Summary 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 suar terbaru pada setiap peserta. Peserta dengan stake yang memungkinkan mereka untuk bisa 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. Sedangkan serangan ketiga adalah serangan gabungan dari serangan pertama dan kedua.

Dampak dari serangan gabungan tidak bisa dianggap enteng, berikut adalah alasan kenapa serangan gabungan adalah serangan yang sangat parah. Pertama, Validator yang jujur tetapi rasional mungkin mengadosi strategi tersebut karena mereka dapat menggunakan untuk meingkatkan pembayaran mereka dari MEV dan biaya transaksi. Kedua, Reorg menyebabkan ketidakpastian dan keterlambatan dalam konfirmasi blokir, yang memengaruhi pengalaman pengguna dan kualitas layanan, dan merusak kepercayaan pengguna pada protocol. Terakhir, 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.