Nama : Ersan Aythamsyach

NIM : 1103184061

Nakamoto: aturan konfirmasi k-deep. Dalam protokol ini, semua penambang bekerja pada rantai terpanjang, tetapi clients yang berbeda dapat memilih nilai k yang berbeda untuk menentukan seberapa dalam blok harus berada dalam rantai terpanjang untuk mengkonfirmasinya. Klien yang memilih nilai yang lebih besar untuk k adalah klien yang lebih konservatif, percaya pada penyerang yang lebih kuat atau menginginkan keandalan yang lebih besar, dan buku besarnya adalah awalan dari klien yang lebih agresif yang memilih nilai k yang lebih kecil. Konsep konsensus fleksibel ini diformalkan dan dikembangkan lebih lanjut pada tahun 2000, di mana klien yang berbeda dapat membuat asumsi yang berbeda tentang sinkronisitas jaringan serta kekuatan musuh.

Gasper adalah protokol kandidat saat ini untuk rantai suar Ethereum 2.0. Protokol Gasper sangat kompleks, menggabungkan gadget finalitas Casper FFG dengan lmd *(Latest Message Driven*) GHOST fork choice rule dengan cara buatan tangan. Dengan tujuan utamany adalah:

1) Kemampuan untuk menyelesaikan blok tertentu di blockchain. Selain toleransi partisi jaringan, finalisasi juga memungkinkan akuntabilitas melalui pemotongan pelanggar protokol.
2) Dukungan dari buku besar terdistribusi yang sangat tersedia yang tidak berhenti bahkan ketika finalitas tidak tercapai. Ketersediaan adalah fitur utama dari blockchain Ethereum global yang ada. Teorema (Informal). Pertimbangkan lingkungan jaringan di mana:

1) Komunikasi tidak sinkron sampai waktu stabilisasi global GST setelah itu komunikasi menjadi sinkron, dan

2) node jujur tidur dan bangun sampai waktu terjaga global GAT setelah semua node terjaga. Node musuh selalu terjaga.

Kemudian

1) (P1 - Finalitas): Buku besar yang diselesaikan LOGfin dijamin aman setiap saat, dan hidup setelah max{GST, GAT}, asalkan kurang dari 33% dari semua node bersifat permusuhan.

2) (P2 - Ketersediaan Dinamis): Jika GST = 0, buku besar YANG tersedia ^{LOGda} dijamin aman dan hidup setiap saat, asalkan setiap saat kurang dari 50% dari node terjaga adalah permusuhan.

Gasper adalah proposal saat ini untuk rantai suar Ethereum 2.0. Berikut ini, kami menunjukkan serangan liveness terhadap Gasper dalam model jaringan sinkron. Terlebih lagi,

serangan itu menyebabkan hilangnya keamanan untuk buku besar yang tersedia secara

dinamis. Dengan demikian, Gasper tidak aman dalam model jaringan sinkron dan tidak memberikan resolusi untuk dilema ketersediaan-finalitas.

Gasper adalah protokol PoS berbasis suara yang menggabungkan Casper FFG dengan mekanisme proposal blok blockchain berbasis komite di mana garpu (yaitu, ujung rantai untuk mengusulkan blok baru atau memilih) dipilih menggunakan aturan 'sub-pohon terberat yang paling rakus' (GHOST) di bawah paradigma 'pesan terbaru yang didorong' (LMD), yaitu, dengan mempertimbangkan hanya suara terbaru per validator. Pemungutan suara Gasper terdiri dari dua bagian, suara GHOST dan suara Casper FFG. Sementara rincian Gasper menghalangi serangan memantul vanili pada lapisan Casper FFG, Gasper rentan terhadap serangan penyeimbangan serupa pada lapisan GHOST.

Adapun attack pada proof of stake Ethereum

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 dapat dikategorikan sangan berbahay untuk PoS dikarenakan sebagai berikut:

1. Validator yang jujur tetapi rasional memungkinkan mengadopsi strategi ini karena mereka dapat menggunakannya untuk meningkatkan pembayaran MEV mereka dan biaya transaksi
2. REORG menyebabkan ketidakpastian dan keterlambatan dalam pengkonfirmasian pemblokiran, yang dimana akan mempengaruhi pengalaman pengguna dan kualitas layanan, dan yang lebih parahnya adalah merusak dari kepercayaan pengguna dalam penggunaan protocol
3. REORG dapat mengurangi throughput pada lapisan kosensus ke titik dimana tidak cukup suara dapat di proses dengan tepat waktu.

Casper adalah POS yang berada di atas POW blockchain, casper sendiri adalah mekanisme kosensus yang menggabungkan algoritma POS dan kesalahan dari byzantine yang dimana system ini membuktikan fitur yang dibutuhkan untuk jarak jauh dan memiliki kesalahan besar.

Fitur casper yang belum tentu di dukung oleh BFT diatara lainy adalah

- Accountability
- Dynamic Validator
- Defenceses
- Modular Overlay