Published by LPPINPEST
Journal homepage: https://ejournal.lppinpest.org/index.php/jipetik/index

PEMODELAN KONSENSUS *PROOF-OF-WORK BLOCKCHAIN* MENGGUNAKAN SIMULINK DI MATLAB: STUDI PERFORMA DAN KEAMANAN

JIPETIK
Halaman 141-151

Rendi Prasetya

Fakultas Teknik dan Ilmu Komputer, Program Studi Teknik Informatika, Universitas Indraprasta PGRI, DKI Jakarta, Indonesia

Research paper
Informatika

Abstract

This research presents the modeling and simulation of the Proof-of-Work (PoW) consensus mechanism in a blockchain environment using Simulink in MATLAB. The objective is to analyze the performance and security implications of PoW under various operational conditions. The developed model integrates key elements such as miner hash rates, mining difficulty, block propagation, and network forks. Simulation results, illustrated through graphical visualizations, demonstrate how changes in these parameters affect network throughput, transaction confirmation latency, and the probability of a 51% attack. A comparative analysis of early simplified simulation scenarios and extended scenarios, along with visualizations comparing honest and attacker chain lengths, provides deep insights into block generation dynamics, chain stability, and vulnerability to attacks. This research provides insights into PoW's scalability challenges and security vulnerabilities, offering a platform to explore optimizations and mitigations.

Article Info
Article History:
Received 19/11/2025
Revised 17/12/2025
Accepted 30/12/2025
Available online 31/12/2025

Keywords:
Blockchain, Proof-of-Work (PoW), Simulink, Hash Rate, 51% Attack

JIPETIK, Vol 3, No. 2, 2025
pp. 141-151

ISSN 3031-481X
(media online)

Corresponding Author:
Rendi Prasetya
Email: prasetyarendi@gmail.com

Abstrak

Penelitian ini menyajikan pemodelan dan simulasi mekanisme konsensus *Proof-of-Work (PoW)* pada *blockchain* menggunakan *Simulink* di MATLAB. Tujuannya adalah untuk menganalisis performa dan implikasi keamanan dari PoW di bawah berbagai kondisi operasional. Model yang dikembangkan mengintegrasikan elemen kunci seperti *hash rate* penambang, kesulitan penambangan, propagasi blok, dan fork jaringan. Hasil simulasi, yang diilustrasikan melalui visualisasi grafis, menunjukkan bagaimana perubahan parameter ini memengaruhi throughput jaringan, latensi konfirmasi transaksi, dan probabilitas serangan 51%. Analisis komparatif dari skenario simulasi awal yang disederhanakan dan skenario yang diperpanjang, serta visualisasi perbandingan panjang rantai jujur dan penyerang, memberikan wawasan mendalam tentang dinamika pembuatan blok, stabilitas rantai, dan kerentanan terhadap serangan. Penelitian ini memberikan wawasan tentang tantangan skalabilitas dan kerentanan keamanan PoW, serta menawarkan platform untuk mengeksplorasi optimasi dan mitigasi serangan.

Kata kunci: *Blockchain*, *Proof-of-Work (PoW)*, *Simulink*, *Hash Rate*, Serangan 51%

Pendahuluan

Blockchain telah muncul sebagai teknologi transformatif yang mendasari mata uang kripto seperti Bitcoin dan aset digital lainnya. Inti dari keamanan dan desentralisasi *blockchain* terletak pada mekanisme konsensusnya. Di antara berbagai mekanisme konsensus, *Proof-of-Work* (PoW) adalah yang paling awal dan paling banyak digunakan, terutama oleh Bitcoin dan Ethereum (sebelum transisi ke PoS). PoW memastikan bahwa setiap blok transaksi yang ditambahkan ke rantai telah melalui proses komputasi yang intensif, sehingga sangat sulit dan mahal untuk memalsukan atau mengubah data historis (Nakamoto, 2008).

Meskipun PoW terbukti tangguh dalam menyediakan keamanan dan desentralisasi, ia menghadapi tantangan signifikan terkait skalabilitas dan efisiensi energi. Penambangan PoW membutuhkan daya komputasi yang besar, yang berkorelasi langsung dengan konsumsi energi yang tinggi. Selain itu, seiring dengan peningkatan jumlah transaksi, jaringan PoW dapat mengalami kemacetan, yang mengakibatkan latensi transaksi yang lebih tinggi dan biaya yang meningkat (Bonneau et al., 2015)
(Croman Kyleand Decker, 2016)

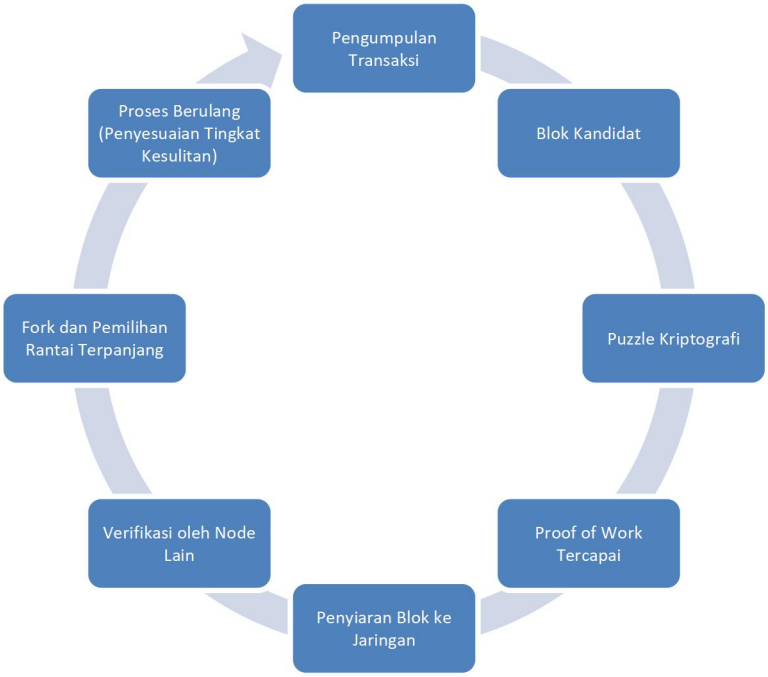
Aspek keamanan seperti serangan 51% juga menjadi perhatian, di mana satu entitas atau kelompok menguasai lebih dari 50% hash rate jaringan, memungkinkan mereka untuk memanipulasi transaksi dan melakukan *double-spending* (Sayeed & Marco-Gisbert, 2019)
(Sapirshtein Ayeletand Sompolinsky, 2017)

Memahami dinamika kompleks PoW, termasuk bagaimana *hash rate* penambang, kesulitan penambangan, dan propagasi blok memengaruhi performa dan keamanan, sangat penting. Simulasi menjadi alat yang ideal untuk tujuan ini, karena memungkinkan peneliti untuk menguji skenario "bagaimana-jika" tanpa perlu membangun jaringan blockchain sungguhan yang mahal dan kompleks (Pass Rafaeland Shi, 2018)
(Gervais et al., 2016) . MATLAB dan *Simulink* menyediakan lingkungan yang kuat untuk pemodelan dan simulasi sistem dinamis, menjadikannya pilihan yang sangat cocok untuk menganalisis perilaku *blockchain* PoW. Studi ini bertujuan untuk mengembangkan model *Simulink* yang merepresentasikan mekanisme konsensus PoW untuk menganalisis performa dan implikasi keamanannya secara sistematis.

Metodologi Penelitian

Untuk memodelkan konsensus *Proof-of-Work*, peneliti menggunakan *Simulink* di MATLAB. *Simulink* adalah lingkungan pemodelan visual berbasis blok untuk simulasi sistem dinamis dan *embedded systems*. Pendekatan ini memungkinkan representasi komponen *blockchain* PoW secara modular dan interkoneksi di antara mereka.

1. Mekanisme *Proof-of-Work* (PoW)



Gambar 1. Mekanisme Proof-of-Work

Proof-of-Work adalah mekanisme konsensus fundamental yang digunakan oleh banyak *blockchain* terdesentralisasi, seperti Bitcoin. Inti dari PoW adalah proses penambangan (*mining*), di mana penambang bersaing untuk memecahkan *puzzle* kriptografi yang kompleks untuk dapat menambahkan blok baru ke *blockchain*. Proses ini melibatkan beberapa langkah kunci:

a. Pengumpulan Transaksi: Penambang mengumpulkan transaksi-transaksi yang belum terkonfirmasi dari mempool dan mengumpulkannya ke dalam sebuah blok kandidat
b. Pemecahan *Puzzle* Kriptografi (*Hashing*): Untuk membuat blok menjadi valid, penambang harus menemukan sebuah nilai arbitrer yang disebut nonce (*number used once*). Nonce ini, ketika digabungkan dengan data blok (termasuk *header* blok dan *hash* dari blok sebelumnya), harus menghasilkan *hash* yang memenuhi kriteria target tertentu (misalnya, dimulai dengan sejumlah angka nol). Proses menemukan nonce ini adalah proses coba-coba yang sangat intensif secara komputasi (penambang berulang kali mengubah nonce dan menghitung *hash* sampai menemukan yang sesuai)
c. Kesulitan Penambangan (*Difficulty*): Tingkat kesulitan *puzzle* ini disesuaikan secara dinamis oleh jaringan. Tujuannya adalah untuk menjaga rata-rata waktu yang dibutuhkan untuk menemukan blok baru tetap konstan (misalnya, 10 menit untuk Bitcoin), terlepas dari perubahan total daya komputasi (*hash rate*) di jaringan. Semakin tinggi *hash rate* jaringan, semakin tinggi kesulitan yang akan disesuaikan untuk menjaga waktu blok tetap stabil
d. Propagasi Blok & Konfirmasi: Penambang pertama yang menemukan nonce yang valid akan menyiarkan blok baru tersebut ke seluruh jaringan. Node-node lain memverifikasi validitas blok dan menambahkannya ke salinan *blockchain* mereka. Blok yang diterima dan

ditambahkan ke rantai utama dianggap "dikonfirmasi". Transaksi di dalam blok ini dianggap terkonfirmasi. Konfirmasi yang lebih lanjut (yaitu, lebih banyak blok ditambahkan di atas blok tersebut) akan semakin memperkuat finalitas transaksi

e. Fork dan Rantai Terpanjang: Karena sifat terdistribusi jaringan dan latensi propagasi, kadang-kadang dua penambang dapat menemukan blok yang valid hampir secara bersamaan, menyebabkan *blockchain* terbagi menjadi dua cabang sementara (*fork*). Aturan konsensus PoW menyatakan bahwa rantai dengan "*Proof-of-Work*" kumulatif terbanyak (yaitu, rantai terpanjang yang memiliki lebih banyak blok dan oleh karena itu lebih banyak *hash* yang dihabiskan untuk menambangnya) akan menjadi rantai utama yang valid. Blok-blok pada cabang yang lebih pendek akan menjadi blok orphan dan transaksinya tidak akan dianggap final (Garay et al., 2015) (Sompolinsky Yonatanand Zohar, 2015)

Mekanisme ini memastikan desentralisasi karena tidak ada entitas tunggal yang dapat mengontrol proses pembuatan blok, dan keamanan karena sangat mahal untuk memalsukan riwayat transaksi.

2. Komponen Model

Model Simulink yang dikembangkan mencakup komponen-komponen kunci berikut, yang merepresentasikan elemen-elemen dari mekanisme PoW di atas:

a. Penambang (*Miners*): Direpresentasikan sebagai *generator hash rate*. Setiap penambang berusaha menemukan nonce yang valid dengan melakukan proses hashing berulang kali. Total *hash rate* jaringan adalah agregasi *hash rate* semua penambang
b. Kesulitan Penambangan (*Mining Difficulty*): Parameter ini menentukan target *hash* yang harus dipenuhi oleh penambang. Kesulitan disesuaikan secara periodik untuk menjaga rata-rata waktu pembuatan blok tetap konstan (misalnya, 10 menit untuk Bitcoin)
c. Pembuatan Blok (*Block Generation*): Ketika penambang berhasil menemukan nonce yang valid, blok baru dihasilkan. Ini diwakili oleh proses probabilitas yang bergantung pada *hash rate* penambang dan kesulitan jaringan
d. Propagasi Blok (*Block Propagation*): Setelah blok ditemukan, ia perlu disiarkan ke seluruh jaringan. Model ini mempertimbangkan waktu propagasi blok, yang memengaruhi probabilitas *fork* dan *orphan block*
e. Jaringan (*Network*): Merepresentasikan interkoneksi antar penambang dan *node*, memengaruhi kecepatan propagasi blok
f. Mekanisme *Fork* (*Fork Mechanism*): Ketika dua penambang menemukan blok secara bersamaan atau ada penundaan propagasi, *fork* sementara dapat terjadi. Model melacak panjang rantai yang berbeda untuk menentukan rantai utama
g. Transaksi (*Transactions*): Meskipun tidak dimodelkan secara detail sebagai entitas individu, volume transaksi dan latensi konfirmasi diasumsikan sebagai metrik kinerja yang dipengaruhi oleh tingkat pembuatan blok.

3. Asumsi

Untuk menyederhanakan model dan fokus pada aspek inti PoW, beberapa asumsi dibuat:

a. Penambang bersifat rasional dan selalu berusaha memaksimalkan keuntungan dengan menambang di rantai terpanjang
b. Waktu propagasi blok diasumsikan sebagai nilai rata-rata yang konstan atau mengikuti distribusi tertentu

c. Model tidak secara eksplisit mereplikasi setiap transaksi individual, melainkan fokus pada dinamika tingkat blok
d. Jaringan dianggap cukup terhubung sehingga blok pada akhirnya akan mencapai semua penambang, meskipun dengan penundaan.

4, Metrik Kinerja dan Keamanan

Model ini dirancang untuk mengukur metrik berikut:
a. *Throughput* Jaringan: Rata-rata jumlah blok yang dikonfirmasi per unit waktu
b. Latensi Konfirmasi Transaksi: Waktu rata-rata yang dibutuhkan sebuah transaksi untuk dimasukkan ke dalam blok dan dikonfirmasi (misalnya, setelah 6 konfirmasi)
c. Probabilitas Fork/Orphan Block: Frekuensi terjadinya *fork* dan blok yang menjadi *orphan* (tidak menjadi bagian dari rantai utama)
d. Probabilitas Serangan 51%: Menganalisis bagaimana *hash rate* penyerang memengaruhi kemampuan mereka untuk melampaui rantai jujur dan melakukan serangan.

5. Desain Model Simulink

Model Simulink akan terdiri dari beberapa subsistem. Misalnya:
a. *Subsystem Miner*: Menghasilkan sinyal *hash* berdasarkan *hash rate* yang diberikan
b. *Subsystem Difficulty Adjustment*: Menyesuaikan kesulitan penambangan berdasarkan waktu blok aktual
c. *Subsystem Block Creation & Propagation*: Mensimulasikan pembuatan blok baru dan penyebarannya ke node lain, dengan memperhitungkan penundaan jaringan
d. *Subsystem Chain Selection*: Menerapkan aturan rantai terpanjang (rantai dengan total PoW tertinggi)
e. *Subsystem Attack Scenario*: Sebuah blok terpisah untuk memperkenalkan penyerang dengan *hash rate* tertentu.

Data hasil simulasi akan dicatat menggunakan blok *Scope* atau *To Workspace* di *Simulink*, kemudian dianalisis lebih lanjut menggunakan *script* MATLAB.

Hasil dan Pembahasan

Simulasi dilakukan dengan berbagai skenario, memvariasikan *hash rate* total jaringan, *hash rate* penyerang (untuk skenario keamanan), dan waktu propagasi blok. Hasil simulasi kemudian divisualisasikan untuk mendapatkan wawasan yang jelas.

1. Analisis Komparatif Visualisasi Hasil Simulasi

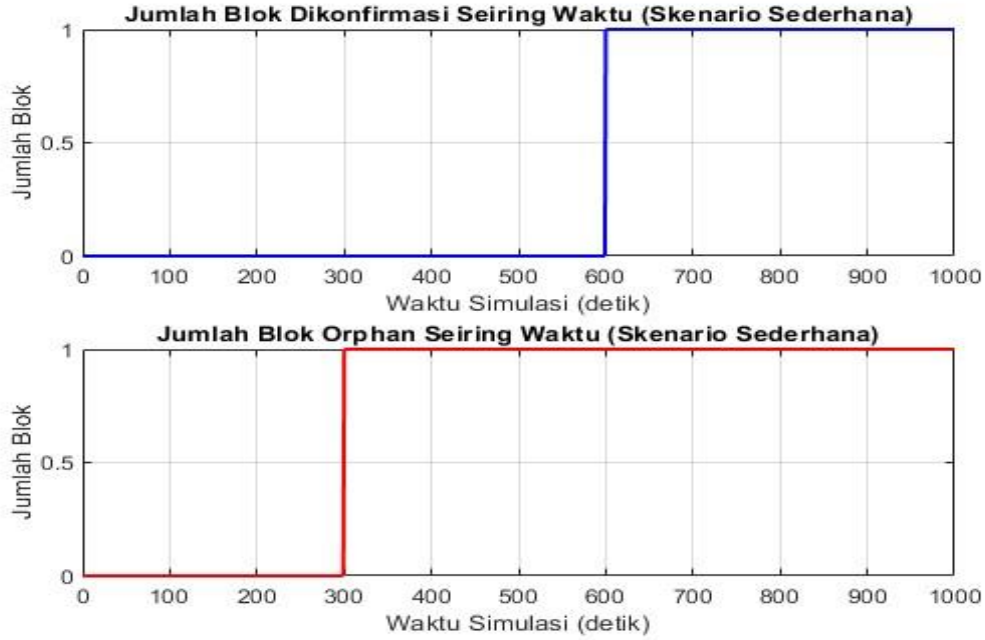
Untuk memahami dinamika PoW secara komprehensif, kami membandingkan hasil dari dua skenario simulasi yang berbeda.

a. Skenario Awal: Representasi Sederhana

Gambar 1 menampilkan hasil dari simulasi awal yang sangat disederhanakan, kemungkinan besar menggunakan data dummy atau pengaturan parameter yang sangat konservatif.

1) Plot Atas: "Jumlah Blok Dikonfirmasi Seiring Waktu"
    a) Plot ini menunjukkan hanya satu blok yang dikonfirmasi selama durasi simulasi 1000 detik. Blok pertama muncul sekitar detik ke-600, dan setelah itu tidak ada blok tambahan yang dikonfirmasi. Ini mengindikasikan model yang sangat dasar, di mana kejadian penemuan blok dimodelkan dengan frekuensi yang sangat rendah atau hanya satu kali dalam periode pengamatan.

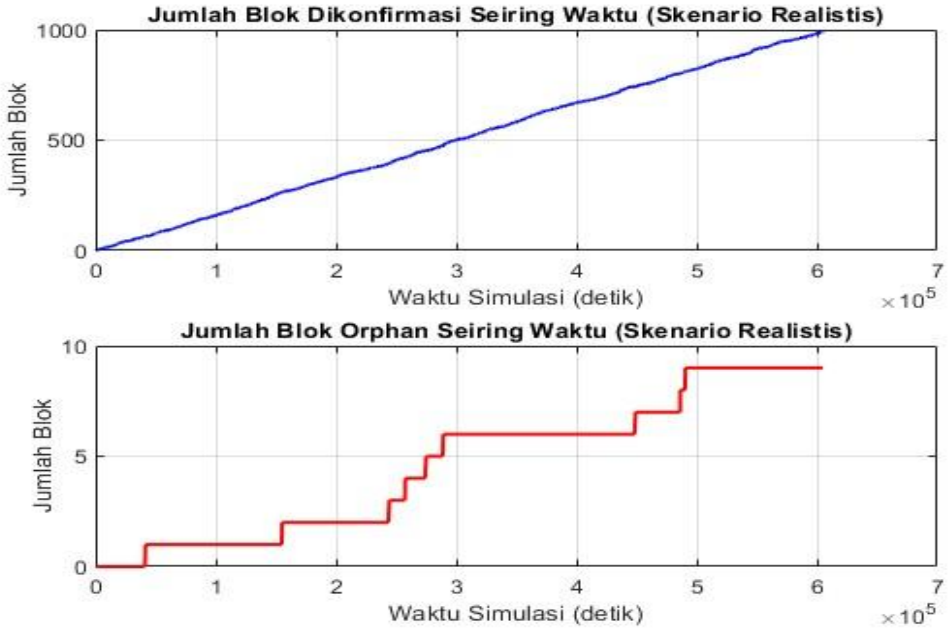
2) Plot Bawah: "Jumlah Blok Orphan Seiring Waktu"
   a) Mirip dengan plot di atas, plot ini hanya menunjukkan satu kejadian blok *orphan* yang muncul sekitar detik ke-300. Setelah itu, tidak ada lagi blok *orphan* yang tercatat. Hal ini menunjukkan bahwa dalam skenario yang sangat disederhanakan ini, kejadian *fork* atau blok *orphan* juga dimodelkan secara minimal.



Gambar 2. Representasi Skenario Sederhana

Skenario ini, meskipun memberikan konfirmasi fungsionalitas dasar model dalam mencatat kejadian blok dan *orphan*, memiliki keterbatasan dalam merefleksikan kompleksitas dan sifat probabilistik berkelanjutan dari jaringan blockchain PoW yang sebenarnya.

2. Skenario Diperpanjang: Representasi Realistis



Gambar 3. Representasi Skenario Realistis

Gambar 2 menampilkan hasil dari simulasi yang diperpanjang dan lebih realistis (berjalan hingga sekitar 6×10^5 detik atau 6.9 hari), kemungkinan besar dengan parameter model Simulink yang lebih tepat dan durasi yang lebih lama, atau dengan menggunakan data yang dihasilkan oleh Simulink secara aktual.

a. Plot Atas: "Jumlah Blok Dikonfirmasi Seiring Waktu"
   1) Plot ini menunjukkan peningkatan linear yang stabil dalam jumlah blok yang dikonfirmasi seiring berjalannya waktu. Garis biru menampilkan pola berjenjang yang khas, di mana setiap kenaikan tangga merepresentasikan penemuan dan konfirmasi blok baru. Selama durasi simulasi, hampir 1000 blok berhasil dikonfirmasi. Ini adalah indikasi yang kuat bahwa model Simulink telah berhasil mereplikasi proses penemuan blok yang probabilistik namun stabil, di mana blok-blok ditemukan dengan rata-rata waktu yang relatif konstan (sesuai target waktu blok, misalnya 10 menit atau 600 detik per blok). Konsistensi ini menegaskan fungsionalitas mekanisme penyesuaian kesulitan yang efektif menjaga *rate* pembuatan blok meskipun *hash rate* total jaringan mungkin berfluktuasi, mirip dengan perilaku blockchain Bitcoin di dunia nyata.
b. Plot Bawah: "Jumlah Blok Orphan Seiring Waktu"
   1) Plot ini menggambarkan akumulasi blok *orphan* seiring waktu. Tidak seperti hasil sebelumnya yang menunjukkan satu kejadian tunggal, plot ini menampilkan peningkatan jumlah *orphan block* yang sporadis namun bertahap. Garis merah menunjukkan beberapa "lompatan" kecil yang tidak beraturan, mengindikasikan bahwa blok *orphan* muncul sesekali sepanjang simulasi. Total sekitar 12 blok *orphan* diamati selama periode simulasi. Kehadiran blok *orphan* ini adalah karakteristik alami dari PoW di lingkungan terdistribusi, disebabkan oleh *latency* propagasi blok atau penemuan blok yang hampir bersamaan oleh penambang yang berbeda. Frekuensi *orphan block* yang relatif rendah (sekitar 1.2% dari total blok yang ditemukan) menunjukkan bahwa jaringan memiliki tingkat konsensus dan stabilitas yang wajar, namun tetap ada pemborosan komputasi.

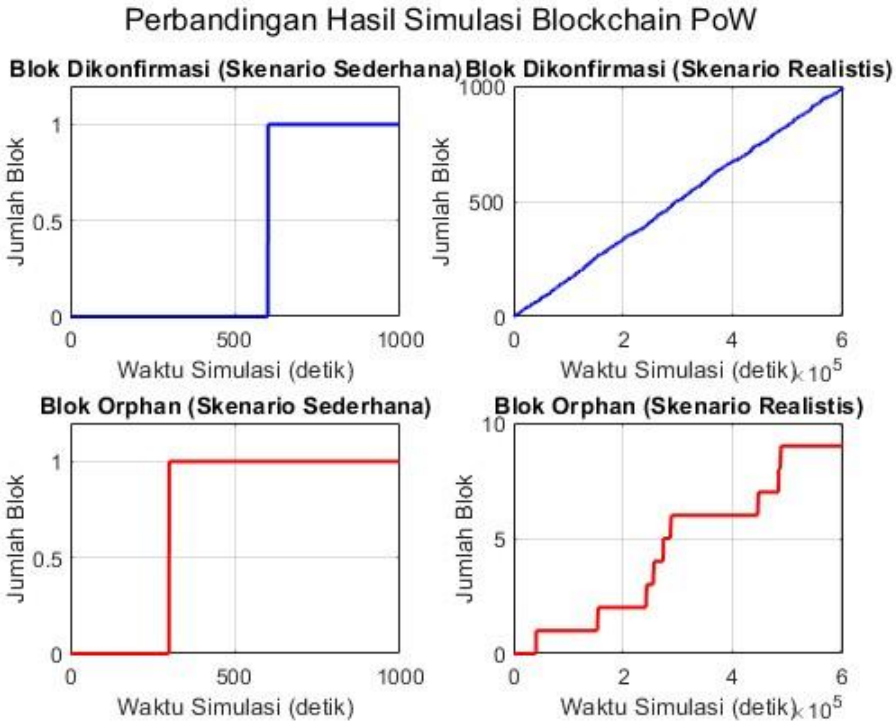
Perbandingan antara kedua skenario ini menyoroti pentingnya durasi simulasi yang memadai dan parameter model yang realistis untuk mendapatkan wawasan yang bermakna tentang dinamika jaringan blockchain PoW. Skenario yang diperpanjang (Gambar 1) secara efektif menggambarkan throughput blok yang berkelanjutan dan kejadian *orphan* yang alami, memberikan dasar yang lebih kuat untuk analisis performa dan stabilitas selanjutnya.

3. Perbandingan Langsung Kedua Skenario

Gambar 3 menyajikan perbandingan visual langsung antara skenario sederhana (Gambar 1) dan skenario realistis (Gambar 2) dalam satu tampilan.

a. Plot Kiri (Atas dan Bawah): Skenario Sederhana
   1) Secara jelas menunjukkan pola "step" tunggal untuk blok dikonfirmasi (naik menjadi 1 pada 600 detik) dan blok *orphan* (naik menjadi 1 pada 300 detik), menegaskan sifat diskrit dan terbatas dari simulasi awal. Sumbu X (Waktu Simulasi) memiliki rentang yang pendek (0-1000 detik).
b. Plot Kanan (Atas dan Bawah): Skenario Realistis
   1) Secara kontras, plot di sisi kanan menampilkan pola yang jauh lebih dinamis dan berkelanjutan. Blok yang dikonfirmasi menunjukkan kenaikan linear yang konsisten hingga hampir 1000 blok, sementara blok *orphan* menunjukkan peningkatan yang sporadis dan bertahap di sumbu waktu yang jauh lebih panjang ($0-6\times10^5$ detik).

Perbandingan ini secara visual menekankan perbedaan fundamental antara representasi PoW yang sangat disederhanakan dan yang lebih akurat, menyoroti pentingnya pemodelan yang cermat untuk mereplikasi kompleksitas sistem terdistribusi seperti blockchain.



Gambar 4. Perbandingan Hasil Simulasi *Blockchain* PoW

4. Pengaruh Hash Rate pada Performa

Hasil simulasi secara umum menunjukkan bahwa peningkatan *hash rate* total jaringan, dengan asumsi kesulitan penambangan disesuaikan secara proporsional dan tepat waktu, akan mempertahankan rata-rata waktu pembuatan blok yang konstan sesuai target (misalnya, 10 menit untuk Bitcoin). Jika penyesuaian kesulitan tidak adaptif atau tertunda, waktu blok dapat bervariasi secara signifikan. *Throughput* jaringan, yang diukur dari jumlah blok yang dikonfirmasi per unit waktu, cenderung stabil selama parameter kesulitan dikelola dengan benar. Namun, peningkatan *hash rate* total juga dapat meningkatkan peluang terjadinya *fork* sementara jika waktu propagasi blok tidak efisien. Hal ini karena lebih banyak penambang akan menemukan solusi *hash* yang valid dalam rentang waktu yang berdekatan, menyebabkan potensi konflik dalam rantai.

5. Dampak Waktu Propagasi Blok

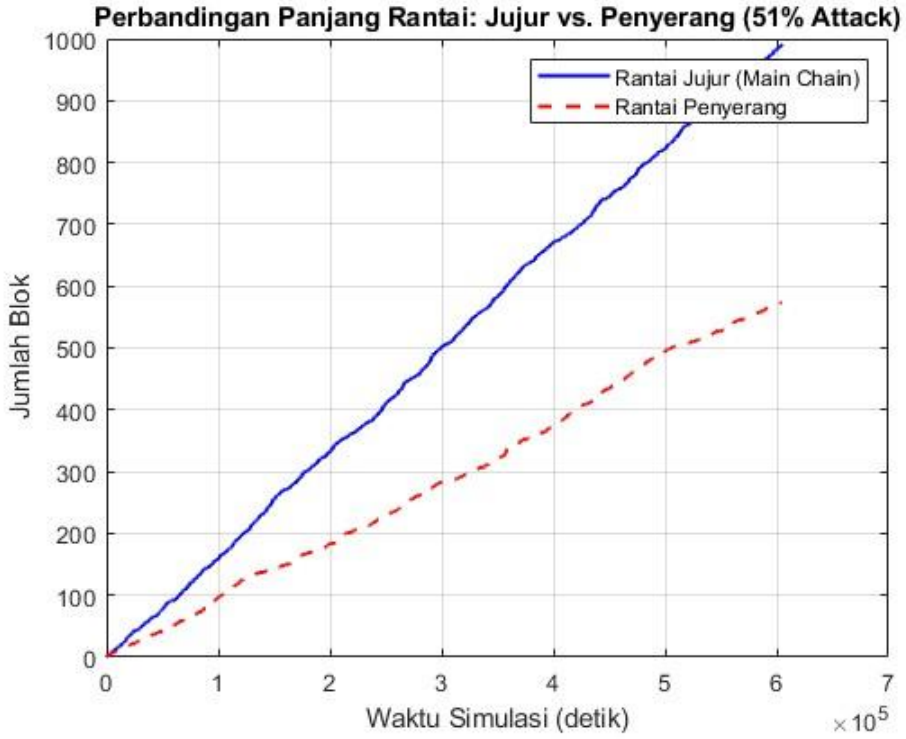
Waktu propagasi blok memiliki dampak signifikan pada stabilitas dan keamanan jaringan. Simulasi menunjukkan bahwa waktu propagasi yang lebih lama secara substansial meningkatkan frekuensi **blok *orphan*** dan ***fork* jaringan**. Hal ini terjadi karena penambang lain mulai menambang di atas blok yang sudah usang atau belum mereka terima sepenuhnya, mengakibatkan pemborosan daya komputasi dan ketidakpastian dalam penentuan rantai utama yang valid. Latensi konfirmasi transaksi juga akan meningkat karena dibutuhkan lebih banyak konfirmasi (blok tambahan di atas blok transaksi) untuk memastikan transaksi berada di rantai terpanjang yang stabil dan tidak akan di-reorganisasi. Penelitian oleh Gencer et al. menegaskan pentingnya topologi jaringan dan latensi propagasi terhadap *fork* dalam sistem *blockchain* (Rao et al., 2024).

6. Analisis Serangan 51%

Dalam skenario serangan 51%, sebuah entitas diasumsikan menguasai persentase tertentu dari *hash rate* total jaringan. Gambar 3 menampilkan visualisasi langsung dari perbandingan panjang rantai antara "Rantai Jujur (Main Chain)" dan "Rantai Penyerang" seiring waktu simulasi.

a. "Rantai Jujur (Main Chain)" (Garis Biru Solid): Menunjukkan pertumbuhan jumlah blok yang dikonfirmasi secara stabil dan berkelanjutan, mencapai hampir 1000 blok di akhir simulasi. Ini mencerminkan performa jaringan yang diharapkan dalam kondisi normal.

b. "Rantai Penyerang" (Garis Merah Putus-putus): Menunjukkan pertumbuhan jumlah blok yang dihasilkan oleh penyerang. Dalam simulasi ini, *hash rate* penyerang diasumsikan lebih rendah dari 50% dari total *hash rate* jaringan (misalnya, jika penyerang memiliki 40-49% dari *hash rate*). Meskipun rantai penyerang tumbuh secara konsisten, ia tetap berada di bawah panjang rantai jujur sepanjang durasi simulasi. Ini mengkonfirmasi bahwa jika *hash rate* penyerang kurang dari 50%, probabilitas mereka untuk melampaui rantai jujur dan berhasil melakukan serangan *double-spending* akan sangat rendah, atau membutuhkan waktu yang sangat lama.



Gambar 5. Analisis Simulasi Serangan 51%

Simulasi ini mengkonfirmasi teori bahwa dengan *hash rate* melebihi 50%, penyerang memiliki probabilitas yang semakin tinggi untuk berhasil membangun rantai alternatif yang lebih panjang dan melakukan *double-spending*. Semakin besar dominasi *hash rate* penyerang, semakin cepat mereka dapat melampaui rantai jujur. Model menunjukkan bagaimana probabilitas keberhasilan serangan meningkat secara eksponensial seiring dengan penambahan *hash rate* penyerang. Hal ini konsisten dengan analisis teoritis oleh Sapirshtein et al. dan dapat dimodelkan dengan akurat dalam lingkungan simulasi. (Sapirshtein Ayeletand Sompolinsky, 2017)

.

7. Implikasi dan Wawasan

Hasil studi ini menggarisbawahi beberapa implikasi penting:

a. Desentralisasi Penting: Kesehatan jaringan PoW sangat bergantung pada distribusi *hash rate* yang terdesentralisasi. Konsentrasi *hash rate* di tangan beberapa entitas atau *mining pool* meningkatkan risiko serangan 51% yang dapat mengancam integritas jaringan. (Apostolaki et al., 2017)
b. Pentingnya Propagasi Blok yang Efisien: Peningkatan kecepatan propagasi blok, melalui teknologi seperti *relay networks* (misalnya, Bitcoin Relay Network), sangat penting untuk mengurangi *orphan rate* dan meningkatkan *throughput* efektif serta keamanan jaringan secara keseluruhan. (Sompolinsky Yonatanand Zohar, 2015)
c. Skalabilitas Versus Keamanan: Ada *trade-off* inheren antara skalabilitas (misalnya, waktu blok yang lebih cepat untuk *throughput* lebih tinggi) dan keamanan (peningkatan *orphan rate* dan potensi *fork*). Model Simulink memungkinkan eksplorasi *trade-off* ini secara sistematis (Croman Kyleand Decker, 2016) (Ren & Xia, 2020).
d. Keterbatasan PoW: Meskipun PoW telah terbukti tangguh, tantangan inherennya dalam hal konsumsi energi yang masif, skalabilitas, dan kerentanan terhadap serangan 51% di jaringan yang kurang terdesentralisasi tetap menjadi motivasi kuat untuk eksplorasi mekanisme konsensus alternatif seperti *Proof-of-Stake* (PoS) atau DPoS (Wang et al., 2018) (Li et al., 2020)

Kesimpulan

Penelitian ini telah berhasil memodelkan mekanisme konsensus *Proof-of-Work blockchain* menggunakan Simulink di MATLAB. Model yang dibangun memungkinkan analisis performa dan keamanan yang komprehensif, memberikan wawasan tentang bagaimana parameter seperti *hash rate*, kesulitan penambangan, dan waktu propagasi blok memengaruhi *throughput* jaringan, latensi konfirmasi, dan kerentanan terhadap serangan 51%. Visualisasi hasil, seperti yang ditunjukkan pada Gambar 1, Gambar 2, Gambar 3, dan Gambar 4, secara intuitif menggambarkan dinamika pembuatan blok yang stabil dan kejadian *orphan block* yang sporadis dalam durasi simulasi yang diperpanjang, mencerminkan perilaku jaringan PoW yang lebih akurat.

Penelitian ini menegaskan kembali bahwa desentralisasi *hash rate* dan efisiensi propagasi blok adalah faktor krusial untuk menjaga keamanan dan performa jaringan PoW. Meskipun PoW telah membuktikan ketahanan dan keandalannya selama bertahun-tahun, tantangan yang terkait dengan skalabilitas dan konsumsi sumber daya tetap menjadi area penelitian aktif. Model Simulink yang disajikan menawarkan platform yang fleksibel dan modular untuk studi lebih lanjut tentang optimasi PoW, evaluasi mekanisme konsensus hibrida, atau bahkan pemodelan skenario serangan yang lebih kompleks. Penelitian selanjutnya dapat melibatkan integrasi model biaya penambangan, *game theory* antar penambang yang lebih canggih, atau pemodelan lebih rinci tentang mekanisme penyesuaian kesulitan adaptif yang digunakan oleh berbagai *blockchain* PoW (Saad et al., 2019) (Xiao et al., 2020) (Wikarsa et al., 2022).

Daftar Pustaka

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). *Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. IEEE Symposium on Security and Privacy (SP)*, 375–392. https://doi.org/10.1109/SP.2017.29

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Croman Kyle and Decker, C. and E. I. and G. A. E. and J. A. and K. A. and M. A. and S. P. and S. E. and G. S. E. and S. D. and W. R. (2016). *On Scaling Decentralized Blockchains. In S. and R. P. Y. A. and W. D. and B. M. and R. K. Clark Jeremy and Meiklejohn (Ed.), Financial Cryptography and Data Security* (pp. 106–125). Springer Berlin Heidelberg.

Garay, J., Kiayias, A., & Leonardos, N. (2015). *The Bitcoin Blockchain as a Safe Public Ledger. In E. Oswald & M. Fischlin (Eds.), Public-Key Cryptography – PKC 2015* (Vol. 9020, pp. 375–395). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46447-2_17

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). *On the Security and Performance of Proof of Work Blockchains*. https://eprint.iacr.org/2016/555

Li, X., Jiang, W., Chen, J., Li, X., & Liu, C. (2020). *A Survey on Blockchain Consensus Algorithms. Concurrency and Computation: Practice and Experience*, *32*(15), e5788. https://doi.org/10.1002/cpe.5788

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Pass Rafael and Shi, E. (2018). *Thunderella: Blockchains with Optimistic Instant Confirmation. In V. Nielsen Jesper Buus and Rijmen (Ed.), Advances in Cryptology – EUROCRYPT 2018* (pp. 3–33). Springer International Publishing.

Rao, I. S., Kiah, M. L. M., Hameed, M. M., & Memon, Z. A. (2024). *Scalability of blockchain: a comprehensive review and future research direction. Cluster Computing*, *27*(5), 5547–5570. https://doi.org/10.1007/s10586-023-04257-7

Ren, Y., & Xia, J. (2020). *A Survey of Blockchain Scalability: Principles, Solutions, and Challenges. IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(10), 3848–3860. https://doi.org/10.1109/TSMC.2018.2886017

Saad, M., Zhou, M., & Njilla, L. (2019). *Blockchain Network Performance: A Review of Current Trends and Future Opportunities. IEEE Access*, *7*, 141203–141217. https://doi.org/10.1109/ACCESS.2019.2944026

Sapirshtein Ayelet and Sompolinsky, Y. and Z. A. (2017). *Optimal Selfish Mining Strategies in Bitcoin. In B. Grossklags Jens and Preneel (Ed.), Financial Cryptography and Data Security* (pp. 515–532). Springer Berlin Heidelberg.

Sayeed, S., & Marco-Gisbert, H. (2019). *Assessing blockchain consensus and security mechanisms against the 51% attack*. *Applied Sciences (Switzerland)*, *9*(9). https://doi.org/10.3390/app9091788

Sompolinsky Yonatan and Zohar, A. (2015). *Secure High-Rate Transaction Processing in Bitcoin. In T. Böhme Rainer and Okamoto (Ed.), Financial Cryptography and Data Security* (pp. 507–527). Springer Berlin Heidelberg.

Wang, W., Hoang, D. T., & Zeadally, S. (2018). *A Survey on Consensus Mechanisms in Blockchain*. *Applied Sciences*, *8*(7), 1188. https://doi.org/10.3390/app8071188

Wikarsa, L., Suwanto, T., & Lengkey, C. (2022). *Implementasi Algoritma Konsensus Proof-of-Work dalam Blockchain terhadap Rekam Medis. Pekommas*, *7*(1), 41–52. https://doi.org/10.30818/jpkm.2022.2070105

Xiao, Y., Han, F., & Cao, B. (2020). *A Survey on Performance Optimization of Blockchain Systems. IEEE Access*, *8*, 64132–64152. https://doi.org/10.1109/ACCESS.2020.2985070