Nama : Raudhatul Rafiqah A

NIM : 1103180225

Week 5 - Blockchain Assignment

Bentuk cryptograpy saat satu user memastikan adanya kegiatan telah diupayakan dengan user lain yang bernama Proof-of-Work oleh consensus pada Blockchain. Consensus ini diciptakan untuk menghindari serangan manipulasi data dengan cara memvalidasikan data dengan user lain, akan tetapi consensus ini memiliki kelemahan, yaitu pada saat penyerang mengubah data sebanyak 51% menjadikan data atau memanipulasinya 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.