

Technical Whitepaper: Proof of Sequential Sorting Race (PoSSR)

Consensus Protocol for High-Throughput Distributed Ledger Technology

- **Project Code:** rnr-core
- **Version:** 2.0 (Genesis Definition)
- **Status:** Draft Specification

Pengantar

1. Ringkasan Eksekutif

- **Tantangan Konvensional:** *Blockchain* konvensional menghadapi hambatan fundamental yang dikenal sebagai *Scalability Trilemma*. Mekanisme *Proof of Work* (PoW) klasik memboroskan energi untuk komputasi *hash* yang redundan, sementara *Proof of Stake* (PoS) cenderung mengarah pada sentralisasi kekayaan.
- **Solusi rnr-core:** rnr-core memperkenalkan paradigma baru: *Proof of Sequential Sorting Race* (PoSSR). Protokol ini menggantikan pencarian *nonce* acak dengan kompetisi algoritma pengurutan (*sorting*).
- **Performa:** Dengan memecah blok 1 GB menjadi 10 *shard* kompetitif berukuran 100 MB, PoSSR mencapai *throughput* 35.791 TPS dengan finalitas 1 menit, berjalan di atas infrastruktur perangkat keras komoditas (*consumer-grade hardware*) melalui manajemen memori yang efisien.

2. Filosofi Konsensus: Dari *Brute-Force* ke Efisiensi Algoritmik

Dalam PoSSR, "Mining" didefinisikan ulang sebagai upaya untuk menurunkan entropi data. 2.1. The Entropy Reduction Principle

Data transaksi yang masuk ke *mempool* bersifat acak (*chaos*). Tugas validator adalah mengorganisir data tersebut menjadi urutan yang terstruktur secara matematis.

- **Hash-based PoW (Bitcoin):** Menebak angka acak. Tidak ada nilai intrinsik pada hasil komputasi.
- **Sorting-based PoSSR:** Mengurutkan data. Komputasi difokuskan pada manipulasi memori dan logika algoritma. Efisiensi *node* diukur dari seberapa cepat ia dapat memanipulasi struktur data di dalam RAM.

2.2. Validasi Asimetris

Kunci keamanan PoSSR adalah ketidakseimbangan biaya komputasi:

- **Cost to Generate (Sorting):** Mahal dan kompleks. Kompleksitas waktu rata-rata adalah $\$O(N \log N)\$$.
- **Cost to Verify (Checking):** Sangat murah dan cepat. Verifikasi urutan hanya

membutuhkan pemindaian linear dengan kompleksitas $O(N)$.

3. Arsitektur Teknis PoSSR3.1. Mekanisme "The Race" (Balapan 100 MB)

Alih-alih satu *node* memproses seluruh blok, PoSSR menggunakan sistem *parallel sharding race*.

- **Input Workload:** Setiap *node* validator mengambil paket data transaksi sebesar 100 MB.
- **Algorithmic Lottery (VRF):** Setiap siklus blok diawali dengan *Verifiable Random Function* (VRF) yang menentukan "Rule of the Race".
 - **Contoh:** Blok #1005 memerintahkan penggunaan *Merge Sort*. Blok #1006 memerintahkan *Radix Sort*.
 - **Tujuan:** Mencegah pembuatan ASIC (*Application-Specific Integrated Circuit*) yang hanya unggul di satu algoritma, memaksa penggunaan CPU *general-purpose* yang fleksibel.
- **Execution:** *Node* mengurutkan 100 MB data berdasarkan *Key* unik (*Hash Transaksi + Block Seed*). Di sinilah "Race" terjadi. Kemenangan ditentukan oleh:
 - Kecepatan *Memory Bandwidth* (RAM).
 - Efisiensi implementasi kode (*Software Optimization*).
 - Latensi jaringan (*Network Propagation*).

3.2. Struktur Blok Agregat (1 GB)

Blok dalam rnr-core bersifat dinamis dengan batas atas (*cap*) masif.

- **Komposisi:** Blok terbentuk dari agregasi 10 Pemenang Tercepat.
- **Kalkulasi:** $10 \text{ Node} \times 100 \text{ MB/Node} = 1.000 \text{ MB (1 GB)}$.
- **Struktur Header:** *Header* blok berisi 10 *Merkle Root* dari 10 pemenang tersebut, membentuk *Super-Root* yang menjamin integritas 1 GB data.

4. Skalabilitas & Performa4.1. Kalkulasi Throughput (TPS)

Dengan ukuran blok 1 GB dan waktu blok 1 menit, rnr-core dirancang untuk menangani beban transaksi global, mencapai 35.791 TPS.

4.2. Manajemen Penyimpanan: *Rolling Pruning*

Untuk memungkinkan *throughput* sebesar ini tanpa menyebabkan sentralisasi penyimpanan, PoSSR menerapkan *Protocol-Level Pruning*.

- **Pruning Window:** 25 Blok.
- **Mekanisme:** *Node* validator hanya diwajibkan menyimpan data transaksi mentah (*raw block data*) selama 25 menit terakhir.
- **Persistent State:** Yang disimpan selamanya hanyalah *Account State Trie* (saldo akhir) dan *Block Headers*.
- **Dampak:** Kebutuhan penyimpanan stabil di kisaran 25 GB – 30 GB, memungkinkan

partisipasi perangkat kelas konsumen (*consumer-grade*).

5. Model Ekonomi (Tokenomics)

Ekonomi rnr-core dirancang untuk stabilitas jangka panjang dengan kurva emisi yang dapat diprediksi namun semakin langka (*deflationary pressure*).

- **Ticker:** RNR
- **Total Max Supply:** 5.000.000.000 (5 Miliar) Koin.
- **Unit Terkecil:** 0,00000001 (8 desimal).

5.2. Skema Insentif & Halving

Berbeda dengan Bitcoin yang memotong *reward* secara drastis (50%), rnr-core menggunakan pendekatan *Decay Function*.

- **Base Reward:** 10 Koin per pemenang (Total 100 koin per blok terdistribusi ke 10 *node*).
- **Halving Interval:** Setiap 3.500.000 Blok (Estimasi waktu: $\approx 6,6$ tahun).
- **Decay Rate:** 7%.

Model ini menjamin bahwa insentif bagi penambang tetap relevan selama puluhan tahun, memberikan waktu yang cukup untuk adopsi jaringan sebelum *reward* menjadi sangat kecil.

6. Analisis Keamanan

6.1. Resistensi Sybil & Bot

Dalam PoSSR, membuat 1.000 identitas *node* palsu tidak memberikan keuntungan jika identitas tersebut tidak memiliki daya komputasi (*Computational/Memory Power*) untuk menyelesaikan *sorting* 100 MB. "Tiket masuk" untuk memvalidasi blok adalah bukti kerja nyata (*Proof of Execution*), bukan sekadar kepemilikan koin atau alamat IP.

6.2. Collision Resistance

Setiap set data 100 MB memiliki satu, dan hanya satu, urutan yang benar berdasarkan algoritma yang dipilih.

- Jika *Node A* mencoba curang dengan mengubah urutan 1 transaksi saja, *Merkle Root* akan berubah total.
- Verifikator akan langsung mendeteksi ketidakcocokan *hash* dalam hitungan milidetik dan membuang blok tersebut (*Slashing Condition*).

7. Roadmap Implementasi

- **Phase 1 (Core Engine):** Pengembangan pustaka algoritma *sorting* (*Go-based*) dan integrasi VRF.
- **Phase 2 (P2P Network):** Implementasi protokol *gossip* untuk transmisi data 100 MB dengan latensi rendah.
- **Phase 3 (Pruning & State):** Integrasi *database LevelDB* dengan logika *auto-pruning*.
- **Phase 4 (Mainnet Launch):** *Genesis Block* dengan parameter 1 GB/1 Menit.

8. Penutup

rnr-core dengan konsensus PoSSR membuktikan bahwa performa tingkat institusi (35k+ TPS) dapat dicapai dalam jaringan terdesentralisasi. Dengan memindahkan fokus dari "*Energy Mining*" ke "*Efficiency Racing*", rnr-core membangun infrastruktur yang adil, cepat, dan siap untuk masa depan.