# Whitepaper Spesifikasi Protokol ROUTE N ROOT (RNR)

Oleh: Shobikhul Irfan

**Prakata**

- Lisensi Kode: MIT License.
- Lisensi Dokumen: CC BY 4.0.
- Penulis menggunakan bantuan asisten AI untuk memperdalam riset dan analisis keamanan dalam penyusunan dokumen ini.

## Abstrak

Tantangan fundamental dalam teknologi blockchain adalah menciptakan kelangkaan digital yang aman dan terdesentralisasi. Solusi perintis, Proof of Work (PoW), berhasil membuktikannya dengan mengorbankan efisiensi energi dalam skala besar. ROUTE N ROOT (RNR) menjawab tantangan ini dari sudut pandang yang berbeda secara fundamental. Kami mengajukan Proof of Bandwidth (PoB), sebuah mekanisme konsensus baru yang memanfaatkan kualitas konektivitas internet—sebuah sumber daya yang terdistribusi secara global dan vital secara ekonomi—sebagai dasar dari keamanan jaringan. Dengan memvalidasi throughput, latensi, dan stabilitas, RNR menciptakan sistem yang secara inheren efisien dan tahan terhadap sentralisasi komputasi. Diperkuat oleh Proof of History (PoH) untuk finalitas transaksi yang cepat, arsitektur RNR secara mandiri menawarkan fondasi yang kokoh untuk generasi berikutnya dari aset digital terdesentralisasi.

## Bab 0: Manifesto - Menuju Kontrak Sosial Digital yang Berkelanjutan

Kelahiran Bitcoin memperkenalkan sebuah kontrak sosial digital yang radikal: sebuah sistem nilai yang tidak dapat disensor, disita, atau dimanipulasi, yang diamankan oleh hukum fisika melalui Proof of Work. Kontrak ini berhasil, namun ia mengandung cacat tragis—sebuah dahaga tak terpuaskan akan energi yang mengancam kelestarian lingkungan kita.

Dunia kini berada di persimpangan jalan. Kita membutuhkan aset digital yang netral dan langka, tetapi kita tidak bisa membangun masa depan finansial di atas fondasi yang merusak masa depan planet ini.

ROUTE N ROOT (RNR) dibangun di atas keyakinan bahwa keamanan digital tidak harus berbanding lurus dengan konsumsi energi. Kami menolak premis bahwa pemborosan adalah harga dari kepercayaan.

Kami mengajukan sebuah pilar fundamental baru untuk konsensus terdesentralisasi: **Proof of Bandwidth**. Sebuah mekanisme yang mengamankan jaringan dengan memvalidasi sumber daya yang sudah menopang peradaban digital kita—konektivitas. Ini adalah konsensus yang

berasal dari partisipasi dalam infrastruktur global, bukan dari perlombaan komputasi yang terisolasi.
Ini bukan sekadar sebuah whitepaper. Ini adalah argumen bahwa masa depan uang digital haruslah cerdas, efisien, dan berkelanjutan. Ini adalah undangan untuk membangun sebuah kontrak sosial digital yang baru, yang aman untuk aset kita dan ramah untuk dunia kita.

# Bab 1: Pendahuluan

## 1.1. Visi: Menuju Konsensus Berbasis Realitas Fisik

Visi di balik RNR bukanlah untuk meniru, melainkan untuk berinovasi secara fundamental. Kami bertanya: "Selain daya komputasi (PoW) atau modal (PoS), sumber daya apa di dunia nyata yang terdistribusi secara luas, sulit dipalsukan, dan partisipasinya dapat diverifikasi secara kriptografis?"
Jawaban kami adalah **konektivitas jaringan**. Di era digital, bandwidth berkualitas tinggi adalah sumber daya ekonomi yang nyata. RNR dibangun di atas hipotesis bahwa dengan mengukur dan memvalidasi sumber daya ini secara handal, kita dapat membangun jaringan terdesentralisasi yang aman dan efisien. Visi kami adalah menciptakan protokol yang keamanannya berakar pada realitas infrastruktur digital global yang sudah ada, bukan pada perlombaan artifisial yang boros energi.

## 1.2. Tujuan Utama Protokol

Tujuan RNR adalah untuk membuktikan hipotesis ini melalui desain yang kokoh:

- **Keamanan dari Verifikasi Bandwidth**: Menciptakan keamanan jaringan yang berasal dari kesulitan untuk memalsukan koneksi internet berkualitas tinggi secara konsisten di hadapan penguji acak yang dipilih secara kriptografis (via VRF). Desain PoB secara inheren menyaring partisipan dengan koneksi yang buruk, memperkuat jaringan terhadap serangan *spam* dan DDoS.
- **Efisiensi sebagai Prinsip Desain**: Membangun protokol yang konsumsi energinya sebanding dengan operasi pusat data standar, bukan meningkat seiring dengan harga aset, sehingga menciptakan model keamanan yang berkelanjutan. Ini dilakukan dengan menggantikan komputasi intensif dengan validasi berbasis kualitas koneksi untuk meminimalkan konsumsi daya.
- **Desentralisasi Geografis & Infrastruktur**: Mendorong partisipasi global dengan mendasarkan validasi pada sumber daya (konektivitas) yang lebih terdistribusi daripada fasilitas penambangan khusus atau akumulasi modal yang besar.
- **Integritas Data yang Dapat Dibuktikan**: Menggunakan ZK-SNARKs untuk memastikan setiap klaim performa jaringan dapat diverifikasi secara matematis oleh seluruh jaringan tanpa perlu kepercayaan, menciptakan fondasi konsensus yang objektif.
- **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.

# Bab 2: Analisis Lanskap Mekanisme Konsensus

Untuk memahami inovasi RNR, penting untuk memetakannya dalam lanskap solusi yang ada untuk masalah konsensus terdesentralisasi. Setiap mekanisme utama menawarkan pertukaran (*trade-off*) yang berbeda.

| Parameter | **Proof of Work (PoW)** | **Proof of Stake (PoS)** | **Proof of Bandwidth (PoB) - RNR** |
|---|---|---|---|
| **Sumber Daya Dasar** | Daya Komputasi (Energi) | Modal (Kekayaan) | Konektivitas Jaringan (Infrastruktur) |
| **Vektor Sentralisasi** | Ekonomi Skala (Pabrik ASIC, Listrik Murah) | Akumulasi Modal ("Kaya semakin kaya") | Kedekatan Geografis dengan Infrastruktur Internet (Dapat dimitigasi dengan parameter regional) |
| **Biaya Serangan** | Biaya CAPEX (*Hardware*) & OPEX (Listrik) yang sangat tinggi. | Biaya Modal (Harga dari 51% token yang di-*stake*). Rentan terhadap serangan modal besar. | Biaya OPEX (Sewa *server* & koneksi *premium* di banyak lokasi). Menuntut diversifikasi infrastruktur. |
| **Prinsip Keamanan** | Mahalnya biaya untuk "memalsukan" pekerjaan komputasi. | Mahalnya biaya untuk "mempertaruhkan" modal yang bisa hilang (*slashed*). | Sulitnya "memalsukan" performa jaringan yang superior dan stabil secara konsisten di hadapan banyak penguji acak. |
| **Dampak Ekonomi** | Mendorong industri perangkat keras & konsumsi energi. | Mendorong akumulasi modal dan *staking*. | Mendorong investasi pada infrastruktur konektivitas internet berkualitas tinggi. |

**Kesimpulan Analisis**: PoW dan PoS telah terbukti sebagai model yang valid dengan kelebihan dan kekurangannya masing-masing. **Proof of Bandwidth (PoB) yang diusulkan oleh RNR bukanlah variasi dari keduanya, melainkan sebuah pilar ketiga yang fundamental**. Ia menggeser paradigma keamanan dari "siapa yang memiliki komputer tercepat" atau "siapa yang memiliki modal terbanyak" menjadi "siapa yang memiliki kontribusi infrastruktur jaringan paling andal dan dapat dibuktikan". Pendekatan ini menawarkan serangkaian *trade-off* yang unik dan berpotensi menjadi fondasi yang kokoh untuk jaringan yang benar-benar terdesentralisasi dan efisien.

# Bab 3: Mekanisme Konsensus Inti (Proof of

# Bandwidth & Proof of History)

Protokol ROUTE N ROOT (RNR) mengimplementasikan mekanisme konsensus hibrida yang menggabungkan *Proof of Bandwidth* (PoB) dengan *Proof of History* (PoH) untuk mengatasi trilema *blockchain*: skalabilitas, keamanan, dan desentralisasi, dengan pendekatan yang efisien secara energi.

## 3.1. Proof of Bandwidth (PoB): Fondasi Keamanan Jaringan

PoB berfungsi sebagai "tes kesehatan" berkelanjutan bagi setiap *node* yang ingin berpartisipasi dalam konsensus. Idenya adalah untuk memastikan bahwa *node* memiliki koneksi internet yang cepat, stabil, dan responsif. Keamanan berasal dari sulitnya memalsukan koneksi berkualitas tinggi secara konsisten.

### 3.1.1. Konsep dan Filosofi

Jaringan RNR ibarat tim estafet. Setiap pelari (*node*) harus mampu berlari cepat (*throughput*), memiliki reaksi sigap (latensi), dan tidak pernah menjatuhkan tongkat (kehilangan paket). PoB adalah proses kualifikasi untuk memastikan hanya "atlet jaringan" terbaik yang bisa bergabung dengan tim.

### 3.1.2. Metrik Kunci dan Target Kinerja

PoB mengevaluasi tiga metrik fundamental dari sebuah koneksi jaringan:

1. ***Throughput* Unggah (Kecepatan)**: Kapasitas mentah *node* untuk mengirim data (MB/s). **Target: ≥ 7 MB/s**. Ini penting untuk penyebaran blok dan transaksi yang cepat.
2. **Latensi (Waktu Respons)**: Waktu perjalanan bolak-balik paket data kecil (ms). **Target: ≤ 100 ms**. Krusial untuk finalitas transaksi cepat dan sinkronisasi konsensus.
3. **Kehilangan Paket (Keandalan)**: Persentase paket data yang hilang saat transmisi. **Target: 0.1%**. Menunjukkan koneksi yang stabil dan andal.

### 3.1.3. Arsitektur PoB (PoB)

Untuk mengatasi kelemahan fundamental, yaitu ketergantungan pada laporan subjektif dan kerentanan terhadap kolusi serta serangan *Distributed Reflective Denial-of-Service* (DRDoS), Arsitektur ini didasarkan pada tiga pilar kriptografis:

1. ***Handshake* Pembuktian Kepemilikan IP**: Untuk menutup celah serangan DRDoS.
2. ***Verifiable Random Functions* (VRF)**: Untuk pemilihan penguji yang tidak dapat dimanipulasi.
3. ***Zero-Knowledge Proofs* (ZK-SNARKs)**: Untuk verifikasi hasil tes yang *trustless* (tanpa kepercayaan).

Proses verifikasi koneksi dirancang untuk menghilangkan kepercayaan subyektif dan menggantinya dengan kepastian matematis. Berikut adalah alur kerja teknis dalam PoB:

- **Fase 1: Inisiasi, Pemilihan Penguji, dan *Handshake* Keamanan**
  Tahap ini memastikan bahwa setiap ujian dimulai dengan adil dan para pengujinya dipilih dengan cara yang tidak dapat dimanipulasi untuk mencegah kolusi.

1. **Inisiasi Tes**: Sebuah *node* ("Kandidat") yang ingin membuktikan kualitas koneksinya menyiarkan sebuah transaksi khusus ke jaringan, menandakan kesiapannya untuk diuji.
2. **Pemilihan Penguji (via VRF)**: Untuk memastikan proses pengujian adil dan mencegah persekongkolan, pemilihan penguji dilakukan melalui *Verifiable Random Function* (VRF).
    - Protokol mengambil data publik yang selalu baru dan tidak dapat diprediksi sebagai "nomor acuan" lotre (misalnya, *hash* dari blok yang baru saja dibuat).
    - Setiap *validator* aktif menggunakan kunci privat mereka (rahasia) dan nomor acuan publik untuk menjalankan fungsi VRF, menghasilkan nomor acak unik dan bukti kriptografis kecil.
    - Jaringan memverifikasi bukti tersebut, lalu memilih 5 hingga 8 *validator* dengan nomor acak terendah sebagai "Komite Penguji". Proses ini tidak dapat dimanipulasi karena tidak ada yang bisa memprediksi atau memengaruhi *output* VRF, secara efektif membubarkan potensi kartel. Ini seperti lotre yang adil, memastikan pembentukan Komite Penguji sepenuhnya acak dan tahan manipulasi.
3. ***Handshake* Anti-DRDOS**: Sebelum pengiriman data bervolume tinggi, setiap anggota Komite Penguji melakukan *challenge-response handshake* dengan Kandidat untuk memverifikasi kepemilikan alamat IP.
    - Penguji mengirimkan pesan acak unik (*nonce*) yang telah ditandatangani secara digital ke alamat IP Kandidat.
    - Kandidat harus menandatangani *nonce* tersebut dengan kunci privat *node*-nya dan mengirimkannya kembali.
    - Hasilnya, *handshake* ini membuktikan bahwa operator *node* benar-benar mengontrol alamat IP tersebut. Pengiriman data uji bervolume tinggi hanya dimulai setelah *handshake* berhasil, sepenuhnya menutup vektor serangan DRDoS. Ini mencegah serangan DDoS reflektif (DRDoS).

- **Fase 2: Komitmen, Transmisi, dan Eksekusi Terbukti**
  Ini adalah inti dari proses PoB, di mana ujian yang sebenarnya dilakukan antara Kandidat dan setiap anggota Komite Penguji secara paralel.
    1. **Komitmen Data Uji**: Setiap Penguji secara lokal menghasilkan satu blok data acak (misalnya, 8 MB). Alih-alih langsung mengirimkannya, Penguji hanya menyiarkan "sidik jari" digitalnya (*hash*) ke jaringan. Ini adalah "komitmen" atau janji bahwa data inilah yang akan digunakan, dan Penguji tidak bisa lagi mengubah data uji setelah komitmen ini dipublikasikan. Ini seperti Penguji menyegel materi ujian.
    2. **Transmisi Data**: Setelah komitmen diterima, Penguji kemudian mengirimkan blok data 8 MB yang asli ke Kandidat. *Node* Kandidat secara internal akan menyalakan *stopwatch* presisi tinggi saat *byte* pertama data tiba dan menghentikannya saat *byte* terakhir diterima, mencatat durasi transmisi mentah. Ini untuk mengukur kecepatan (*throughput*) dan waktu respons (*latency*).
    3. **Eksekusi Terbukti**: Setelah menerima semua data, Kandidat wajib melakukan sebuah komputasi yang telah ditentukan pada data tersebut, misalnya menghitung *Merkle Root*-nya. Ini adalah langkah krusial untuk membuktikan bahwa data tersebut tidak hanya diterima, tetapi juga diproses.
- **Fase 3: Pembuktian *Zero-Knowledge* dan Verifikasi Jaringan**
  Pada tahap akhir, seluruh jaringan akan memvalidasi hasil ujian dan memberikan skor akhir. Ini adalah fase yang paling transformatif, di mana Kandidat tidak lagi menyiarkan

hasil pengukurannya yang subjektif.

1. **Pembuatan Bukti (ZK-SNARKs)**: Kandidat menggunakan semua bahan—komitmen *hash* dari penguji, *Merkle Root* yang ia hitung, dan durasi transmisi yang tercatat—dan memasukkannya ke dalam algoritma ZK-SNARK (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*). Hasilnya adalah sebuah bukti kriptografis yang sangat kecil, secara matematis menegaskan: "Saya membuktikan bahwa saya menerima data yang cocok dengan komitmen awal, melakukan komputasi yang benar, dan seluruh proses ini memakan waktu persis sekian milidetik". Ini seperti membuktikan Anda tahu rahasia tanpa mengungkapkannya, memungkinkan Kandidat membuktikan hasil kerjanya tanpa menunjukkan proses atau data mentah.
2. **Publikasi Bukti**: Kandidat menyiarkan bukti ZK-SNARK yang kecil itu ke seluruh jaringan, bersama dengan *input/output* publik (*hash* komitmen, *Merkle root* hasil, dan durasi waktu). Ini mencegah pelaporan hasil yang dimanipulasi.
3. **Verifikasi Instan oleh Jaringan**: Setiap *node* lain di jaringan dapat menjalankan fungsi verifikasi yang sangat cepat pada bukti tersebut. Jika bukti valid, jaringan kini memiliki kepastian matematis bahwa Kandidat benar-benar menerima dan memproses data dari Penguji dalam durasi waktu yang diklaim. Proses verifikasi ini tidak lagi bergantung pada "laporan jujur" dari siapa pun, menjadikan PoB objektif dan *trustless*.
4. **Agregasi dan Penilaian Skor**: Protokol mengumpulkan durasi waktu yang telah terverifikasi dari semua anggota Komite Penguji. Untuk menghindari hasil yang tidak adil karena anomali jaringan, protokol mengambil nilai tengah (*median*) dari semua durasi yang valid (bukan rata-rata). Nilai median ini kemudian digunakan untuk menghitung skor PoB akhir berdasarkan target protokol (misalnya, jika waktu transmisi 8 MB adalah 1 detik, maka *throughput*-nya adalah 8 MB/s). Jika skor akhir memenuhi ambang batas minimal (misalnya, 0.85), maka Kandidat dinyatakan lulus ujian dan status *validator*-nya dikonfirmasi.

### 3.1.4. Kesimpulan Arsitektural dari PoB

Dengan arsitektur ini, *Proof of Bandwidth* berubah secara fundamental:

- **Dari Subjektif menjadi Objektif**: Keberhasilan tes didasarkan pada bukti kriptografis yang dapat diverifikasi oleh siapa saja, bukan laporan yang bisa dimanipulasi.
- **Tahan Kolusi**: Pemilihan penguji via VRF membuat koordinasi antar anggota kartel menjadi sangat sulit dan tidak efektif.
- **Aman dari Serangan Eksternal**: *Handshake* keamanan secara definitif menutup vektor serangan DRDoS.
- **Menjadi *Trustless***: Jaringan tidak perlu lagi "mempercayai" *validator* untuk melaporkan hasil dengan jujur. Prinsip "jangan percaya, verifikasi" kini diterapkan sepenuhnya.

## 3.2. Proof of History (PoH): Utilitas Pengoptimalan Waktu

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

PoB. PoH bekerja dengan membuat sekuens *hash* di mana *output* dari satu *hash* menjadi *input* untuk *hash* berikutnya. Dengan menyertakan *timestamp* dan urutan secara kriptografis di dalam *header* blok, PoH mengurangi waktu sinkronisasi dan kemungkinan terjadinya *fork*. Ini secara efektif memisahkan masalah pengurutan (*ordering*) dari masalah kesepakatan (*agreement*), memungkinkan PoB fokus hanya pada validasi produsen blok yang sah.

### 3.3. Perbandingan Model Keamanan: PoB vs. PoW

Sangat penting untuk memahami bahwa PoB tidak bekerja seperti *Proof of Work* (PoW).

- PoW mengamankan jaringan dengan memaksa peserta (penambang) untuk berlomba memecahkan teka-teki kriptografis yang boros energi dan membutuhkan kekuatan komputasi masif. Keamanan berasal dari mahalnya biaya untuk memenangkan perlombaan ini.
- **PoB mengamankan jaringan dengan memaksa peserta (*validator*) untuk lulus "tes kebugaran jaringan" yang ketat dan berkelanjutan**. Keamanan berasal dari sulitnya untuk secara konsisten memalsukan koneksi internet berkualitas tinggi di hadapan banyak penguji acak. Skor PoB adalah laporan hasil tes, bukan solusi dari sebuah teka-teki.

## Bab 4: Arsitektur Protokol dan Jaringan

### 4.1. Siklus Hidup Blok (Interval 30 Detik)

Setiap blok di jaringan RNR diciptakan, disebarkan, dan difinalisasi dalam sebuah siklus waktu yang terstruktur ketat selama **30 detik** untuk memaksimalkan kecepatan dan prediktabilitas.

- **[Tahap Pra-Pembuatan Blok]**: Sebelum siklus dimulai, *validator* terpilih (*Proposer*) menghitung kapasitas blok maksimum yang diizinkan berdasarkan kecepatan unggah terukurnya sendiri dan rumus Kapasitas Blok Dinamis. *Proposer* kemudian memilih transaksi dari *mempool* hingga batas aman ini.
- **Fase 1: Propagasi & Verifikasi Awal (0-10 Detik)**:
    - **Detik 0-1**: *Proposer* membuat blok dengan ukuran yang sudah dijamin aman dan wajib menyiarkannya ke semua *peer* yang terhubung dengannya dalam waktu kurang dari 1 detik.
    - **Detik 1-10**: Setiap *validator* yang menerima blok ini akan segera melakukan verifikasi cepat pada *header* blok, tanda tangan *proposer*, urutan PoH, dan skor PoB *proposer*. Jika verifikasi berhasil, *validator* wajib menyiarkan ulang blok tersebut ke *peer*-nya dalam kurang dari 1 detik. Proses siaran berantai ini bertujuan agar blok diterima oleh **minimal 85% dari total *validator* aktif sebelum detik ke-10**, sesuai target propagasi jaringan.
- **Fase 2: Verifikasi Penuh & Voting (10-25 Detik)**:
    - Secara paralel dengan proses propagasi, setiap *validator* yang telah menerima blok akan melakukan verifikasi penuh. Proses ini memeriksa validitas setiap transaksi di dalam blok, memastikan tidak ada *double-spending*, dan semua transaksi sesuai dengan aturan protokol.
    - Setelah verifikasi penuh berhasil, setiap *validator* akan membuat dan menyiarkan pesan "*vote*" (suara persetujuan) untuk *hash* blok tersebut.
- **Fase 3: Buffer & Finalitas (25-30 Detik)**:

- Jendela waktu 5 detik ini berfungsi sebagai periode *buffer* untuk memberikan toleransi terhadap keterlambatan jaringan (*network latency/jitter*), memastikan sebagian besar pesan "*vote*" sudah diterima oleh mayoritas *validator*.
- Pada akhir detik ke-30, jika sebuah blok telah menerima "*vote*" dari **lebih dari 85% *validator***, blok tersebut dianggap **final dan tidak dapat diubah lagi**. Siklus baru untuk blok berikutnya pun dimulai.

## 4.2. Kapasitas Blok Dinamis: Pencegahan Kemacetan

**Ukuran maksimum setiap blok tidak statis, melainkan disesuaikan oleh *Proposer* sebelum blok dibuat untuk mencegah kemacetan (*congestion*) jaringan**. Ini memastikan blok yang dibuat sesuai dengan kapabilitas pengiriman *Proposer* dalam jendela waktu 10 detik.

- **Rumus**: Kapasitas Blok Maks = 0.30 × Upload_Validator (MB/s) × 10 detik

## 4.3. Logika Resolusi Fork

Jika terjadi *fork* (dua *validator* membuat blok pada ketinggian yang sama), jaringan akan memilih rantai berdasarkan urutan prioritas:

1. **Bobot PoB Kumulatif Tertinggi**: Memilih rantai dengan total bobot PoB tertinggi (Σ difficulty_target).
2. ***Timestamp* PoH Terkecil**: Jika bobot kumulatifnya sama, jaringan akan memilih rantai dengan *timestamp* PoH paling awal.
3. ***Hash* Blok Terkecil**: Sebagai pilihan terakhir jika kedua metrik di atas identik, jaringan akan memilih rantai dengan nilai *hash* blok terkecil secara leksikografis.

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

## 4.4. Kecepatan Finalitas Transaksi

**Sebuah transaksi dapat dianggap final dalam satu siklus blok (30 detik) pada kondisi jaringan ideal**. Klaim ini didasarkan pada fakta bahwa PoH menyediakan urutan transaksi yang definitif sebelum konsensus. RNR dengan PoH dan aturan resolusi *fork* yang jelas, memungkinkan tercapainya tingkat finalitas ekonomi yang sangat tinggi dengan sangat cepat. Finalitas ekonomi berarti biaya untuk membatalkan transaksi yang telah dikonfirmasi menjadi sangat mahal sehingga secara praktis tidak mungkin terjadi.

# Bab 5: Partisipasi Jaringan: Peran dan Aturan Validator

## 5.1. Proses Menjadi Validator: Kualifikasi dan Onboarding

### 5.1.1. Kualifikasi Awal: Skor PoB Minimal

Kualifikasi fundamental adalah kemampuan untuk membuktikan dan mempertahankan **Skor PoB minimal 0.85**. Kegagalan dalam memenuhi standar ini akan mengakibatkan penolakan

masuk atau pengeluaran dari set *validator* aktif.

### 5.1.2. Biaya Masuk Dinamis: Mekanisme Anti-Sybil

Untuk menyeimbangkan keamanan dan aksesibilitas, **biaya masuk untuk menjadi *validator* tidak bersifat statis, melainkan disesuaikan secara dinamis berdasarkan jumlah *validator* aktif di jaringan**. Biaya ini diwajibkan untuk menyediakan kapasitas *bandwidth* yang setara dengan durasi operasional *validator* standar.

- **Fase Awal (<100 Validator)**: Biaya masuk diatur pada tingkat dasar 6 jam kapasitas *bandwidth* operasional untuk mendorong pertumbuhan awal.
- **Fase Pertumbuhan (100-1000 Validator)**: Biaya masuk meningkat secara linear seiring bertambahnya jumlah *validator* untuk meningkatkan biaya serangan Sybil secara progresif (misalnya, meningkat 1 jam untuk setiap 100 *validator* baru).
- **Fase Dewasa (> 1000 Validator)**: Biaya masuk mencapai puncaknya di 24 jam kapasitas *bandwidth* untuk memaksimalkan keamanan pada jaringan yang sudah matang.

## 5.2. Siklus Hidup dan Tanggung Jawab Validator Aktif

Setelah diterima ke dalam set *validator* aktif, *node* memiliki tanggung jawab krusial:

- **Partisipasi dalam Konsensus**: *Validator* wajib berpartisipasi aktif dalam setiap putaran konsensus, yang mencakup menerima, memverifikasi secara penuh, dan memberikan suara (*vote*) untuk blok-blok kandidat.
- **Kewajiban Propagasi Data**: *Validator* berfungsi sebagai tulang punggung jaringan. Mereka wajib menyiarkan ulang blok dan transaksi yang telah diverifikasi ke *peer* mereka dalam batas waktu yang sangat singkat (≤ 1 detik) untuk menjamin tercapainya target propagasi jaringan.
- **Re-Verifikasi PoB Berkala: Pemeliharaan Status**: Status *validator* tidak permanen. Setiap *validator* harus secara periodik (misalnya, setiap 100 blok) menjalani kembali "ujian koneksi PoB". Proses ini jauh lebih ringan daripada "Biaya Masuk Dinamis" dan dirancang sebagai tugas latar belakang yang tidak mengganggu tugas utama *validator*.
    - **Jika Gagal**: *Validator* akan ditempatkan dalam status "*probation*" (masa percobaan). Jika gagal lagi pada ujian berikutnya, mereka akan dikeluarkan sementara dari set *validator* aktif dan kehilangan hak untuk mendapatkan imbalan blok hingga berhasil lolos ujian PoB lagi. Mekanisme ini memastikan kesehatan dan kecepatan jaringan selalu terjaga.

## 5.3. Sistem Reputasi dan Jenjang Karier

RNR menerapkan sistem reputasi sebagai jenjang karier bagi *validator*.

- **Inisiasi**: *Node* yang baru divalidasi akan memulai dengan skor reputasi dasar (*baseline*). Protokol memastikan *node* baru tetap menerima kesempatan yang adil untuk dipilih sebagai *peer* dalam tugas-tugas jaringan rutin.
- **Akumulasi**: Skor reputasi akan meningkat secara bertahap seiring dengan kinerja positif yang konsisten (misalnya, partisipasi konsensus tanpa cela, keberhasilan re-verifikasi, waktu aktif yang tinggi).
- **Prioritas**: *Node* dengan skor reputasi yang tinggi akan diprioritaskan oleh protokol untuk dipilih sebagai *peer* dalam fungsi-fungsi jaringan yang paling kritis. Mekanisme pembobotan ini memperkuat keamanan jaringan dengan mengandalkan *validator* yang

paling terbukti handal, tanpa mengecualikan partisipasi dari *validator* yang lebih baru.

## 5.4. Aturan Protokol Kritis dan Sanksi

- **Kapasitas Blok Dinamis**: Ukuran blok maksimum ditentukan oleh *Proposer* sebelum pembuatan blok, berdasarkan hasil pengukuran PoB terakhirnya. Ini adalah aturan protokol yang ketat untuk mencegah kemacetan (*congestion*) jaringan.
- **Sanksi Pelanggaran**: Tindakan yang merusak integritas jaringan, seperti memproduksi blok yang melampaui kapasitas yang dihitung atau mengirimkan bukti PoB yang dimanipulasi, akan dikenakan sanksi berjenjang. Sanksi ini dapat berupa denda *bandwidth*, penurunan skor reputasi, pengeluaran sementara, hingga larangan permanen (*permanent ban*) dari jaringan.

# Bab 6: Model Keamanan

## 6.1. Filosofi Keamanan: Integritas Melalui Transparansi

Keamanan RNR tidak berasal dari penyembunyian data transaksi. Sebaliknya, **semua transaksi bersifat transparan**. Keamanan dicapai melalui dua pilar:

1. **Keamanan Kepemilikan (Tanda Tangan Digital)**: Setiap transaksi harus memiliki tanda tangan digital yang valid, yang hanya bisa dibuat oleh pemilik kunci privat yang sah. Ini membuktikan otorisasi transaksi.
2. **Keamanan Histori (Rantai *Hash* yang Tak Terpecahkan)**: Setiap blok terhubung secara kriptografis ke blok sebelumnya melalui *hash*. Mengubah satu transaksi di masa lalu akan merusak seluruh rantai, membuatnya mudah terdeteksi.

Tugas *validator* bukanlah mendekripsi data, melainkan memverifikasi keaslian tanda tangan dan keutuhan rantai. Dengan tidak mengimplementasikan *smart contract* yang kompleks (secara bawaan), RNR secara desain menghilangkan seluruh kategori vektor serangan yang umum terjadi pada *platform* lain.

## 6.2. Mitigasi Serangan Jaringan

- **Serangan Sybil dan DDoS**: RNR menerapkan beberapa strategi pertahanan:
    1. **Biaya Masuk Dinamis**: Membuat serangan Sybil skala besar menjadi tidak ekonomis seiring pertumbuhan jaringan, karena biaya pendaftaran *node* baru akan menjadi mahal.
    2. ***Rate Limiting* Permintaan Verifikasi**: *Validator* aktif akan membatasi laju permintaan verifikasi dari *node* baru yang tidak dikenal untuk mencegah serangan banjir.
    3. **Sistem Reputasi Terdesentralisasi**: *Validator* dengan reputasi tinggi akan diprioritaskan saat memilih *peer* untuk ujian koneksi atau propagasi blok, mempersulit *node* baru berbahaya untuk langsung memengaruhi inti jaringan.
    4. **Topologi Jaringan Acak**: Setiap *node* akan terhubung ke sejumlah *peer* yang dipilih secara acak, membuat penyerang tidak dapat dengan mudah menargetkan dan mengisolasi *validator* tertentu.

## 6.3. Mitigasi Serangan *Onboarding* oleh *Node* Baru

Protokol RNR-30 memiliki mekanisme untuk mendeteksi dan menghukum calon *node* yang mencoba mengganggu proses verifikasi mereka sendiri. Jika beberapa *validator* yang ditugaskan untuk menguji satu kandidat *node* yang sama secara bersamaan melaporkan serangan DDoS yang berasal dari alamat IP kandidat tersebut, protokol akan menandai kandidat tersebut sebagai pelaku serangan dan secara otomatis memasukkan alamat IP-nya ke dalam daftar hitam (*blacklist*) jaringan untuk periode waktu yang signifikan.

## 6.4. Mekanisme Pertahanan Terhadap Validator Berbahaya (Pengkhianat)

Jaringan RNR dilindungi dari *validator* aktif yang bertindak jahat melalui tiga lapisan pertahanan:

1. **Kegagalan PoB Otomatis**: *Validator* yang menggunakan sumber dayanya untuk menyerang jaringan kemungkinan besar akan gagal dalam siklus re-verifikasi PoB berkala. Ini akan menyebabkannya masuk masa percobaan (*probation*) dan dikeluarkan secara otomatis.
2. **Degradasi Reputasi**: Perilaku non-kooperatif, seperti menolak berpartisipasi dalam konsensus atau menyiarkan blok, akan secara cepat menurunkan skor reputasi *validator*, mengisolasinya dari fungsi jaringan yang krusial.
3. **Ejeksi Paksa melalui Tata Kelola (*Governance*)**: Sebagai jalan terakhir, **mayoritas super (> 85%) dari *validator* yang tersisa dapat secara kolektif mengajukan proposal darurat melalui sistem tata kelola untuk mengeluarkan *validator* berbahaya secara permanen dari jaringan**.

# Bab 7: Tokenomics (RNR)

## 7.1. Filosofi Ekonomi dan Utilitas Token

Model ekonomi RNR dibangun di atas tiga pilar: menginsentifkan keamanan jaringan melalui imbalan yang adil, menciptakan nilai jangka panjang melalui mekanisme deflasi, dan menyediakan utilitas fundamental di dalam ekosistem. Utilitas utama dari token RNR mencakup:

- Menjadi medium untuk pembayaran biaya transaksi.
- Berfungsi sebagai alat untuk berpartisipasi dalam tata kelola *on-chain*.
- Menjadi mekanisme imbalan bagi *validator* dan kontributor kesehatan jaringan.

## 7.2. Emisi dan Distribusi Imbalan Blok

- **Emisi Awal**: Imbalan blok awal ditetapkan sebesar **100 RNR per blok**.
- **Jadwal Pengurangan**: Untuk mengontrol inflasi, imbalan blok akan berkurang sebesar 1 RNR setiap 1.000.000 blok.
- **Imbalan Minimum Abadi**: Imbalan tidak akan pernah mencapai nol, melainkan akan berhenti pada **nilai minimum 1 RNR per blok selamanya**. Ini menjamin bahwa selalu ada insentif ekonomi dasar bagi *validator* untuk terus mengamankan jaringan, bahkan di masa depan yang jauh.

- **Struktur Distribusi**:
    - **80% dari imbalan blok** dialokasikan kepada *validator* yang berhasil membuat dan menyiarkan blok (*Proposer*).
    - **20% sisanya** didistribusikan secara merata kepada hingga 20 *node* teratas yang berkontribusi pada data pengukuran PoB yang valid untuk blok tersebut. Struktur ini secara eksplisit memberi insentif kepada *node* untuk menjaga koneksi berkualitas tinggi, bahkan jika mereka tidak terpilih sebagai *Proposer*.
    - Sisa pecahan dari pembagian imbalan (setelah pembulatan ke bawah 8 desimal) akan dibakar (*burned*), menjadikannya mekanisme deflasi minor.

## 7.3. Mekanisme Biaya Transaksi dan Pembakaran (*Burning*)

RNR mengadopsi mekanisme biaya transaksi ganda yang canggih, mirip dengan EIP-1559 Ethereum.

- ***Base Fee* (Biaya Dasar)**: Setiap transaksi dikenakan biaya dasar yang dihitung sebesar **0.00000001% dari nilai transaksi**. **Biaya ini dibakar (*burned*), menghapusnya secara permanen dari peredaran**. Ini berfungsi sebagai mekanisme deflasi minor yang nilainya meningkat seiring dengan meningkatnya aktivitas ekonomi di jaringan.
- ***Priority Fee* (Biaya Prioritas)**: Pengguna dapat secara opsional menambahkan biaya prioritas pada transaksi mereka untuk mendapatkan inklusi yang lebih cepat ke dalam blok saat jaringan sedang sibuk. Biaya ini diberikan langsung kepada *validator* pembuat blok dan berfungsi sebagai insentif tambahan.

# Bab 8: Model Tata Kelola (*Governance*)

## 8.1. Prinsip Dasar: 1 Validator, 1 Suara

**RNR mengadopsi model tata kelola "satu *validator*, satu suara"**. Prinsip ini secara fundamental dirancang untuk memastikan desentralisasi kekuasaan. Berbeda dengan model *coin-based voting*, model RNR mendasarkan hak suara pada partisipasi aktif dan terverifikasi (melalui PoB). Ini menciptakan sebuah meritokrasi di mana kontributor aktif menjadi pengambil keputusan]. Resistensi Sybil untuk tata kelola secara langsung terkait dengan mekanisme konsensus PoB itu sendiri, di mana biaya operasional dan "biaya masuk" menjadi penghalang ekonomi.

## 8.2. Lingkup dan Proses Proposal

*Validator* aktif dapat mengajukan proposal untuk mengubah parameter protokol yang dapat diatur (*governable parameters*).

- **Lingkup**: Parameter yang dapat diubah mencakup, namun tidak terbatas pada: metrik dan target PoB, jumlah imbalan blok, struktur biaya transaksi, parameter sanksi, dan peningkatan fungsionalitas protokol.
- **Proses**: *Validator* mengajukan proposal dengan menyiarkan jenis transaksi khusus (*Proposal Transaction*). Transaksi ini harus berisi definisi perubahan yang diusulkan secara terstruktur dan mungkin memerlukan deposit RNR (yang akan dibakar) untuk mencegah *spam*. Proposal yang valid akan memasuki periode pemungutan suara.

## 8.3. Mekanisme Voting dan Finalitas Keputusan

- **Mekanisme**: Selama periode pemungutan suara, *validator* lain memberikan suara dengan menyiarkan *Vote Transaction* yang merujuk pada ID proposal.
- **Ambang Batas Keputusan**: Sebuah proposal dianggap diterima dan akan diimplementasikan jika disetujui oleh **mayoritas super (*supermajority*) yang melebihi 85% dari total *validator* aktif**. Ambang batas yang sangat tinggi ini dipilih secara sadar untuk memastikan bahwa setiap perubahan kritis terhadap protokol inti memiliki dukungan yang luar biasa dari jaringan, melindungi stabilitas dan mencegah terjadinya *hard fork* yang kontroversial.

# Bab 9: Parameter Awal Jaringan

## 9.1. Tabel Parameter

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

| Parameter | Nilai |
|---|---|
| Waktu Blok | 30 detik |
| Target Propagasi | 85% *node* dalam ≤10 detik |
| Jendela Retarget PoB | Setiap 50 blok |
| Skor PoB Minimal | 0.85 |
| Minimum Peer Pengukuran | 8 *peer* |
| Jumlah Peer Sampling | 10 *peer* |
| Batas Penyesuaian *Difficulty* | ±20% per jendela *retarget* |
| Batas Tx Pembuatan *Wallet* | 15 transaksi per blok |
| Penerima Imbalan PoB | Hingga 20 *node* kontributor teratas |

## 9.2. Penjelasan Detail Parameter

- **Jendela *Retarget* dan Penyesuaian *Difficulty* Adaptif**: Setiap 50 blok (sekitar 25 menit), jaringan akan mengevaluasi jumlah rata-rata *validator* aktif selama periode tersebuttersebut. *Difficulty* (standar kelulusan tes PoB) akan disesuaikan secara dinamis (maksimal ±20% per jendela *retarget*) untuk menjaga agar jumlah *validator* aktif di jaringan tetap berada dalam rentang yang sehat. Jika jumlah *validator* terlalu tinggi, protokol akan memperketat target metrik PoB; jika terlalu rendah, protokol akan melonggarkan target.
- **Proses *Peer Sampling* dan Pengukuran**: Untuk memastikan hasil tes PoB objektif dan tahan terhadap manipulasi, sebuah *node* akan mengambil sampel acak sebanyak 10 *validator* dari daftar *validator* aktif sebagai *peer* penguji. Hasil tes PoB dari *node* penguji akan dianggap valid hanya jika ia berhasil mendapatkan hasil pengukuran yang valid dari minimal 8 dari 10 *peer* yang di-*sampling*. Aturan ini memastikan skor PoB tidak bergantung pada satu koneksi tunggal dan mempersulit *node* berbahaya untuk berkolusi.
- **Batas Transaksi Pembuatan *Wallet***: Ini adalah mekanisme pertahanan terhadap serangan *spam* dan *state bloat* (penggembungan data jaringan). Dengan membatasi jumlah transaksi "pembuatan *wallet*" (atau transaksi pertama dari sebuah *wallet*) hingga 15 per blok, protokol secara efektif membatasi laju pembuatan akun baru. Ini tidak akan

memengaruhi pengguna normal, tetapi akan membuat serangan *spam* menjadi sangat lambat dan tidak efisien bagi penyerang.

# Referensi dan Landasan Teoretis


- *Bitcoin: A Peer-to-Peer Electronic Cash System* (Satoshi Nakamoto, 2008)
- *Solana: A new architecture for a high-performance blockchain* (Anatoly Yakovenko, 2017)
- *Peercoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* (Sunny King & Scott Nadal, 2012)
- *Ethereum Improvement Proposal 1559 (EIP-1559)* (Vitalik Buterin, et al.)
- *The Byzantine Generals Problem* (Leslie Lamport, Robert Shostak, and Marshall Pease, 1982)
- *The Sybil Attack* (John R. Douceur, 2002)
- *What Is A Distributed Reflection Denial of Service Attack?* | Twingate
- *libp2p: A Modular Network Stack* (Protocol Labs)
- *UDP-Based Amplification Attacks* | CISA
- *Projects < Digital Currency Initiative (DCI)* - MIT Media Lab
- *What Is a DrDoS Attack? - Definition by ThreatDotMedia* - Threat.media
- *DDoS Amplification Attacks* - Noction
- *DNS amplification DDoS attack* | Cloudflare
- *What is DNS Amplification* | *DDoS Attack Glossary* - Imperva
- *Challenge-response authentication* - Wikipedia
- *libp2p* | IPFS Docs
- *libp2p*
- *Peer Discovery and Routing* - libp2p
- *Challenges Using the Linux Network Stack for Real-Time Communication*
- *Sending data from Windows is slow over any network with high latency but linux is fast*
- *Is it possible to process millions of datagrams per second with Windows?* - Super User
- *Throughput comparison of Windows and Linux client-server operating systems on IPv4 and IPv6* - ResearchGate
- *TCP Window Scaling // Windows vs Linux // Crazy Performance Difference* - Reddit
- *On the Performance of TCP implementations of Linux and Windows* - Super User
- *Cross-platform normalization of microarray and RNA-seq data for machine learning applications* - PMC
- *(PDF) Evaluating Cross-Platform Normalization Methods for Integrated Microarray and RNA-seq Data Analysis* - ResearchGate
- *Cross-platform normalization enables machine learning model training on microarray and RNA-seq data simultaneously* - ResearchGate
- *Gossipsub v1.1 brings hardening extensions to PubSub* | IPFS Blog & News


# Lampiran - Pertanyaan Umum (FAQ) dan Rasional Desain

Bagian ini membahas beberapa pertanyaan umum dan memberikan justifikasi untuk keputusan desain arsitektur yang fundamental dalam protokol RNR, dirancang untuk membantu pembaca

memahami konsep-konsep kunci dengan cepat.

**T: Apakah *Proof of Bandwidth* (PoB) sama dengan "menambang" di *Proof of Work* (PoW)?**
J: Tidak, keduanya sangat berbeda. PoW adalah kompetisi komputasi untuk memecahkan teka-teki kriptografis yang boros energi. Sebaliknya, PoB adalah proses verifikasi atau "tes kebugaran" yang mengukur kualitas koneksi jaringan sebuah *node*. PoB tidak memecahkan teka-teki, melainkan melaporkan hasil pengukuran, membuatnya jauh lebih efisien. Analoginya, PoW seperti berlomba memecahkan teka-teki sihir untuk membuka pintu kastil, sementara PoB adalah proses seleksi ketat untuk menjadi penjaga elit kastil yang tepercaya.

**T: Jika semua transaksi transparan, bagaimana jaringan RNR bisa dianggap aman?**
J: Keamanan RNR tidak berasal dari penyembunyian data (*privasi*), melainkan dari integritas dan otentisitas data yang diverifikasi secara kriptografis. Transparansi adalah sebuah fitur, bukan kelemahan. Keamanan dijamin melalui dua pilar: **Tanda Tangan Digital** (memastikan setiap transaksi hanya bisa diotorisasi oleh pemilik kunci privat yang sah) dan **Rantai *Hash* yang Tak Terpecahkan** (memastikan histori transaksi tidak dapat diubah setelah dicatat dalam blok). Tugas *validator* bukanlah mendekripsi, melainkan memverifikasi bukti-bukti kriptografis ini.

**T: Apa sebenarnya fungsi *Proof of History* (PoH)? Apakah itu bagian dari konsensus?**
J: PoH bukanlah mekanisme konsensus itu sendiri, melainkan sebuah utilitas pengoptimalan. Anggap PoH sebagai "sekretaris super cepat" yang tugasnya hanya satu: memberi stempel waktu dan nomor urut pada setiap transaksi yang masuk bahkan sebelum para direktur (*validator*) rapat untuk menyetujuinya. Ini membuat proses "rapat" (konsensus PoB) menjadi jauh lebih cepat karena urutan peristiwanya sudah jelas dan terbukti secara kriptografis.

**T: Mengapa waktu blok ditetapkan selama 30 detik? Mengapa tidak lebih cepat?**
J: Waktu blok 30 detik dipilih sebagai **keseimbangan optimal antara kecepatan finalitas dan stabilitas jaringan**. Waktu ini memberikan ruang yang cukup (10 detik) untuk fase propagasi, memastikan bahwa bahkan dalam kondisi jaringan global yang tidak ideal, sebuah blok baru memiliki cukup waktu untuk mencapai mayoritas *validator*. Ini secara signifikan mengurangi kemungkinan terjadinya *fork* yang tidak disengaja dan meningkatkan prediktabilitas jaringan.

**T: Apa tujuan dari "Kapasitas Blok Dinamis"? Bukankah lebih baik jika ukurannya tetap?**
J: Kapasitas Blok Dinamis adalah **mekanisme pencegahan kemacetan (*congestion*) yang proaktif**. Daripada memiliki ukuran blok tetap yang mungkin terlalu besar untuk disiarkan oleh *validator* dengan koneksi yang lebih lambat, protokol memastikan bahwa *validator* yang membuat blok hanya akan membuat blok dengan ukuran yang mampu ia siarkan dalam jendela waktu 10 detik. Ini memastikan "pengirim" tidak pernah membebani jaringan lebih dari kemampuannya, menjaga alur data tetap lancar.

**T: Apa bedanya "Biaya Masuk *Bandwidth*" untuk *node* baru dan "Re-Verifikasi PoB"?**
J: Keduanya adalah tes yang berbeda dengan tujuan yang berbeda.

- **Biaya Masuk (Ujian SIM)**: Ini adalah tes awal yang panjang dan berat (setara 6-24 jam kapasitas *bandwidth*). Tujuannya adalah sebagai penghalang masuk yang signifikan untuk menyaring penyerang dan membuktikan keseriusan serta kapasitas *node* baru.
- **Re-Verifikasi (Tes Kesehatan Rutin)**: Ini adalah tes singkat dan ringan yang dilakukan

secara berkala (setiap 100 blok) oleh *validator* aktif. Tujuannya hanya untuk memastikan kualitas koneksi mereka tidak menurun seiring waktu.

**T: Bukankah syarat PoB akan menyebabkan monopoli oleh negara/wilayah dengan internet terbaik?**

J: Risiko sentralisasi geografis ini ada, namun dimitigasi melalui beberapa cara:

1. **Standar yang Wajar**: Target PoB (misalnya, 7 MB/s *upload*) dirancang untuk menjadi standar koneksi "berkualitas baik", bukan standar "elit dunia". Ini dapat dicapai oleh banyak koneksi internet modern di luar pusat-pusat teknologi utama.
2. **Fokus pada Stabilitas**: PoB tidak hanya mengukur kecepatan, tetapi juga latensi dan keandalan (*packet loss*), memberikan kesempatan bagi koneksi yang stabil meskipun bukan yang tercepat.
3. **Tata Kelola**: Parameter PoB dapat disesuaikan melalui mekanisme tata kelola *on-chain*. Jika komunitas merasa syaratnya terlalu eksklusif, mereka dapat memberikan suara untuk mengubahnya agar lebih inklusif.

**T: Apa yang terjadi jika *validator* diserang atau berkhianat?**

J: Protokol memiliki tiga lapisan pertahanan:

1. **Re-Verifikasi PoB Otomatis**: *Validator* yang tidak responsif karena diserang atau bertindak jahat akan gagal dalam tes kesehatan berkala dan statusnya akan diturunkan atau dicabut secara otomatis.
2. **Sistem Reputasi**: Perilaku non-kooperatif akan menurunkan skor reputasi *validator*, mengisolasinya dari fungsi-fungsi jaringan yang kritis.
3. **Ejeksi Paksa melalui Tata Kelola**: Sebagai jalan terakhir, mayoritas super (> 85%) dari *validator* yang jujur dapat memberikan suara untuk mengeluarkan *validator* berbahaya secara permanen.