Three Attacks on Proof-of-Stake Ethereum

Proof-of-Stake (PoS) Ethereum consensus protocol dibagun dengan menerapkan finality gadget Casper FFG diatas fork choice rule LMD GHOST, a flavor of the Greedy Heaviest-Observed Sub-Tree (GHOST) yang dianggap hanya suara terbaru setiap peserta. Peserta dengan stake yang memungkinkan mereka untuk memilih sebagai bagian dari protocol disebut validator. Varian yang sedikit sederhana dan secara analitis lebih penurut dari PoS Ethereum diberikan oleh Gasper protocol.

Serangan terbaru telah menghadirkan dua serangan terhadap Gasper dan PoS Ethereum. Serangan pertama adalah menggunakan jarak pendek reorganization dari blockchain menetapkan consensus untuk menunda finalitas keputusan consensus. reogs jarak pendek juga memungkinkan validator untuk meningkatkan pendapatan mereka dari berpartisipasi dalam protocol. Hasilnya, validator yang jujur tapi rasional akan menyimpang dari protocol dan mengancam asumsi yang mendasari argument keamanan untuk itu. Serangan kedua, mengeksploitasi penundaan jaringan permusuhan dan pemungutan suara strategis dengan fraksi validator musuh yang menghilangkan untuk menghentikan protocol tanpa batas.

Serangan ketiga sangat parah untuk PoS Ethereum karena tiga alas an :

1. Validator yang jujur tetapi rasional mungkin mengadosi strategi tersebut karena mereka dapat menggunakan untuk meingkatkan pembayaran mereka dari MEV dan biaya transaksi.
2. Reorg menyebabkan ketidakpastian dan keterlambatan dalam konfirmasi blokir, yang memengaruhi pengalaman pengguna dan kualitas layanan, dan merusak kepercayaan pengguna pada protocol
3. Reorg bisa kurangi throughput lapisan consensus ke titik di mana tidak cukup suara dapat diproses tepat waktu, mengurangi ketahanan terhadap validator permusuhan dan membahayakan berfungsinya PoS Ethereum

Proof-of-Stake Ethereu: The Gasper Protocol

1. Model

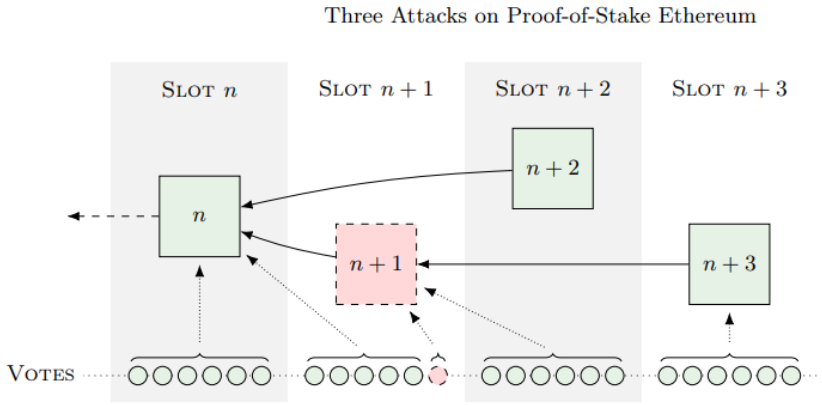
Dalam basic version, rumusan konsesnus state machine replication (SMR) meminta protocol dapat dijalankan di antara perserta protocol N untuk mendapatkan urutan linier dari input transaksi oleh lingkungan ke peserta, ke dalam buku besar Bersama dengan property keamanan berikut:

- Liveness : jika beberapa validator jujur mengetahui sesuatu transaksi, maka tidak terlalu lama kemudian transaksi itu akan masuk ke buku besar sebagai output oleh validator yang jujur
- Safety : Keluaran buku besar validator jujur yang berbeda pada titik yang berbeda dalam waktu yang konsisten. Dengan kata lain tidak terjadi suatu transaksi, yang pernah memasuki buku besar dalam pandangan validator yang jujur di beberapa waktu

2. Protocol
   Menjadi komposit dengan LMD GHOST fork choice rule sebagai dasar dan Casper FFG sebagai finalitas gadged di atas, PoS Ethereum consensus dalam dua tahap dan pada dua skala waktu.
   Pertama, pada skala waktu yang lebih kecil di mana LMD GHOST beroperasi, waktu terus bejalan dalam slot yang disinkronkan dengan durasi 2 Δ. Untuk setiap slot, satu pengusul blok dan komite validator W diambil secara acak dari N validator.

Kedua, pada skala waktu yang lebih besar di mana Casper FFg beroperasi, waktu terus berjalan di zaman terdiri dari 32 slot. Pada tingkat tinggi, Casper FFG adalah protocol consensus toleran kesalahan Bizantium (BFT) gaya tradisional dua fase yang diusulkan dan dipilih.

A Rifined Reorg Attack



1. Refined Reorg Strategy
   Pada gambar 1, menunjukan musuh sebagai pengusul slot n+1 sserta mengendalikan angota komite di slot n+1. Penggambaran permusuhan strategi untuk melakukan 1-reorg:
   a. Di awal slot n+1 musuh secara pribadi membuat block n+1 di block n dan secara pribadi membutikannya. Validator yang melihat block n+1 dan jadi mereka membuktikan kepala rantai sebelumnya, block n.
   b. Di awal slot berikutnya, validator yang jujur mengusulkan block n +2. Dengan asumsi nol latensi jaringan untuk saat inim musuh akhirnya menerbitkan block pribadi dan pengesahan dari slot n+1 pada saat yang sama dengan block n+2 dilepaskan. Validator jujur sekarang melihat kedua blok n+1 serta block n+2. Block ini saling bertentangan karena mereka berbagi induk yang sama, blok n. Hasil lain dari berbagi parent yang sama adalah bahwa balok n+1 mewarisi semua berat balok n, khususnya yang jujur pengesahan dari slot n+1 pemungutan suara untuk n juga mendukungnya.
   c. Oleh karena itu, slot n+2 semua validator yang jujur memilih block n+1 sebagai ketua chain, karena memiliki bobot lebih karena pengesahan permusuhan tubggal dari celah n+1
   d. Akhirnya, di awal slot n+3, validator yang jujur mengusulkan block n+3 menunjuk ke blok n+1 sebagai induknya.