

Whitepaper Resmi: ROUTE N ROOT (RNR-30)

Sebuah Blockchain Layer 1 yang Didukung oleh Proof of Bandwidth dan Proof of History

Lisensi:

- Kode: MIT License

- Dokumen: CC BY 4.0

Abstrak Eksekutif

ROUTE N ROOT (RNR-30) adalah sebuah protokol blockchain Layer 1 inovatif yang dirancang untuk mengatasi trilema blockchain—skalabilitas, keamanan, dan desentralisasi—dengan pendekatan yang efisien secara energi. Protokol ini memperkenalkan mekanisme konsensus hibrida yang menggabungkan **Proof of Bandwidth (PoB)** dengan **Proof of History (PoH)**. Dengan memanfaatkan bandwidth internet sebagai sumber daya validasi utama, RNR-30 secara drastis mengurangi jejak karbon yang terkait dengan konsensus Proof of Work (PoW). Waktu blok yang konstan selama 30 detik menciptakan lingkungan jaringan yang prediktif, sementara PoH memastikan finalitas transaksi yang sangat cepat. Arsitektur RNR-30 tidak hanya menawarkan ketahanan superior terhadap serangan DDoS berbasis lalu lintas, tetapi juga mendorong partisipasi jaringan yang lebih luas dan adil melalui model tokenomics yang unik.

1. Pendahuluan: Visi RNR-30

Di tengah lanskap blockchain yang didominasi oleh mekanisme konsensus yang boros energi atau yang memusatkan kekuasaan pada segelintir pemangku kepentingan, RNR-30 lahir sebagai alternatif. Visi kami adalah menciptakan ekosistem terdesentralisasi yang tidak hanya aman dan cepat tetapi juga berkelanjutan dan dapat diakses oleh siapa saja yang memiliki koneksi internet yang stabil.

Tujuan utama di balik RNR-30 adalah:

- **Efisiensi Energi:** Menggantikan komputasi intensif dengan validasi berbasis bandwidth untuk meminimalkan konsumsi daya.
- **Keamanan Jaringan yang Ditingkatkan:** Desain PoB secara inheren menyaring partisipan dengan koneksi yang buruk, memperkuat jaringan terhadap serangan spam dan DDoS.
- **Finalitas Cepat:** Menggunakan PoH sebagai "jam kriptografis" untuk menyusun urutan transaksi secara definitif sebelum konsensus, memungkinkan finalitas blok tercapai dalam satu siklus propagasi.
- **Distribusi Imbalan yang Adil:** Memberi insentif tidak hanya kepada pembuat blok tetapi juga kepada node yang secara konsisten berkontribusi pada kesehatan dan kecepatan jaringan.

2. Konsep Inti: Proof of Bandwidth dan Proof of History

2.1. Proof of Bandwidth (PoB)

PoB adalah mekanisme yang memvalidasi kemampuan node untuk berpartisipasi dalam konsensus berdasarkan kualitas koneksi internet mereka. Tujuannya adalah untuk memastikan bahwa setiap validator adalah saluran yang andal untuk propagasi data, yang krusial untuk menjaga sinkronisasi dan kesehatan jaringan.

Penjelasan Teknis: Untuk memastikan pengukuran yang akurat dan tidak mudah dimanipulasi, PoB menggunakan pipeline pemrosesan data multi-tahap:

1. **Pengambilan Sampel (Sampling):** Setiap node secara berkala mengukur metrik koneksi ke sejumlah peer yang dipilih secara pseudo-acak untuk mencegah kolusi. Metrik yang diukur adalah:
 - **Latensi:** ≤ 40 ms
 - **Throughput Unggah (Upload):** ≥ 7 MB/s
 - **Kehilangan Paket (Packet Loss):** $\leq 0.1\%$
2. **Penyaringan Derau (Noise Filtering):** Data mentah yang dikumpulkan sering kali mengandung anomali atau nilai ekstrem sesaat. Untuk mengatasinya, nilai-nilai ini disaring menggunakan metode statistik seperti *median filter* untuk membuang pencilan.
3. **Perataan Nilai (Value Smoothing):** Setelah penyaringan awal, hasil pengukuran diratakan menggunakan **Exponential Moving Average (EMA)**. Langkah ini penting untuk menghasilkan tren kinerja yang stabil dan mencegah fluktuasi jangka pendek yang tidak representatif mendiskualifikasi node yang sebenarnya andal.
4. **Perhitungan Skor:** Setiap metrik yang memenuhi ambang batas akan diberikan 1 poin. Skor akhir dihitung dengan rumus:

Rumus:

Skor PoB = (poin_latensi + poin_upload + poin_packet_loss) / 3

poin. Skor akhir dihitung dengan rumus:

$$\text{Skor PoB} = \frac{(\text{poin}_{\text{latensi}} + \text{poin}_{\text{upload}} + \text{poin}_{\text{packet_loss}})}{3}$$

Sebuah node dianggap sebagai validator yang sah jika berhasil mempertahankan **Skor PoB ≥ 0.85** .

2.2. Proof of History (PoH)

PoH berfungsi sebagai jam kriptografis yang menyediakan catatan historis yang dapat diverifikasi tentang urutan dan waktu terjadinya suatu peristiwa atau transaksi. Ini bukanlah mekanisme konsensus itu sendiri, melainkan sebuah komponen yang mengoptimalkan efisiensi konsensus PoB.

Penjelasan Teknis: PoH bekerja dengan cara membuat sekuens hash di mana output dari satu hash menjadi input untuk hash berikutnya. Di antara setiap hash, data transaksi ditambahkan. Dengan menyertakan *timestamp* dan urutan secara kriptografis di dalam header blok, PoH memungkinkan hal-hal berikut:

- **Verifikasi Efisien:** Node dapat memverifikasi urutan transaksi tanpa perlu berkomunikasi

- secara ekstensif dengan node lain atau mengunduh seluruh blok sebelumnya.
- **Sinkronisasi Cepat:** Mengurangi waktu yang dibutuhkan node baru untuk menyinkronkan diri dengan keadaan jaringan saat ini.
- **Pengurangan Konflik Fork:** Dengan menyediakan urutan waktu yang jelas, PoH secara signifikan mengurangi kemungkinan terjadinya fork yang tidak disengaja.

3. Mekanisme Konsensus RNR-30

3.1. Siklus Hidup Blok (30 Detik)

Setiap blok di jaringan RNR-30 memiliki siklus hidup yang terstruktur dan terdefinisi dengan baik selama 30 detik, yang dibagi menjadi tiga fase utama:

1. **Fase Propagasi (0–10 detik):**
 - Setelah menemukan blok, validator wajib menyiarkannya ke jaringan dalam waktu ≤ 1 detik.
 - Tujuannya adalah agar blok diterima oleh $\geq 85\%$ dari total node aktif dalam waktu ≤ 10 detik.
2. **Fase Verifikasi (10–25 detik):**
 - Node penerima segera melakukan verifikasi cepat (tanda tangan, urutan PoH, header, skor PoB) dan menyiarkan ulang blok tersebut ke peer mereka dalam ≤ 1 detik.
 - Secara paralel, verifikasi penuh terhadap semua transaksi di dalam blok dilakukan.
3. **Fase Buffer (25–30 detik):**
 - Jeda waktu 5 detik ini berfungsi sebagai toleransi untuk keterlambatan jaringan dan memastikan proses verifikasi selesai sebelum siklus blok berikutnya dimulai.

3.2. Logika Resolusi Fork

Meskipun PoH mengurangi kemungkinan fork, RNR-30 memiliki mekanisme tie-breaking yang jelas jika dua validator membuat blok pada ketinggian yang sama:

1. **Bobot PoB Kumulatif Tertinggi:** Jaringan akan memilih rantai yang memiliki total bobot PoB ($\Sigma \text{difficulty_target}$) terbesar.
2. **Timestamp PoH Terkecil:** Jika bobotnya sama, rantai dengan timestamp PoH paling awal akan dipilih.
3. **Hash Blok Terkecil:** Jika masih terjadi kesamaan, rantai dengan nilai hash blok terkecil secara leksikografis akan menjadi pemenangnya.

Transaksi yang valid dari blok yang kalah (dikenal sebagai *uncle/ommer blocks*) tidak akan hilang, melainkan dikembalikan ke *mempool* untuk dimasukkan ke dalam blok berikutnya.

3.3 Kecepatan Finalitas Transaksi

Sebuah transaksi dapat dianggap final atau sah dengan sangat cepat, yaitu dalam **satu siklus blok (30 detik)** pada kondisi jaringan yang ideal.

Penjelasan Teknis: Kecepatan ini dimungkinkan berkat mekanisme **Proof of History (PoH)**. PoH berfungsi sebagai "jam kriptografis" yang mencatat dan menyusun urutan semua transaksi secara definitif *sebelum* blok divalidasi oleh konsensus PoB.

- **Finalitas 1 Blok:** Karena urutannya sudah pasti, sebuah blok dapat dianggap final segera setelah berhasil disiarkan dan diverifikasi oleh jaringan tanpa perlu menunggu konfirmasi blok-blok berikutnya.
- **Kondisi Ideal:** Finalitas dalam 30 detik ini tercapai jika tidak ada *fork* atau dua blok yang

valid dibuat pada ketinggian yang sama secara bersamaan. Ini adalah keunggulan signifikan dibandingkan blockchain lain yang mungkin memerlukan beberapa konfirmasi blok (misalnya 6 blok atau lebih) untuk mencapai tingkat finalitas yang sama.

4. Tokenomics (RNR)

Model ekonomi token RNR dirancang untuk memberikan insentif jangka panjang bagi semua partisipan jaringan.

4.1. Imbalan Blok (Block Reward)

- **Imbalan Awal:** 100 RNR per blok.
- **Mekanisme Pengurangan:** Imbalan akan berkurang sebesar 1 RNR setiap 1.000.000 blok. Namun, imbalan tidak akan pernah mencapai nol dan akan berhenti pada nilai minimum **1 RNR per blok** selamanya untuk memastikan keamanan jaringan tetap terjaga.
- **Rumus Matematis:**

Rumus:

$$R(h) = \max(1, 100 - \text{floor}((h-1) / 1,000,000))$$

Penjelasan:

- * $R(h)$: Imbalan blok pada ketinggian blok (h).
- * h : Ketinggian blok saat ini.
- * $\text{floor}(\dots)$: Membulatkan angka ke bawah.

- **Rumus Matematis:**

$$R(h) = \max \left(1, 100 - \left\lfloor \frac{h - 1}{1,000,000} \right\rfloor \right)$$

di mana h adalah ketinggian blok.

4.2. Distribusi Imbalan

Distribusi imbalan dirancang untuk menghargai kontribusi secara adil:

- **70%** diberikan kepada validator penemu blok.
- **30%** didistribusikan secara merata kepada hingga **50 node teratas** yang menjadi kontributor data pengukuran PoB yang valid dan andal untuk blok tersebut. Jika jumlah kontributor kurang dari 50, maka imbalan dibagi rata di antara mereka yang ada.

Sisa pecahan dari pembagian imbalan (setelah pembulatan ke bawah 8 desimal) akan **dibakar**

(burned), menjadikannya mekanisme deflasi minor.

4.3. Biaya Transaksi (Transaction Fees)

- **Base Fee:** Biaya dasar yang dihitung berdasarkan nilai transaksi yaitu 0.0001%. Biaya ini dibakar untuk mengurangi pasokan RNR.
- **Priority Fee:** Biaya tambahan opsional yang dapat disertakan oleh pengguna untuk memprioritaskan transaksi mereka. Biaya ini diberikan langsung kepada validator penemu blok. Tambahan biaya = bytes × rate_per_byte (0.0001 RNR)

5. Aturan Jaringan dan Penalti

5.1. Kapasitas Blok Dinamis

Ukuran maksimum setiap blok tidak statis, melainkan disesuaikan secara dinamis berdasarkan kapasitas upload validator yang menemukannya. Ini memastikan bahwa blok yang dibuat tidak akan menyebabkan kemacetan jaringan.

- **Rumus Kapasitas:**

$$\text{Kapasitas Blok Maks} = 0.30 * \text{Upload_Validator_}(\text{MB/s}) * 10 \text{ detik}$$

Kapasitas ini dirancang agar blok dapat diterima oleh $\geq 85\%$ node dalam fase propagasi 10 detik.

5.2. Aturan dan Sanksi

Untuk menjaga integritas dan kinerja jaringan, RNR-30 menerapkan sistem sanksi yang tegas:

- **Aturan Node Baru:** Node yang ingin bergabung sebagai validator harus "membayar" biaya masuk dengan menyediakan bandwidth setara dengan 6 jam kapasitas operasional validator. Ini diverifikasi melalui pengiriman data dummy ke beberapa validator aktif.
- **Pelanggaran Kapasitas Blok:** Validator yang membuat blok melebihi kapasitas dinamisnya akan menghadapi sanksi berjenjang:
 1. Pelanggaran Pertama: Node ditandai (warning).
 2. Pelanggaran Kedua: Status validator diturunkan dan diwajibkan membayar denda bandwidth 1 jam.
 3. Pelanggaran Ketiga: Dikeluarkan dari set validator dan harus mendaftar ulang dengan denda bandwidth 6 jam.
- **Pemalsuan Bukti (False Proofs):** Memanipulasi data pengukuran PoB adalah pelanggaran serius. Jika terdeteksi melalui verifikasi silang oleh peer, sanksinya meliputi:
 1. Seluruh imbalan blok hangus.
 2. Penurunan status validator sementara.
 3. Pelanggaran berulang akan mengakibatkan larangan permanen (permanent ban).

6. Tata Kelola (Governance)

RNR-30 diatur oleh komunitas validatornya melalui mekanisme voting on-chain yang transparan.

- **Model Voting:** 1 node = 1 suara.

- **Ambang Batas Keputusan:** Sebuah proposal dianggap sah dan akan diimplementasikan jika disetujui oleh mayoritas super (supermajority) sebesar **lebih dari 85%** dari total validator aktif. Ambang batas yang tinggi ini memastikan bahwa setiap perubahan kritis terhadap protokol (seperti penyesuaian parameter konsensus atau model tokenomics) memiliki dukungan yang luar biasa dari jaringan.

7. Parameter Awal Jaringan

Tabel berikut merangkum parameter awal yang ditetapkan untuk peluncuran jaringan RNR-30:

Parameter	Nilai
Waktu Blok	30 detik
Target Propagasi	$\geq 85\%$ node dalam ≤ 10 detik
Jendela Retarget PoB	Setiap 100 blok
Skor PoB Minimal	0.85
Minimum Peer Pengukuran	3 peer
Jumlah Peer Sampling	5 peer
Batas Penyesuaian Difficulty	$\pm 20\%$ per jendela retarget
Batas Tx Pembuatan Wallet	15 transaksi per blok
Penerima Imbalan PoB	Hingga 50 node kontributor teratas

8. Kesimpulan

ROUTE N ROOT (RNR-30) menghadirkan paradigma baru dalam teknologi blockchain dengan memprioritaskan efisiensi, kecepatan, dan keamanan melalui mekanisme konsensus Proof of Bandwidth dan Proof of History. Dengan mengalihkan fokus dari kekuatan komputasi ke kualitas konektivitas, RNR-30 tidak hanya menjadi solusi yang lebih ramah lingkungan tetapi juga membuka pintu bagi partisipasi global yang lebih luas. Arsitektur yang dirancang dengan cermat, model tokenomics yang seimbang, dan tata kelola yang kuat menjadikan RNR-30 sebagai platform yang siap untuk mendukung generasi berikutnya dari aplikasi terdesentralisasi skala besar.