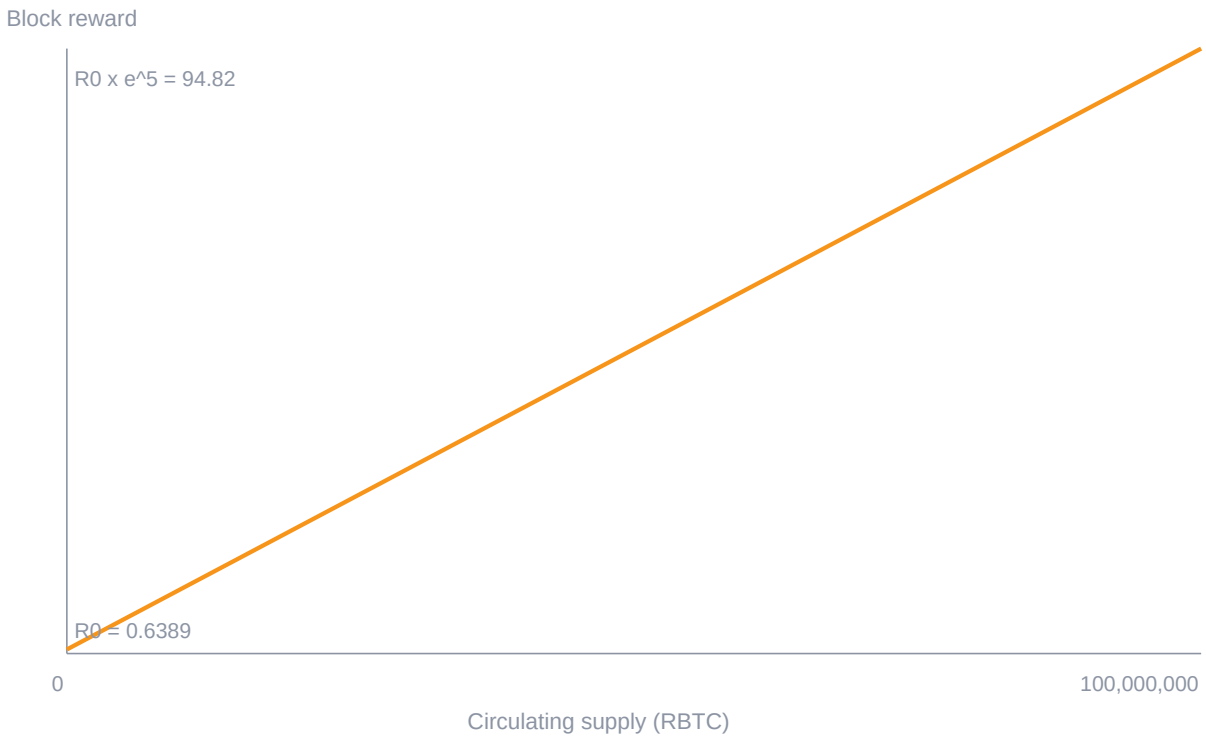
3. Emission Model

The RBTC emission model is based on circulating supply (c), not block height. This means every node can independently compute the same block reward as long as the circulating supply is the same.

r(c) = R0 x [1 + (e^lambda - 1) x (c - premine) / distributable]

R0 = distributable x lambda / (N_total x (e^lambda - 1)) = 99,000,000 x 5.0 / (5,256,000 x (e^5 - 1)) = 0.63887161 RBTC/block

Figure 1 - Block Reward vs. Circulating Supply



The curve shows that once the entire distributable supply has been issued (c -> S_max), the block reward reaches R0 times e^lambda. This is the mathematical inverse of Bitcoin's diminishing-reward model.

4. Token Economics and Distribution

Figure 2 - Maximum Supply Distribution (100,000,000 RBTC)

Treasury premine - 1,000,000 RBTC (1%)

Distributable mining supply - 99,000,000 RBTC (99%)

Figure 3 - Transaction Fee Split (PS-7.3 Fee Split)

70% Miner

20% Treasury

10% Burn

Of the transaction fees collected in each block, 70% is paid to the miner on top of the subsidy, 20% is transferred to the protocol treasury address (genesis::TREASURY_ADDRESS), and the remaining 10% is burned by simply never being added to any output. This rule is enforced at the consensus level in chain::validate_coinbase_fee_split; a coinbase transaction that exceeds these limits causes the block to be rejected.

Figure 4 - Difficulty Retarget Behavior

Difficulty is recomputed every 60 blocks: the actual elapsed block time is compared against the 300-second target, and the required number of leading zero bits is adjusted by at most +/-2 bits. Difficulty rises if blocks arrive faster than target, falls if they arrive slower, and carries over from the previous block between retarget windows.

5. Implementation Status (v0.2.0 - Consensus v2)

- Core blockchain: genesis, block header, SHA-256d, PoW mining, Merkle root, block/chain validation, persistence, emission engine.
- Consensus hardening: full fork choice, chain reorg (cumulative work), chain work comparison, real difficulty retarget, timestamp policy, coinbase maturity.
- Address format: real Bech32 (BIP-173) encoding/decoding with the trbtc testnet prefix.
- Fee split: the 70/20/10 rule is enforced in coinbase validation; mining code (main.rs/rpc.rs) computes and splits fees automatically.
- UTXO/transaction: UTXO set, coinbase, regular transactions, double-spend checks, txid, signing message, secp256k1 signature verification.
- Wallet/profile: signup/login/recovery phrase, export/import bundle, password change, encrypted (non-plaintext) profile storage.
- Mempool: persistence, duplicate/coinbase rejection, policy-based prioritization and size limits.
- RPC: status/height/supply/peers/mempool/block/tx/balance/utxos/submit-tx, explorer and profile endpoints, rate limiting.
- P2P: hello/ping, header/block sync, orphan persistence, known peers, peer reputation/ban score, signed tx relay.
- Automatic updates: the node and desktop app detect a newly published version and shut down or refuse to start.
- Release/ops: config.toml, Dockerfile, smoke test scripts, the Tauri desktop app, seed node deployment docs.

6. Current Roadmap

Phase 1 - Whitepaper and parameter finalization

COMPLETE

Complete.

Phase 2 - Rust MVP/testnet node + public alpha

COMPLETE

Complete: full test suite, clippy, smoke test, public documentation.

Phase 3 - Real open testnet hardening

COMPLETE

Complete (v0.2.0): difficulty retarget, reorg/fork choice, real Bech32, fee split.

Phase 4 - Audit and security review

NOT STARTED

Not started: independent audit, fuzz testing, long-running public testnet.

Phase 5 - Mainnet candidate

NOT STARTED

Not started: stable public testnet, deterministic build/release signing.

7. Items Remaining Before Mainnet

- Wallet security: an in-depth review of encrypted storage, plus hardware wallet support.
- RPC/P2P hardening: an in-depth review of the existing auth/rate-limit/ban-score baseline.
- Checkpoint policy and a long-running public testnet soak test.
- An independent security audit and fuzz testing.
- Deterministic build and release-signing infrastructure.

Disclaimer

This document is not investment advice. RBTC testnet tokens have no monetary value and may be reset at any time. Mainnet is not active, and no real economic value should be carried on this protocol until an independent security audit has been completed.