

# Konsep Implementasi Metode Konsensus *Proof of Work* dan *Proof of Stake* pada Permainan Poker Daring Berbasis Blockchain

Muhammad Rizki Pratama (18220110)  
Program Studi Sistem dan Teknologi Informasi  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung  
18220110@std.stei.itb.ac.id

**Abstract**—Permainan poker daring telah menjadi populer dalam beberapa tahun terakhir, dan semakin banyak platform permainan yang menggunakan teknologi blockchain untuk meningkatkan keamanan, transparansi, dan keadilan. Dalam penelitian ini, kami menjelajahi konsep implementasi metode konsensus *Proof of Work* (PoW) dan *Proof of Stake* (PoS) pada permainan poker daring berbasis blockchain.

**Keywords**—*poker; proof work; proof of stake; keamanan; ledger; PoS; PoW*

## I. PENDAHULUAN

Industri permainan sudah mengalami berbagai evolusi dan pertumbuhan seiring dengan perkembangan teknologi. Salah satu permainan yang sudah termigrasi dan banyak tertransformasi secara digital adalah permainan poker. Dengan jutaan pemain di seluruh dunia yang berinteraksi di dalam permainan, pertumbuhan yang dialami tidak hanya menjadikan permainan sebagai wadah untuk orang mendapatkan hiburan, tetapi juga sampai ke aktivitas ekonomi virtual yang dilaksanakan di dalam permainan. Perkembangan yang begitu pesat ini tidak hanya menimbulkan evolusi terhadap permainan itu sendiri, tetapi juga memunculkan berbagai tantangan baru untuk menjaga keamanan untuk berinteraksi di permainan itu sendiri seperti, *hacking, cheating, fraud*, dan kontrol yang tersentralisasi terhadap aset di dalam permainan. Untuk menanggulangi tantangan yang ada, teknologi *blockchain* dinilai sangat jitu untuk menangani masalah keamanan dan melakukan improvisasi terhadap keamanan interaksi di dalam permainan itu sendiri.

*Blockchain* merupakan teknologi terdistribusi yang memanfaatkan rantai pencatatan akan transaksi dan informasi sehingga semua bersifat transparan, *immutable*, dan aman. *Blockchain* terdiri dari blok-blok yang terhubung dimana tiap blok mengandung data atau transaksi dengan kriptografi unik yang menghubungkan dengan blok sebelumnya. Pada konteks ini, teknologi *blockchain* membuat transaksi di dalam permainan menjadi transparan, kepemilikan aset yang aman, dan mekanisme *anti-cheat*.

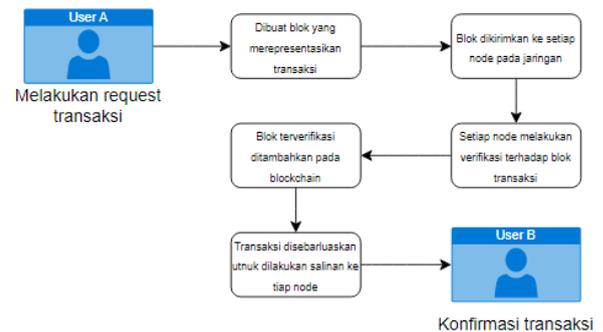
Makalah ini mengeksplorasi konsep implementasi teknologi *blockchain* untuk meningkatkan keamanan dan

pengalaman dalam bermain permainan poker digital secara daring.

## II. LANDASAN TEORI

### A. *Blockchain* (Heading 2)

*Blockchain* merupakan teknologi terdistribusi yang memanfaatkan rantai pencatatan akan transaksi dan informasi sehingga semua bersifat transparan, *immutable*, dan aman. *Blockchain* terdiri dari blok-blok data yang terhubung dimana tiap blok mengandung data atau transaksi dengan kriptografi unik yang menghubungkan dengan blok sebelumnya.



Gambar 2.1 Diagram Mekanisme *Blockchain*

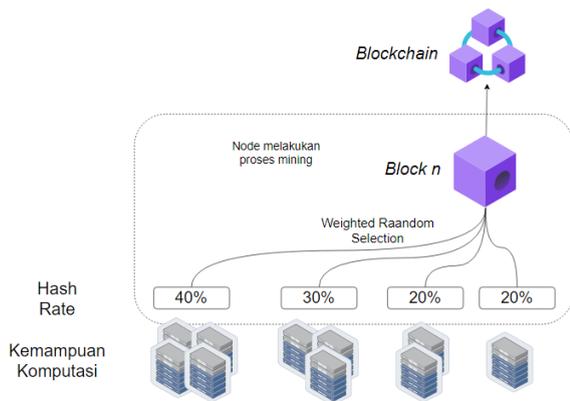
### B. *Konsensus pada Blockchain*

Proses verifikasi sebuah transaksi pada *blockchain* dilakukan oleh semua node pada jaringan *blockchain*. Proses verifikasi dilakukan dengan semua node mencapai konsensus atau menyepakati node mana yang boleh ditambahkan ke *blockchain*. Terdapat dua metode konsensus pada *blockchain*, yaitu *proof of work* dan *proof of stake*.

#### 1) *Proof of Work* (PoW)

*Proof of Work* merupakan metode konsensus yang digunakan dalam *blockchain* dalam melakukan verifikasi penambahan blok transaksi ke dalam *blockchain*. Metode ini mengharuskan node-node yang ada pada jaringan *blockchain* untuk

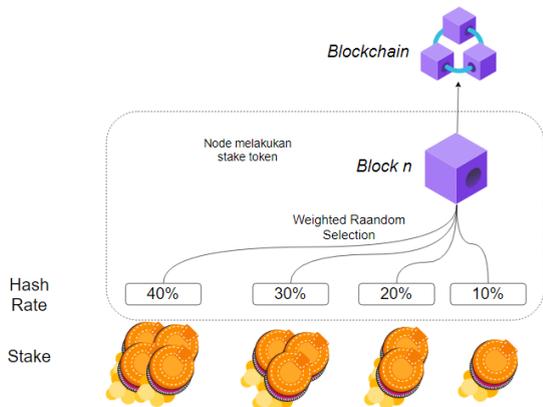
memecahkan suatu masalah matematika secara komputasional. Node yang dapat memecahkan masalah akan mendapat kewenangan untuk menambahkan blok baru. Node yang berhasil menambahkan blok baru kemudian mendapat *reward* berupa koin kripto.



Gambar 2.2 Diagram Mekanisme *Proof of Work*

2) *Proof of Stake (PoS)*

Metode konsensus *proof of stake* mengharuskan node yang ada di dalam jaringan untuk membuktikan kepemilikan koin kripto dalam jumlah tertentu untuk dapat melakukan penambahan blok ke *blockchain*. Node-node yang ada kemudian dipilih secara acak oleh algoritma PoS untuk melakukan *mining* berdasarkan jumlah koin yang dimiliki. Persentase keberhasilan untuk dipilih PoS pada sebuah node akan berbanding lurus dengan jumlah koin yang dimiliki.



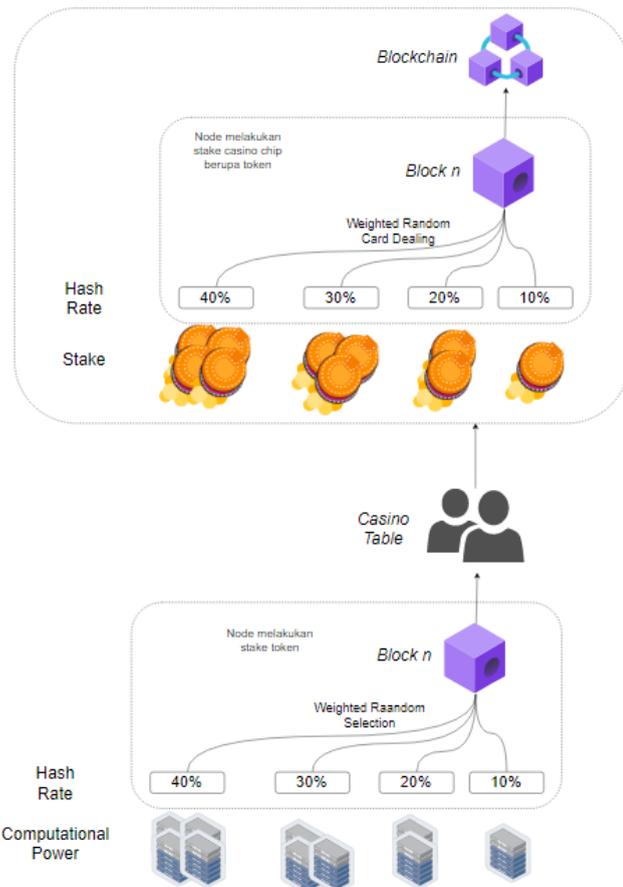
Gambar 2.3 Diagram Mekanisme *Proof of Stake*

C. *Poker*

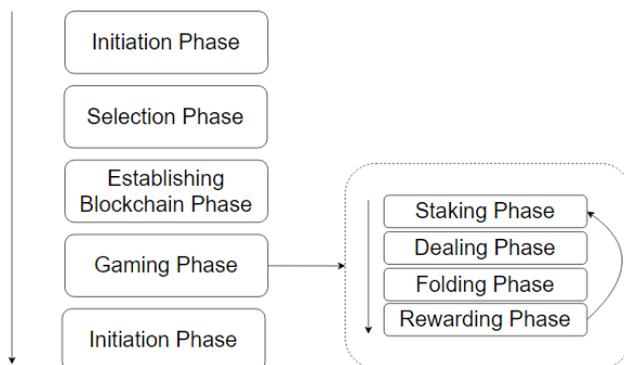
Poker adalah permainan kartu yang dimainkan oleh beberapa pemain di mana taruhan dilakukan berdasarkan kombinasi kartu yang mereka pegang. Dalam permainan poker, pemain bertaruh satu sama lain dalam berbagai bentuk, termasuk taruhan tunai, pot terpusat, atau taruhan yang berlaku untuk periode permainan tertentu. Kombinasi kartu terbaik menentukan pemenangnya, dan strategi,

keterampilan membaca pemain lain, dan keberuntungan menjadi faktor penting dalam kesuksesan.

III. SKEMA RANCANGAN



Gambar 3.1 Diagram Mekanisme *Poker Daring* berbasis *Blockchain*



Gambar 3.2 Diagram Fase Permainan *Poker Daring* berbasis *Blockchain*

Konsep permainan judi daring yang dikembangkan di sini mengadopsi kedua metode konsensus pada *blockchain*. Kedua

konsensus ini digunakan untuk dua sub-proses yang berbeda. Permainan berbasis *blockchain* ini akan terbagi menjadi 5 fase:

1) *Initiation Phase*

Pada fase ini, pemain akan melakukan pendaftaran atau request untuk seleksi. Pemain akan memasuki server permainan dan bersiap untuk melakukan *mining* di fase selanjutnya

2) *Selection Phase*

Permainan dimulai dengan pemain melakukan *mining* terhadap data yang akan dijadikan *balance* pada permainan. Pemain-pemain yang berhasil mendapatkan saldo atau *balance* pada fase ini kemudian diteruskan ke fase selanjutnya.

3) *Establishing Network Phase*

Dibuat jaringan *blockchain* untuk tiap meja permainan. Di tahap ini juga akan dilakukan distribusi pemain ke tiap-tiap jaringan *blockchain* yang sudah dibuat sebelum permainan dimulai berdasarkan jumlah koin yang dihasilkan pada fase seleksi. Pada tahap ini juga dilakukan pencatatan pada tiap *ledger* total koin yang ada pada meja.

4) *Gaming Phase*

Dibuat jaringan *blockchain* untuk tiap meja permainan. Di tahap ini juga akan dilakukan distribusi pemain ke tiap-tiap jaringan *blockchain* yang sudah dibuat sebelum permainan dimulai. Permainan dimulai dengan melakukan *staking* dimana pemain memberikan koin yang akan dilakukan *staking* pada putaran. Lalu, dilakukan *dealing* dimana pemain akan mendapatkan *resource* dengan kekuatan yang relatif dengan koin yang mereka *stake*. Setelah mendapat kartu yang didistribusikan, pemain akan memiliki kesempatan untuk melakukan *withdraw* pada koin yang sudah di *stake* untuk mengurangi atau menambah jumlah koin yang dilakukan *staking*. Selanjutnya adalah *folding phase* dimana dilakukan perhitungan poin berdasarkan operasi matematika terhadap *resource*, poin *folding*, dan jumlah koin yang mereka *stake*. Proses *folding* dilakukan berdasarkan prioritas dengan memegang poin terbanyak pada putaran dan semakin awal seorang pemain melakukan *folding*, semakin besar poin *folding* yang mereka terima. Ini mengadopsi konsep *proof of stake*. Pemain dengan perolehan poin terbanyak pada putaran tersebut mendapatkan semua koin yang dilakukan *staking* di meja tersebut pada *rewarding phase* dan permainan akan memasuki putaran baru sampai tersisa 1 orang yang ada di meja.

5) *Closing Phase*

Permainan ditutup dengan pentransferan masing-masing koin ke alamat *blockchain* pemain.

#### IV. ANALISIS DAN PEMBAHASAN

Perlu ditinjau kelebihan dan kekurangan kedua metode konsensus untuk melihat kecocokan dan keselarasan dengan desain permainan yang diimplementasikan teknologi *blockchain*. Untuk penggunaan *blockchain*, dimaksudkan untuk mengedepankan transparansi terhadap aktivitas yang dilakukan di dalam permainan. Transparansi ini membuat sulitnya para *hacker* dan *cheater* untuk mengganggu permainan dikarenakan mekanisme *ledger* yang digunakan oleh *blockchain*. Mekanisme *ledger* yang didukung oleh dua algoritma konsensus *blockchain* mendukung permainan semakin aman dan semakin menarik.

Berikut analisis kelebihan dan kekurangan dari kedua algoritma. Pertama, algoritma *proof of work* memiliki kelebihan dan kekurangan sebagai berikut:

**Tabel 3.1 Kelebihan dan Kekurangan algoritma *proof of work***

Kelebihan	Kekurangan
Keamanan tinggi	Konsumsi energi tinggi
Desentralisasi	Skalabilitas yang terbatas
Konsistensi dan keandalan	Kemungkinan adanya dominasi
Tahan terhadap DoS	Konsumsi energi tinggi
	Butuh perangkat khusus

Berikut juga merupakan kelebihan dan kekurangan dari algoritma *proof of stake*:

**Tabel 3.2 Kelebihan dan Kekurangan algoritma *proof of stake***

Kelebihan	Kekurangan
Efisiensi energi	Potensi sentralisasi yang tinggi
Skalabilitas	Risiko delegasi yang kurang optimal
Keamanan yang lebih dari PoW	Masalah distribusi kekayaan
Tidak ada ketergantungan pada perangkat spesifik	

Berdasarkan karakteristik di atas dilakukan komparasi terhadap kedua algoritma dan dihasilkan hasil sebagai berikut:

**Tabel 3.3 Komparasi algoritma *proof of work* dan *proof of stake***

Aspek	<i>Proof of Work</i>	<i>Proof of Stake</i>
Efisiensi Energi	Lebih Rendah	Lebih Tinggi
Desentralisasi	Lebih Tinggi	Lebih Rendah
Keamanan	Lebih Tinggi	Lebih Rendah
Skalabilitas	Lebih Rendah	Lebih Tinggi

Berdasarkan karakteristik di atas, diputuskan PoW lebih cocok diimplementasikan ke proses pengumpulan koin atau pada *selection phase* karena di sini akan terlihat kemampuan komputasi dari tiap pemain yang membantu permainan dapat mengelompokkan para pemain ke kelompok-kelompok yang lebih seimbang sehingga dicapai distribusi meja yang lebih efektif. Hal ini juga akan membantu proses keberjalanan permainan yang akan ditunjang oleh PoS menjadi lebih seimbang melalui pengelompokan berdasarkan koin yang didapat dari fase seleksi.

Penggunaan PoW untuk pengelompokan juga meminimalkan kelemahan PoS dalam melakukan distribusi dan pemilihan berdasarkan *stake* pada metode ini sehingga permainan bisa lebih *fair* dan kompetitif. Selain itu, penggunaan PoS juga menambah keseruan permainan karena faktor peluang yang sebanding dengan koin yang dilakukan *staking* sehingga menantang pemain untuk berani melakukan *staking* atau memformulasikan strategi yang lebih unik.

Pencatatan aktivitas atau transaksi di dalam permainan dicatat pada *ledger* yang ada sehingga tercapainya transparansi dan sangat minimnya serangan keamanan terhadap jaringan permainan. Dikuatkannya keamanan pada jaringan permainan juga dilakukan dengan adanya skema penyaringan terlebih dahulu (*Selection Phase*) dengan *proof of work* yang sangat sulit ditembus.

Perlu diingat masih adanya peluang terhadap serangan keamanan dan transparansi terhadap jaringan permainan. Namun, potensinya sangatlah kecil karena *proof of work* membutuhkan biaya dan kapabilitas komputasi yang sangat tinggi untuk dilakukan serangan ke sistemnya.

#### REFERENSI

- [1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
- [2] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13), 127-140. doi: 10.1145/2504730.2504747
- [3] Buterin, V. (2013). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from <https://ethereum.org/whitepaper/>
- [4] Larimer, D. (2014). Delegated Proof of Stake.
- [5] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

#### PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 Mei 2023



Muhammad Rizki Pratama (18220110)