RBTC Final Protocol Specification

Version 1.1 - Corrected MVP/Testnet Draft
Metindeki proje özeti kanonik kabul edilerek düzenlenmiştir.

Düzeltme Notu

Bu belge, önceki Protocol Specification v1.0 içindeki iki önemli problemi düzeltir: (1) PS-7.2 Rust satoshi constants ölçekleme hatası; (2) production/final/değiştirilemez ifadelerinin MVP/testnet prototipi için fazla kesin olması. Mainnet öncesi bu belge yeniden audit edilmelidir.

PS-1 Konsensus Kuralları

- Konsensus algoritması: Pure Proof of Work.
- Hash algoritması: SHA-256d.
- Blok hedefi: 300 saniye / 5 dakika.
- Blok geçerlilik koşulu: hash(block_header) hedef target altında olmalıdır.
- Difficulty retarget hedefi: 2016 blok penceresi; mevcut MVP'de tamamlanması gereken production-consensus işidir.

PS-2 Emisyon Kuralları

Proje durumu	Experimental Rust-based MVP testnet prototype	Mainnet hazır veya production-ready olarak sunulmamalı.
Maksimum arz	100,000,000 RBTC	Değiştirilmez protokol sabiti.
Treasury premine	1,000,000 RBTC (%1)	Genesis/treasury başlangıç arzı.
Dağıtılabilir madencilik arzı	99,000,000 RBTC	PoW emisyonuyla dağıtılır.
Konsensus	Pure Proof of Work	SHA-256d tabanlı bağımsız zincir hedefi.
Hash algoritması	SHA-256d	Block hash, txid ve merkle hesaplarında kullanılacak.
Blok hedefi	5 dakika	Testnet hedef ortalaması.
N_total	5,256,000 blok	50 yıl x 105,120 blok/yıl.
lambda	5.0	Emisyon eğrisi katsayısı.
R0	0.63887161 RBTC/block	8 ondalık kanonik değer.
Fee split hedefi	70% miner / 20% burn / 10% treasury	Production consensus seviyesinde ayrıca tamamlanmalı/doğrulanmalı.

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

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

S_max = 100,000,000 RBTC
premine = 1,000,000 RBTC
distributable = 99,000,000 RBTC
lambda = 5.0
N_total = 5,256,000 blocks
```

Hard cap kuralı: c + r(c) > S_max olduğunda etkili ödül S_max - c ile sınırlanır. Dolaşım hiçbir koşulda 100,000,000 RBTC değerini geçmemelidir.

PS-3 İşlem Ücreti Kuralları

Hedef fee split 70% miner / 20% burn / 10% treasury şeklindedir. Bu kural protokol hedefi olarak korunur; ancak production consensus düzeyinde tam uygulama ve test kapsamı public testnet öncesi ayrıca doğrulanmalıdır.

PS-4 Sadakat Bonus Sistemi

Önceki dokümandaki sadakat bonus formülü ana MVP node kapsamına kanonik consensus kuralı olarak alınmamıştır. Public alpha hedefinde öncelik core PoW/UTXO/RPC/P2P güvenilirliğidir. Bonus sistemi ancak ayrı bir RBTC Improvement Proposal, simülasyon ve consensus test seti sonrası tekrar değerlendirilebilir.

PS-5 Güvenlik ve Onay Kuralları

- SHA-256d kullanımı blok hash, txid ve merkle root hesaplarında korunmalıdır.
- Coinbase maturity hedefi 100 bloktur; current-height bazlı tam uygulama doğrulanmalıdır.
- Büyük tutarlar için yüksek confirmation politikası önerilir; bu kullanıcı/wallet/explorer politikası olarak belgelenmelidir.
- Checkpoint mekanizması mainnet öncesi tasarlanmalı; testnet için esnek kalmalıdır.
- RPC ve P2P public internet'e açılmadan önce rate limit, auth ve message size limit gereklidir.

PS-6 Testnet Parametreleri

Parametre	Değer
Ağ adı	rbtc-testnet
Ticker	tRBTC
P2P port	28333
RPC port	28332
Address prefix hedefi	trbtc
Hash algoritması	SHA-256d
Magic bytes	0xCAFEBABE hedef/öneri; mevcut implementasyonda doğrulanmalı

PS-7 Rust Implementasyon Mimarisi

Mevcut zip/node yapısı tek crate içinde src/ modülleriyle ilerlemektedir. Üretim seviyesinde çoklu crate yapısı hedeflenebilir; ancak mevcut MVP için tek crate kabul edilebilir.

Modül	Amaç
src/emission.rs	r(c) emisyon formülü, R0, hard cap
src/hash.rs	SHA-256d, target/difficulty yardımcıları
src/block.rs	BlockHeader, merkle, PoW mining/validation
src/chain.rs	Chain state, persistence, validation, status
src/transaction.rs	UTXO transaction, signing message, fee validation
src/utxo.rs	UTXO set ve double-spend kontrolü
src/crypto.rs	secp256k1 key/sign/verify ve testnet adres türetme
src/mempool.rs	Mempool persistence/policy
src/rpc.rs	HTTP RPC endpoints

Modül	Amaç
src/p2p.rs	P2P message/sync/relay
src/config.rs / policy.rs	Config ve mempool policy

PS-7.2 Düzeltilmiş Emisyon Motoru (Rust)

```
pub const SATOSHI: u64 = 100_000_000;
pub const S_MAX: u64 = 10_000_000_000_000_000;       // 100,000,000 RBTC * 1e8
pub const PREMINE: u64 = 100_000_000_000_000;        // 1,000,000 RBTC * 1e8
pub const DISTRIBUTABLE: u64 = 9_900_000_000_000_000; // 99,000,000 RBTC * 1e8
pub const LAMBDA: f64 = 5.0;
pub const N_TOTAL: u64 = 5_256_000;

pub fn r0_satoshi() -> f64 {
    let d = DISTRIBUTABLE as f64;
    let n = N_TOTAL as f64;
    d * LAMBDA / (n * (LAMBDA.exp() - 1.0))
}

pub fn block_reward(circulating: u64) -> u64 {
    if circulating >= S_MAX { return 0; }
    let ratio = (circulating as f64 - PREMINE as f64) / DISTRIBUTABLE as f64;
    let reward_f = r0_satoshi() * (1.0 + (LAMBDA.exp() - 1.0) * ratio);
    let remaining = S_MAX - circulating;
    (reward_f.round() as u64).min(remaining)
}
```

Önceki PS-7.2'deki S_MAX/PREMINE/DISTRIB/R0_SAT değerleri 1 RBTC = 10^8 satoshi ölçeğiyle uyumsuzdu. Düzeltilmiş constants yukarıdaki gibidir. Mevcut zip içindeki src/emission.rs bu düzeltmeye daha yakındır ve kanonik kabul edilmelidir.

PS-8 Public Alpha Çıkış Kapısı

- README.md, SECURITY.md, ARCHITECTURE.md, ROADMAP.md, COMMANDS.md, TESTING.md, DISCLAIMER.md tamamlanmalı.
- cargo fmt, cargo test, cargo clippy, scripts/final_smoke_test.sh temiz geçmeli.
- wallet*.json, signed_tx.json, demo_tx.json, mempool.json, known_peers.json, orphans.json, node_a_chain.json, node_b_chain.json repo'da tracked olmamalı.
- README "MVP/testnet prototype" dilini kullanmalı; "mainnet ready" iddiası olmamalı.
- GitHub release tag: alpha-testnet-prototype veya v0.1.0-alpha önerilir.