Nama : Ersan Aythamsyach

NIM : 1103184061

Sybil Attack

Penyerangan dengan metode ini dilakukan dengan cara membuat node palsu yang ditaruh ke dalam jaringan asli dengan memberlakukan adanya identitas palsu untuk dapat membuat node tersebut. Namun sayangnya, penyerangan dengan metode ini tidak dapat berlaku dalam keseluruhan blok karena terdapat beberapa blok yang membutuhkan biaya yang cukup tinggi untuk diserang.

BGP Hijack

Serangan dengan metode ini memanfaatkan perbedaan pandangan antara sistem yang dimiliki oleh blockchain dengan pandangan yang dimiliki oleh router. Walaupun jaringan blockchain acapkali disebut sebagai jaringan yang terdesentralisasi, namun dari sudut pandang internet router jaringan blockchain merupakan jaringan sentral karena terdapat sekitar 100 IP Prefixes yang mengelola 20% bitcoin host.Dengan mengetahui hal tersebut, salah satu skenario penyerangan dengan metode ini adalah dengan cara membajak IP prefixes yang memiliki kemungkinan untuk dapat mencegah atau membatalkan transaksi yang terjadi pada jaringan.

DDoS Attack

Penyerangan dengan metode ini kurang lebih mirip dengan penyerangan DDoS pada umumnya yaitu penyerang membanjiri traffic secara extreme, Penyerangan jenis ini adalah salah satu yang paling sering dilakukan ke dalam teknologi blockchain dengan tujuan untuk menghalangi transaksi sehingga transaksi tersebut tidak dapat dieksekusi. Namun karena sifat terdistribusi yang dimiliki oleh blockchain, maka serangan dengan metode ini tidak akan berdampak pada keseluruhan aktivitas jaringan namun hanya pada beberapa tingkat tertentu saja.

Blockchain Attacks

Terdapat beberapa jenis attacks yang terkenal dalam dunia blockchain antara lain Eclipse Attacks, Selfish Miner Attack dan yang akan kita bahas pada makalah ini yaitu 51%-Attack. Pada sistem blockchain, para entitas yang melakukan validasi (untuk seterusnya akan disebut penambang), hanya akan menyebarkan blok baru kepada seluruh penambang yang terdapat pada jaringan dan hal ini cukup berbahaya karena akan dapat dimonopoli oleh attackers (selanjutnya akan disebut dengan penyerang). Adalah sebuah hal yang berbahaya ketika seorang penyerang memonopoli koneksi masuk dan keluar blok, maka akan terjadi isolasi pada penambang yang terdapat dalam suatu jaringan tersebut. Terlebih, apabila blok ini memiliki kunci yang strategis terhadap banyak blok lainnya, penambang akan membutuhkan lebih banyak daya komputasi yang pada akhirnya akan digunakan untuk membantu kebutuhan si penyerang ini. Penyerangan seperti ini disebut dengan Eclipse Attack. Berbeda dengan Eclipse Attack, Selfish Miner Attack merupakan sebuah cara di mana penyerang dalam suatu kondisi tertentu mendapatkan reward yang tidak proporsional. Dalam konteks hal ini, penyerang dapat menjaga suatu blok agar bersifat private hingga blok ini tumbuh cukup besar, lalu ketika ada suatu cabang dari blok mendekat, para penyerang akan menyebarkan blok-blok yang telah disimpan secara private tadi sehingga dalam kondisi ini penyerang dan penambang akan sama-sama menghabiskan banyak resources. Namun dalam kondisi ini, penyerang tentu mendapatkan keunggulan persaingan jika dibandingkan dengan penambang.