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

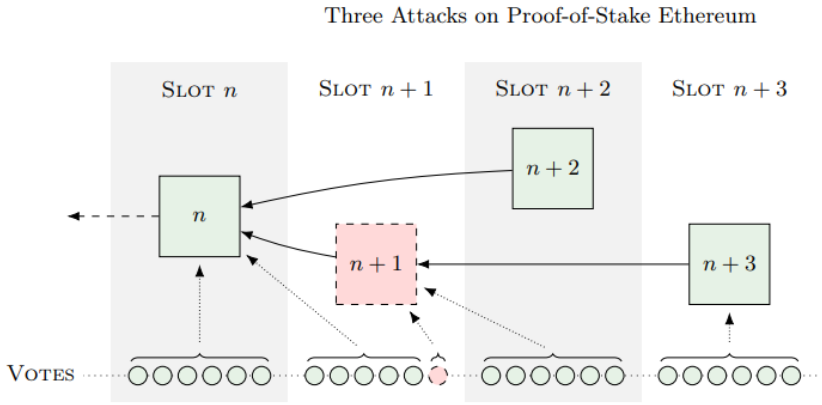
Dalam basic version, rumusan konsesnus state machine replication (SMR) meminta protocol dapat dijalankan di antara perserta protocol N untuk mendapatkan urutan linier dari input transaksi oleh lingkungan ke peserta, ke dalam buku besar Bersama dengan property keamanan berikut:

- 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.

CASPER THE FRIENDLY FINALITY GADGET

Penelitian ini memperkenalkan 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. Penelitian ini memperkenalkan sistem Penelitian ini, 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 blokir 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. Penelitian ini mempresentasikan Casper, bukti baru dari sistem pasak yang berasal dari literatur toleransi kesalahan Bizantium. Casper tetap tidak sempurna. Misalnya, mekanisme proposal blok yang sepenuhnya dikompromikan akan mencegah Casper dari menyelesaikan blok baru. Casper adalah peningkatan keamanan ketat berbasis PoS untuk hampir semua rantai PoW. Itu masalah yang tidak sepenuhnya diselesaikan Casper, terutama yang terkait dengan serangan 51%, masih dapat diperbaiki menggunakan garpu lunak yang diaktifkan pengguna. Sistem Casper saat ini dibangun berdasarkan bukti mekanisme proposal blok kerja. Kami berharap untuk mengubah mekanisme proposal blok menjadi bukti kepemilikan. Kami ingin membuktikan keamanan yang akuntabel dan masuk akal keaktifan bahkan ketika bobot set validator berubah dengan hadiah dan penalti.

PROOF OF STAKE MADE SIMPLE WITH CASPER

Sebagian besar blockchain publik seperti Bitcoin dan mengandalkan bukti kerja untuk mencapai mufakat. Peserta, yang disebut penambang, bersaing untuk memecahkan teka-teki kriptografi untuk tambahkan blok baru dan terima hadiah. arena biaya modal awal yang tinggi dan skala ekonomi, penambang menjadi lebih besar dan sistem menjadi lebih terpusat. Akhirnya, satu-satunya cara bukti kerja mencegah penyerang melanggar konsensus adalah dengan menghabiskan banyak upaya komputasi pada perangkat utama blockchain: untuk bertahan melawan penyerang, jaringan harus mengeluarkan uang sebanyak penyerang. Proof of stake menggunakan seperangkat validator untuk mencapai konsensus pada rantai utama. Validator ini menyetor sejumlah cryptocurrency blockchain dan memberikan suara yang ditimbang berdasarkan saham mereka. Tidak perlu listrik dikonsumsi, dan sistem sepenuhnya terdesentralisasi karena tidak ada skala ekonomi. Itu keuntungan terbesar dari bukti kepemilikan seperti Casper adalah penyerang dapat diidentifikasi dan deposit mereka dapat segera dihancurkan. Sebagai bukti kerja, Anda tidak dapat menghancurkan perangkat keras penyerang setelah serangan. Tujuan penelitian ini adalah untuk menjelaskan secara detail apa itu proof of stake dan apa itu Casper. Penelitian ini menggambarkan protokol, peran validator, dan cara menyelesaikan blok. Penelitian ini kemudian membuktikan bahwa Casper menjamin keamanan yang akuntabel dan kehidupan yang masuk akal. Kontribusi utama Penelitian ini adalah merilis basis kode sederhana untuk bereksperimen dengan algoritma konsensus. Penelitian ini telah merinci dan mudah-mudahan membuatnya lebih mudah untuk memahami bagaimana Casper berhasil mencapai konsensus menggunakan bukti kepemilikan. Implementasi Casper Penelitian ini memungkinkan siapa saja yang memiliki pengetahuan dasar tentang python untuk memahami detail protokol dan memvisualisasikan apa yang terjadi di dalam jaringan. Dengan plot blockchain seperti yang terlihat oleh masing-masing validator, kita dapat lebih memahami bagaimana latensi memengaruhi penyebaran blok dan jumlah pos pemeriksaan yang dibenarkan atau diselesaikan. Penelitian ini telah bereksperimen dengan berbagai parameter untuk Casper dan menemukan bahwa konsensus dapat dicapai bahkan dalam kondisi yang merugikan. Algoritme ini secara mengejutkan kuat untuk node yang terputus dan akan andal mencapai konsensus bahkan dengan latensi tinggi.

INCENTIVE ON CASPER

Dalam makalah ini, kami menganalisis kontrak Casper FFG yang dievaluasi pada testnet Ethereum khusus. Kami menjelaskannyamekanisme inti dan menunjukkan bahwa skema insentifnya memastikan liveness sambil memberikan safety terhadap finalisasi sejarah yang saling bertentangan,

yaitu, pos pemeriksaan. Sebagai protokol finalitas yang dapat dilapisi pada blockchain PoW dan PoS, hibrida Casper FFG dapat menarik bagi khalayak luas dalam ekosistem blockchain. Temuan kami tentang liveness, safety, insentifkompatibilitas, dan implementasi tetap sangat relevan untuk transisi Ethereum ke desain yang terpecah di manaFilosofi Casper FFG terbawa.

A Survey on Long-Range Attacks for Proof of Stake Protocols

Revolusioner Bitcoin yang membuatnya terkenal di seluruh dunia, ada jauh lebih banyak potensi dari teknologi yang mendasarinya. Nakamoto menggunakan primitif kriptografi yang kuat untuk memperkenalkan menghasilkan teknologi blockchain, peer-to-peer terdistribusi. Prevalensi teknologi blockchain, dalam hal keamanan, privasi, dan kekekalan, pada kenyataannya, beberapa serangan dapat diluncurkan terhadap mereka. 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 kemungkinan penanggulangan dan penerapannya. blockchain ini didasarkan pada concept of Proof of Work (PoW). Secara praktis, kami menganggap pengguna dapat dipercaya karena dia menghabiskan banyak uang upaya komputasi untuk memverifikasi beberapa transaksi. Sebaliknya protokol Proof of Stake (PoS), pengguna yang validasi transaksi yang dipilih berdasarkan kekayaan (stake). Serangan Jarak Jauh yang berhasil tidak hanya akan mengubah beberapa blok tetapi akan memungkinkan musuh untuk sepenuhnya menulis ulang sejarah semua transaksi yang disimpan dalam blockchain. Seperti dimaklumi, serangan ini mungkin tidak berasal dari implementasi protokol tertentu, tetapi dari desainnya, membuatnya agak sulit untuk ditambal. Tindakan pencegahan ini dapat memberikan perlindungan penuh dari semua ancaman tersebut. Bahkan lebih solusi yang diusulkan bersifat parsial untuk setiap ancaman secara individual. Terlepas dari timestamping dan mengintegrasikan rantai terpanjang aturan dan pos pemeriksaan bergerak yang tampaknya terintegrasi oleh semua protokol, ada keragaman dalam integrasi sisanyapenanggulangan dari protokol. Sedangkan penggunaan TEE sangat menjanjikan, mereka tidak diterapkan oleh salah satu dari protokol sebagai adopsi mereka menyiratkan kendala perangkat keras