BLOCKCHAIN

WEEK 4 ETHEREUM POW AND POS

Nama : Sultan Chisson Obie

Kelas : TK-42-Pil

NIM : 1103194158

KONSENSUS

konsensus adalah persetujuan umum atau kemufakatan secara online menggunakan sistem komputer. Masing-masing pihak bermusyawarah secara anonim melalui mekanisme konvensi. Mudahnya, konsensus adalah suatu proses perhitungan rumit untuk menghasilkan persetujuan umum secara bersama tentang validasi suatu transaksi di dalam algoritma baik Proof Of Work ataupun Proof Of Stake. Dengan begitu setiap transaksi yang terjadi dalam suatu blockchain dapat dipercaya kebenaran dan validitasnya sebab transaksi bisa dikatakan valid kalau sudah dicek oleh berbagai pihak yang terlibat dalam konsensus tersebut atau sering kita sebut sebagai miners atau penambang. Verifikasi oleh para notch meliputi seluruh detail mulai dari alamat penerima dan pengirim nominal yang dikirim apakah benar saldonya berpindah serta tandatangan yang diikutsertakan didalam transaksi tersebut sehingga proses transaksi di blockchain bisa dipastikan lancar dan sampai tujuan dengan aman dan seluruh pemilik koin tidak kehilangan koinnya akibat manipulasi data berkat mekanisme konsensus ini.

Proof Of Work

Apa itu Proof Of Work?

Proof-of-work adalah mekanisme yang memungkinkan jaringan Ethereum yang terdesentralisasi untuk mencapai konsensus, atau menyetujui hal-hal seperti saldo akun dan urutan transaksi. Ini mencegah pengguna dari "menggandakan pengeluaran" koin mereka dan memastikan bahwa rantai Ethereum sangat sulit untuk diserang atau dimanipulasi. Proof-of-work adalah algoritma dasar yang menetapkan kesulitan dan aturan untuk pekerjaan yang dilakukan miners. Proof-of-work adalah algoritma dasar yang menetapkan kesulitan dan aturan untuk pekerjaan yang dilakukan penambang. Pertambangan adalah "pekerjaan" itu sendiri. Ini adalah tindakan menambahkan blok yang valid ke chain. Ini penting karena panjang rantai membantu jaringan mengikuti chain Ethereum yang benar dan memahami keadaan Ethereum saat ini. Semakin banyak "pekerjaan" yang dilakukan, semakin panjang chain-nya, dan semakin tinggi nomor bloknya, semakin yakin jaringan tersebut tentang keadaan saat ini.

Bagaimana POW dalam Ethereum bekerja?

Transaksi Ethereum diproses menjadi blok. Protokol POW mengharuskan penambang untuk melalui perlombaan coba-coba yang intens untuk menemukan nonce untuk sebuah blok. Hanya blok dengan nonce yang valid yang dapat ditambahkan ke rantai. Saat berlomba membuat blok, penambang akan berulang kali memasukkan kumpulan data, yang hanya bisa didapatkan dari mengunduh dan menjalankan chain penuh melalui fungsi matematika. Dataset digunakan untuk menghasilkan mixHash di bawah target nonce, seperti yang ditentukan oleh kesulitan blok. Cara terbaik untuk melakukan ini adalah melalui trial and error. Kesulitan menentukan target untuk hash. Semakin rendah target, semakin kecil kumpulan hash yang valid. Setelah dibuat, ini sangat mudah untuk diverifikasi oleh penambang dan klien lain. Bahkan jika satu transaksi diubah, hashnya akan sangat berbeda, menandakan penipuan. Hashing membuat penipuan mudah dikenali.

Security pada POW Ethereum

Penambang akan menerima insentif untuk melakukan validasi pada proses transaksi di Ethereum. Tujuan dari proof-of-work adalah untuk memperpanjang rantai (chain). Rantai terpanjang paling dapat dipercaya sebagai rantai yang valid karena telah menyelesaikan pekerjaan komputasi paling banyak. Dalam sistem PoW Ethereum, hampir tidak mungkin untuk membuat blok baru yang menghapus transaksi, membuat yang palsu, atau mempertahankan rantai kedua. Itu karena penambang jahat harus selalu memecahkan blok lebih cepat daripada orang lain. Untuk melakukan kejahatan dalam proses ini membutuhkan lebih dari 51% kekuatan mining jaringan. Energi yang dihabiskan mungkin saja lebih besar daripada keuntungan yang didapatkan.

Economics

POW bertanggung jawab untuk mengeluarkan mata uang baru ke dalam sistem dan memberi insentif kepada penambang untuk melakukan pekerjaan itu.

Penambang yang berhasil membuat blok mendapatkan hadiah dua ETH yang baru dicetak tetapi tidak lagi menerima semua biaya transaksi, karena base fee dibakar, sedangkan hadiah tip dan blok diberikan kepada penambang. Seorang penambang juga bisa mendapatkan 1,75 ETH untuk uncle block. Uncle block adalah blok valid yang dibuat oleh penambang secara praktis bersamaan dengan penambang lain yang menambang blok yang berhasil. Blok paman biasanya terjadi karena latensi jaringan. Konsep yang cocok disematkan pada penambang/miner POW adalah siapa cepat dia dapat. Karena pada prosesnya, siapa penambang tercepat yang berhasil memecahkan kode transaksi pada blok tertentu dialah yang akan mendapatkan fee dari koin yang ditambang.

Proof Of Stake

Apa itu POS?

Semakin banyaknya miners di dunia. Ternyata meningkatkan hacker pula yang akan menyerang proses penambagan koin. Hal ini terjadi karena makin banyaknya jasa penyewaan Hash Power yang digunakan penambang untuk memperoleh hasil lebih banyak pada metode POW. Oleh karena itu munculah proposal baru yang disebut Proof Of Stake. Proof Of Stake adalah mekanisme konsensus yang menjadikan aset atau koin yang dimiliki sebagai taruhan atau jaminan jika kalian akan melakukan verifikasi data di block chain dengan benar jika terjadi sebuah bad behavior atau ada seorang miner yang mencoba melakukan perubahan data maka koin yang mereka steak akan hilang. Validator POS memiliki tanggung jawab yang sama seperti penambang dengan mekanisme POW cuma perbedaannya POS tidak memerlukan sebuah komputer dengan spesifikasi tinggi dan energi listrik yang berlebih dan sebagai gantinya memerlukan koin dengan nominal tertentu untuk dikunci.

Jumlah miners pada POS bermacam macam. Semakin banyak jumlah miners, maka semakin tinggi skala desentralisasi blockchain. Perbedaan yang dapat dilihat pada POW dan POS adalah jika di POW seseorang yang melakukan proses validasi dalam transaksi blockchain disebut miners / penambang, pada POS disebut sebagai validator yang dipilih secara acak, sehingga meminimalisir validator yang memiliki proses transaksi lebih tinggi dengan validator lainnya.

Bagaimana POS dalam Ethereum bekerja?

Berbeda dengan POW, validator tidak perlu menggunakan sejumlah besar daya komputasi karena mereka dipilih secara acak dan tidak bersaing. Mereka tidak perlu menambang block, mereka hanya perlu membuat block saat dipilih dan memvalidasi block yang diusulkan. Validasi ini dikenal sebagai “attesting” (pengesahan). Validator akan mendapat reward karena menyelesaikan blok yang diusulkan kepadanya. Jika validator terbukti melakukan malicious block, validator akan kehilangan koin yang sudah dikunci. Cara kerja validasi adalah saat user mengirimkan transaksi di shard, validator akan bertanggung jawab untuk menambahkan transaksi user ke blok shard. Validator dipilih secara random untuk mengusulkan blok baru.

Security pada POS Ethereum

Ancaman serangan pada POS 51% masih ada, tetapi lebih berisiko bagi penyerang. Untuk melakukan penyerangan, penyerang harus mengontrol 51% dari ETH yang dipertaruhkan. Tidak hanya uang, bahkan dapat menyebabkan nilai ETH turun. Untuk menangani ini, ada insentif tinggi yang diberikan kepada validator yang juga bertanggung jawab untuk mencegah tindakan kejahatan ini.

Kesimpulan

Dalam transaksi yang dilakukan secara online saat ini diperlukan suatu entitas yang dapat dipercayai kedua belah pihak yang melakukan transaksi sebagai bukti transaksi yang dilakukan adalah benar adanya. Kesepakatan ini dikenal sebagi consensus. Konsensus adalah persetujuan umum atau kemufakatan secara online menggunakan sistem komputer. Masing-masing pihak bermusyawarah secara anonim melalui mekanisme konvensi didalam komputer. Pada Ethereum terdapat dua mekanisme konsesus yang berlaku, yaitu Proof of Work dan Proof of Stake. POS (Proof of Stake) adalah mekanisme hasil pengembangan dari POW (Proof of Work). Yang membedakan keduanya adalah sistem penangana transaksi yang terjadi didalam blockchain. Pada POW, penambang / miners yang bekerja untuk menambang dan menyelesaikan kode transaksi dalam blockchain. Sedangkan pada POS, ada seorang yang disebut sebagai validator yang akan memvalidasi transaksi yang terjadi didalam blockchain. Validator di pilih secara random. Baik miner atau validator akan mendapat reward setelah berhasil menyelesaikan / memvalidasi block transaksi.