

BAB I

PENDAHULUAN

1.1. Latar Belakang

Struktur basis data yang mendasari untuk transaksi *bitcoin* dan mata uang digital lainnya adalah buku besar yang terdesentralisasi, yang disebut *blockchain*, yang menyimpan seluruh riwayat transaksi. Nama tersebut berasal dari fakta bahwa transaksi digabungkan ke dalam blok dan setiap blok di *blockchain* (kecuali untuk blok pertama yaitu blok genesis) merujuk pada blok sebelumnya. Setiap *node* yang berpartisipasi dalam jaringan *bitcoin* memiliki salinan *blockchain*-nya sendiri, yang disinkronkan dengan *node* lain menggunakan protokol *peer-to-peer* [1].

Blockchain telah diharapkan menjadi revolusi dunia keuangan yang akan memungkinkan kontrol atas uang berpindah dari institusi seperti Bank menjadi kontrol penuh atas pengguna, dengan mengurangi intervensi dari pihak ketiga menjadi transaksi *peer-to-peer*. Namun, kunci untuk data terpusat memiliki repositori yang keamanan datanya terjamin. Contoh dari sebuah penyimpanan data yang tidak aman ialah ketika salah satu peserta dari *blockchain* menerbitkan *ledger* yang tidak nyata. Sejak *ledger* didistribusikan peserta lain tidak akan dapat memastikan keakuratan dari entri yang diterbitkan ini. Ini menyebabkan data yang disimpan dalam jaringan seperti itu akan ditandai sebagai tidak dapat diandalkan.

Algoritma *proof of work* memberikan keamanan jaringan dalam bentuk penambangan blok. Poin utama *proof of work* adalah bahwa setiap *node* yang ingin berpartisipasi dalam penambangan harus menyelesaikan masalah yang sulit secara komputasi untuk memastikan validitas blok yang baru ditambang. Setiap blok baru memberikan sejumlah koin untuk penambang. Dalam protokol sistem *proof of work* keamanan jaringan didukung oleh fisik sumber daya yang langka seperti perangkat keras khusus dan energi listrik. Hal ini membuat sistem yang diamankan dengan *proof of work* tidak efisien dari sudut pandang sumber daya [1]. Untuk meningkatkan keuntungan, penambang dipaksa untuk terus menggunakan lebih banyak sumber daya untuk penambangan. Hal ini membuat biaya serangan terhadap sistem yang diamankan dengan *proof of work* menjadi sangat tinggi, tetapi ketidakramahan ekologis dari protokol *proof of work* telah mengakibatkan upaya untuk membangun protokol konsensus serupa yang jauh lebih hemat sumber daya.

Berbeda dengan algoritma *proof of stake* yang memiliki implementasi dengan keamanan yang tidak didasarkan pada komputasi yang mahal. Konsepnya sederhana, alih-alih memerlukan *mining power*, kemungkinan untuk membuat blok dan menerima hadiah sebanding dengan kepemilikan saham pengguna dalam *node*. Seorang pengguna yang memiliki fraksi p dari jumlah total koin yang beredar menciptakan blok baru dengan probabilitas p . Pengguna dengan taruhan tertinggi dalam sistem memiliki kemungkinan paling besar untuk memvalidasi transaksi, karena mereka merupakan kontributor yang lumayan besar walaupun mekanisme pemilihannya sendiri acak.

Pada penelitian sebelumnya, terdapat beberapa analisis komparatif yang dilakukan untuk membandingkan algoritma konsensus. Namun, sebagian besar perbandingan dibuat antara *proof of work* dan *delegated proof of stake* yang mana penelitian tersebut juga tidak memberikan perbandingan secara lengkap dan juga menyeluruh. Selain itu, dalam menemukan perbedaan kinerja, tidak terdapat analisis relevan yang dilakukan untuk membedakan proses yang berjalan [15]. Meskipun terdapat beberapa sumber yang menyatakan perbandingan kinerja, akan tetapi pengujian yang sebenarnya seringkali tidak pernah diuji dan data kinerja diambil dari sumber dokumen dan *whitepaper cryptocurrency*. Di sisi lain, sebagian besar hasil penelitian sebelumnya membahas berdasarkan informasi teoretis tanpa bukti konsep seperti pengujian simulasi. Tanpa simulasi tes, kita akan kesulitan membuktikan fakta dan data yang berasal penelitian yang ada.

Maka dari itu, tujuan dari penelitian ini adalah untuk mengidentifikasi perbandingan berdasarkan beberapa parameter kunci untuk evaluasi dari dua algoritma konsensus ini yang merupakan *proof of work* dan *proof of stake*, untuk mengetahui algoritma mana yang lebih ideal. Studi literatur yang ada akan digunakan sebagai referensi dan simulasi akan diuji untuk keluar dengan data pembandingan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan maka dapat dirumuskan beberapa permasalahan yang akan diteliti, yaitu:

1. Bagaimana penerapan analisa perbandingan algoritma konsensus *proof of work* dengan algoritma konsensus *proof of stake*?
2. Bagaimana hasil dari analisa perbandingan algoritma konsensus *proof of work* dengan algoritma konsensus *proof of stake*?

1.3. Batasan Masalah

Agar penelitian ini tidak melebar kemana-mana maka penelitian ini akan diberi batasan-batasan masalah seperti berikut ini:

1. Algoritma konsensus akan yang digunakan untuk pengujian adalah algoritma konsensus *proof of work* dan algoritma konsensus *proof of stake*.
2. Penelitian ini khusus membahas tentang analisa perbandingan.
3. Data yang digunakan sebagai sumber merupakan data yang diambil dari *Data On-Chain*.

1.4. Maksud dan Tujuan Penelitian

Berdasarkan dari uraian permasalahan, maka maksud dan tujuan yang ingin dicapai dari penelitian ini adalah:

a. Maksud Penelitian

Mengetahui bagaimana blok baru bisa tercipta dalam *blockchain* dengan algoritma konsensus *proof of work* dan algoritma konsensus *proof of stake*.

b. Tujuan Penelitian

a) Bagi Pengguna

1. Merekomendasikan pengguna untuk memahami bagaimana blok baru bisa tercipta dengan algoritma konsensus tertentu didalam teknologi *blockchain*.
 2. Mengetahui *blockchain* dengan algoritma konsensus tertentu yang paling ideal untuk melakukan transaksi dalam skala mikro.
- b) Bagi Pengembang
3. Mengetahui algoritma konsensus mana yang lebih baik untuk *project* yang akan mereka kembangkan.
 4. Mengetahui *blockchain* mana yang paling ideal untuk melakukan transaksi dengan tingkat skalabilitas tinggi.
- c) Bagi Insitusional
5. Mengetahui tingkat desentralisasi, skalabilitas dan keamanan dalam teknologi *blockchain* dengan algoritma konsensus tertentu.
 6. Mengetahui *blockchain* dengan algoritma konsensus tertentu yang paling ideal untuk melakukan transaksi dalam skala mikro.

1.5. Manfaat Penelitian

a. Bagi Pengembang atau Institusi

Penelitian ini diharapkan dapat membantu untuk menemukan algoritma konsensus paling ideal berdasarkan trilema dalam teknologi *blockchain* yang meliputi skalabilitas, desentralisasi dan keamanan.

b. Bagi Peneliti

Penelitian ini diharapkan dapat memberikan manfaat dan menjadi sarana untuk memilih algoritma konsensus paling ideal didalam teknologi *blockchain*.

1.6. Metodologi Penelitian

Pada penelitian ini peneliti menggunakan beberapa metode penelitian seperti berikut:

1.6.1. Jenis Penelitian

Sesuai dengan judul dalam penelitian ini yaitu "Analisa Perbandingan Algoritma Konsensus *Proof of Work* dan *Proof of Stake* Untuk Menambah Data Baru Pada Teknologi Blockchain", maka penelitian ini termasuk kedalam jenis penelitian deskriptif kuantitatif dan observatif. Hal ini dikarenakan penelitian ini memiliki tujuan untuk mengetahui algoritma konsensus dengan tingkat efisiensi yang mampu menyelesaikan masalah meliputi skalabilitas, desentralisasi dan keamanan dengan proses analisis data, penelitian ini menggunakan data-data numerik dan angka yang diolah dengan metode statistik, setelah diperoleh hasilnya kemudian dideskripsikan dengan menguraikan kesimpulan yang didasari oleh angka dan juga observasi dengan metode statistik tersebut.

1.6.2. Metode Pengumpulan Data

Melakukan pengumpulan data yang diperoleh dari hasil kuesioner dengan skala *Likert* untuk pengolahan data, serta melakukan pencarian data-data lain sebagai pendukung.

1.6.3. Metode Pengolahan Data

Data yang sudah diseleksi tadi, akan diolah dengan menggunakan studi literatur dan observasi lanjutan dengan metode *on-chain* sebagai data pendukung.

1.7. Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini akan membahas tentang latar belakang penelitian, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab kedua ini akan membahas tentang kajian pustaka, dan teori-teori yang berkaitan dengan penelitian ini.

BAB III METODE PENELITIAN

Bab ini berisikan tentang metode penelitian yang dipakai seperti alat dan bahan penelitian, serta alur penelitian yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini, hasil dan pembahasan berisikan hasil dan juga pembahasan lebih lanjut dari penelitian.

BAB V PENUTUP

Pada bab ini berisikan tentang kesimpulan dari hasil penelitian yang sudah dibuat serta memberikan saran untuk pengembangan lebih lanjut kepada peneliti berikutnya.

DAFTAR PUSTAKA

Berisikan sumber teori yang dijadikan sebagai referensi di dalam penelitian ini.