Nama : M. Imam Whidyarto

NIM : 1103184089

Kelas : TK-42-PIL

Proof of Work merupakan protokol yang bertujuan mencegah dari serangan cyber misalnya serangan berbentuk DDoS (Distributed Denial-of-Service) yang ingin menguras tenaga sumber daya sistem dengan cara mengirim permintaan-permintaan fiktif. Konsep PoW sudah ada sejak lama, bahkan sebelum bitcoin.

Proof of work adalah persyaratan yang dibuat untuk mendefinisikan suatu perhitungan penambangan. Jika sekumpulan data tertentu hanya dapat menghasilkan satu hash saja, lalu bagaimana seorang penambang dapat memastikan mereka bisa menghasilkan hash di bawah target?

Mereka akan mengubah masukan dengan menambahkan bilangan bulat yang disebut nonce (nomor yang nantinya digunakan sekali). Setelah hash yang valid ditemukan, hash itu akan disiarkan ke jaringan dan blok baru akan ditambahkan ke blockchain.

Mining atau penambangan adalah aktivitas yang sangat kompetitif. Kadang kala mining bahkan terasa seperti lotre ketimbang kompetisi. Rata-rata, seseorang akan menghasilkan proof of work yang dapat diterima setiap sepuluh menit.

Miner nantinya akan berkumpul bersama untuk meningkatkan peluang mereka untuk mining. Semakin cepat mereka menghasilkan blok baru dalam kurun waktu terbatas, maka makin cepat pula mereka mendapat imbalan. Imbalan yang diterima penambang akan digunakan untuk menutup biaya transaksi dan dibagikan ke masing-masing penambang yang ikut melakukan mining.

Menambang dalam blockchain yang menggunakan konsensus proof of work memang sulit. Mengubah satu aspek saja dalam blockchain dapat membuat penambang harus melakukan mining ulang di seluruh blok lainnya. Keuntungannya, proof of work akan meminimalisasi peluang pengguna untuk memonopoli daya komputasi jaringan

Blockchain memiliki konsensus bernama Proof-of-Work, yaitu bentuk kriptografi saat satu user memastikan dan memastikan adanya kegiatan telah diupayakan dengan user lain. Konsensus ini diciptakan untuk menghindari serangan manipulasi data dengan cara memvalidasikan data dengan user lain, akan tetapi konsensus ini memiliki kelemahan, kelemahan pada konsensus ini adalah pada saat penyerang mengubah data sebanyak 51% menjadikan data manipulasi menjadi data mayoritas. Metode ini dapat mengembalikan transaksi yang sudah selesai sehingga akan terdapat kondisi double-spend dalam suatu transaksi. Penambang adalah pilar atau pendukung utama dari algoritma ini yang berperan dalam memverifikasi dan merekam sebuah transaksi sehingga membuat algoritma ini memiliki kredibilitas yang dipertanyakan.

Ada pula penyerangan Eclipse, yaitu kondisi saat seorang penyerang memonopoli koneksi keluar masuk blok, sehingga akan terjadi isolasi pada user yang ada pada jaringan tersebut. Terlebih lagi, apabila blok ini memiliki kunci yang strategis terhadap mayoritas blok lainnya, user akan membutuhkan lebih banyak daya komputasi yang pada akhirnya akan digunakan untuk membantu kebutuhan si penyerang ini. Serangan seperti ini juga memiliki konsep yang sama dengan Selfish dan Stubborn mining yaitu penyerangan dari salah satu user untuk kepentingan pribadi.

Penyerangan dilakukan pada saat transaksi, ketika transaksi sudah masuk kedalam blok, dan masing-masing memiliki hash sebagai verifikasi data, akan tetapi sebagai penyerang hash tersebut dapat dimanipulasi, walaupun invalid penyerang hanya tinggal memanipulasi data hingga 51% sehingga transaksi yang dimanipulasi dianggap valid oleh konsensus ataupun keamanan yang berjalan.