Nama : Muh. Farhan Ardhi Nugraha

NIM : 1103184032

Kelas : TK – 42- PIL

* Three Attacks on Proof-of-Stake Ethereum

Baru-baru ini, dua serangan diajukan terhadap Proof-of-Stake (PoS) Ethereum: satu di mana reorganisasi jangka pendek dari bawah -rantai konsensus berbohong digunakan untuk meningkatkan keuntungan validator individu dan menunda keputusan konsensus, dan satu di mana penundaan jaringan permusuhan dimanfaatkan untuk menghentikan keputusan konsensus tanpa batas. Kami menyediakan halus varian dari serangan ini, sangat melonggarkan persyaratan pada ad- pasak dan pengaturan waktu jaringan yang berbeda, dan dengan demikian membuat serangan lebih banyak berat. Menggabungkan teknik dari kedua serangan yang disempurnakan, kami memperoleh serangan ketiga yang memungkinkan musuh dengan fraksi yang semakin kecil saham dan tidak ada kontrol atas propagasi pesan jaringan (dengan asumsi alih-alih propagasi pesan probabilistik) untuk menyebabkan konflik jarak jauh. reorganisasi rantai sensus. Jujur-tetapi-rasional atau bermotivasi ideologis

validator yang terhormat dapat menggunakan serangan ini untuk meningkatkan keuntungan mereka atau menghentikan protokol, mengancam penyelarasan insentif dan keamanan PoS Ethereum. Serangan itu juga dapat menyebabkan destabilisasi konsensus dari kemacetan

dalam pengolahan suara.

* Casper the Friendly Finality Gadget

Casper, bukti sistem finalitas berbasis pasak yang menutupi bukti yang ada dari

kerja blockchain. Casper adalah mekanisme konsensus parsial yang menggabungkan bukti algoritma taruhan penelitian dan teori konsensus toleransi kesalahan Bizantium. Kami memperkenalkan sistem kami, buktikan beberapa fitur yang diinginkan, dan menunjukkan pertahanan terhadap revisi jarak jauh dan kecelakaan besar. Lapisan luar Casper menyediakan hampir semua bukti rantai kerja dengan perlindungan tambahan terhadap memblokir pengembalian.

Selama beberapa tahun terakhir telah ada banyak penelitian tentang blockchain berbasis “bukti kepemilikan” (PoS)

algoritma konsensus. Dalam sistem PoS, blockchain menambahkan dan menyetujui blok baru melalui proses di mana

siapa pun yang memegang koin di dalam sistem dapat berpartisipasi, dan pengaruh yang dimiliki agen sebanding dengan

jumlah koin (atau 'taruhan') yang dimilikinya. Ini adalah alternatif yang jauh lebih efisien untuk 'penambangan' proof of work (PoW)

dan memungkinkan blockchain untuk beroperasi tanpa biaya perangkat keras dan listrik penambangan yang tinggi.

Ada dua aliran pemikiran utama dalam desain PoS. Bukti taruhan pertama, berbasis rantai meniru bukti

mekanisme kerja dan menampilkan rantai blok dan mensimulasikan penambangan dengan secara acak memberikan hak untuk

membuat blok baru untuk pemangku kepentingan. Ini termasuk karya Peercoin[3], Blackcoin, dan Iddo Bentov.

Sekolah lain, Byzantine Fault Toleran (BFT) berbasis bukti pasak, didasarkan pada tubuh tiga puluh tahun

penelitian algoritma konsensus BFT seperti PBFT .peserta protokol adalah

mengikuti protokol dengan jujur, maka, terlepas dari latensi jaringan, algoritme tidak dapat menyelesaikan konflik

blok. Penggunaan kembali algoritma BFT untuk proof of stake pertama kali diperkenalkan oleh Tendermint, dan sudah modern

inspirasi seperti . Casper mengikuti tradisi BFT ini, meskipun dengan beberapa modifikasi.

* Highway: Efficient Consensus with Flexible Finality

Baru-baru ini ada banyak kemajuan dalam merancang sinkron sebagian yang efisien

Protokol konsensus BFT yang dimaksudkan sebagai mesin konsensus inti untuk Proof of Stake

sistem blockchain. Sementara solusi tercanggih mencapai kinerja yang hampir optimal

di bawah model teoretis ini, masih ada ruang untuk perbaikan, karena beberapa aspek praktis

sistem tersebut tidak ditangkap oleh model ini. Terutama, selama eksekusi reguler,

karena insentif keuangan dalam sistem seperti itu, orang mengharapkan sebagian besar node

untuk jujur ​​mengikuti aturan protokol dan hanya sedikit dari mereka yang salah, kemungkinan besar karena masalah jaringan sementara. Secara intuitif, fakta bahwa hampir semua node berperilaku jujur ​​seharusnya menghasilkan kepercayaan yang lebih kuat pada blok yang diselesaikan dalam periode tersebut, namun tidak demikian di bawah model klasik, di mana finalitas adalah biner.

Kami mengusulkan Highway, protokol konsensus baru yang aman dan hidup di par-

model BFT yang sangat sinkron, sementara pada saat yang sama menawarkan peningkatan praktis atas solusi yang ada. Secara khusus, finalitas blok di Highway bukan biner tetapi dinyatakan oleh fraksi node yang perlu melanggar aturan protokol agar blok dapat kembali

terbalik. Selama periode partisipasi yang jujur, finalitas blok mungkin mencapai lebih dari 1∕3

(seperti apa yang akan menjadi maksimum untuk protokol klasik), hingga genap 1 (kepastian lengkap). Setelah finalitas ditentukan dengan cara ini, Highway menawarkan fleksibilitas sehubungan dengan konfigurasi ambang keamanan di antara node yang menjalankan protokol, memungkinkan node dengan ambang batas yang lebih rendah

tua untuk mencapai finalitas lebih cepat daripada yang membutuhkan tingkat kepercayaan yang lebih tinggi.

* Incentives in Ethereum’s Hybrid Casper Protocol

hybrid Casper the Friendly Finality Gadget (FFG): protokol pos pemeriksaan Proof-of-Stake yang dilapiskan ke blockchain Proof-of-Work Ethereum. Kami menjelaskan fungsionalitas intinya dan skema penghargaan, dan menjelajahi propertinya. Temuan kami menunjukkan bahwa mekanisme insentif yang diterapkan Casper memastikan keaktifan, sekaligus memberikan jaminan keamanan yang lebih baik daripada protokol Proof-of-Work standar. Berdasarkan implementasi protokol dengan dampak minimal sebagai kontrak cerdas di blockchain, kami membahas masalah tambahan terkait parametrisasi, pendanaan, throughput, dan overhead jaringan serta mendeteksi potensi keterbatasan.

Ketentuan Indeks.

* A Survey on Long-Range Attacks for

Proof of Stake Protocols

Terlepas dari argumen umum tentang prevalensi teknologi blockchain, dalam hal keamanan, privasi, dan kekekalan, pada kenyataannya, beberapa serangan dapat diluncurkan terhadap mereka. Makalah ini memberikan tinjauan literatur sistematis tentang serangan jarak jauh untuk bukti protokol pasak. Jika berhasil, serangan ini dapat mengambil alih rantai utama dan sebagian, atau bahkan seluruhnya, menulis ulang riwayat transaksi yang disimpan di blockchain. Untuk tujuan ini, kami menjelaskan cara kerja protokol bukti pasak, fundamentalnya properti, kekurangannya, dan permukaan serangannya. Setelah menghadirkan serangan jarak jauh, kami membahas kemungkinanpenanggulangan dan penerapannya.