TUGAS 6

NAMA : SHELY BELINDA BR GINTING

NIM : 1103190009

1. Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma

Akibatnya, satu periode singkat asinkron sudah cukup untuk mengatur sistem konsensus sedemikian rupa sehingga kedua rantai tumbuh di paralel tanpa batas. Tidak ada pos pemeriksaan yang akan diselesaikan, kios protokol. Terlebih lagi, karena flip-flop pilihan garpu s antara dua rantai, blockchain yang mendasarinya dirender tidak aman oleh aturan pilihan garpu yang dimodifikasi. dua arah interdependensi Casper FFG dan blockchain memberikan pengaruh utama musuh atas simpul jujur pada proposal lapisan dan dengan demikian memungkinkan serangan ini. Sebaliknya, gaya BFT sinkron sebagian yang terisolasi protokol, mirip dengan Casper FFG, pada akhirnya akan pulih er dari periode asinkron dan kembali keaktifan,

sambil tetap aman di seluruh. Demikian pula, tipikal yang terisolasi protokol rantai terpanjang yang tersedia secara dinamis dengan garpu utuh aturan pilihan bisa saja mengalami pelanggaran keamanan selama dan segera setelah periode asinkron, tetapi akan memiliki 'sembuh' akhirnya, yaitu, dari beberapa titik, tidak ada lagi keamanan pelanggaran terjadi dan transaksi dimasukkan ke dalam buku besar.

2. Three Attacks on Proof-of-Stake Ethereum

Kami memberikan ringkasan singkat tentang protokol PoS Ethereum/Gasper danlingkungan jaringan yang dirancang untuknya. Eksposisi sedikit diidealkan dandisederhanakan untuk memudahkan pemahaman. Untuk semua detailnya, lihat makalah dari Gasper dan spesifikasi protokol rantai suar PoS Ethereum

Ingatlah bahwa serangan penyeimbang terdiri dari dua langkah: Pertama, permusuhan pengusul blok memulai dua rantai yang bersaing – sebut saja Kiri dan Kanan. Kemudian segelintir suara permusuhan per slot, dirilis di bawah lingkungan yang dipilih dengan cermat sikap, cukup untuk mengarahkan suara validator yang jujur untuk menjaga sistem tetap seri antara dua rantai dan akibatnya menghentikan konsensus.

3. Casper the Friendly Finality Gadget

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.

Casper the Friendly Finality Gadget adalah overlay di atas mekanisme proposal—mekanisme yang mengusulkan blok1. Casper bertanggung jawab untuk menyelesaikan blok-blok ini, pada dasarnya memilih rantai unik yang mewakili transaksi kanonik dari buku besar. Casper memberikan keamanan, tetapi keaktifan tergantung pada proposal yang dipilih mekanisme. Artinya, jika penyerang sepenuhnya mengontrol mekanisme proposal, Casper melindungi dari penyelesaian dua pos pemeriksaan yang saling

bertentangan, tetapi para penyerang dapat mencegah Casper menyelesaikan pos pemeriksaan di masa mendatang.

4. Highway: Efficient Consensus with Flexible Finality

Dalam sistem blockchain yang khas, validator ditugaskan untuk melakukan konsensus berulang pada rantai transaksi yang terus berkembang yang mereka terima dari lingkungan eksternal. Dalam proses, mereka melampirkan transaksi ke dalam blok yang membentuk blockchain, di mana setiap blok merujuk ke pendahulunya dengan hash. Yang pertama, blok genesis, adalah bagian dari definisi protokol. Di Highway, karena set validator adalah konstan atau hanya tunduk pada perubahan yang sangat terkontrol (antara era yang berbeda, lihat Subbagian, validator khusus ditunjuk langsung untuk membangun blok dalam slot waktu tertentu. Mereka melakukannya dengan melampirkan transaksi dari antrian lokal dan hash dari blok yang mereka yakini harus menjadi pendahulunya. Seperti yang mungkin terjadi bahwa validator tidak merujuk ke blok yang dibangun terakhir (baik secara sengaja, atau karena kegagalan jaringan), himpunan blok adalah pohon, dengan jalur unik yang mengarah dari masing-masing blok blok ke root: genesis blok G. Tujuan utama dari protokol konsensus dalam skenario seperti itu adalah memilih satu cabang dari pohon seperti itu. Untuk blok B, kami merujuk ke semua blok yang ada di cabang-cabang lain bersaing dengan B, seolah-olah salah satu dari mereka akan dipilih, B tidak bisa.

5. Incentives in Ethereum’s Hybrid Casper Protocol

Kontribusi dari makalah ini adalah sebagai berikut. Kami pertama-tama memberikan gambaran umum tentang protokol Casper FFG dan menggambarkan fungsi intinya. Untuk alasan tentang kehidupan dan keamanan, kami mengembangkan kerangka matematis untuk skema insentif, kondisi pemotongan, dan aturan pilihan garpu. Hasil teoretis pertama kami adalah bahwa dengan skema penghargaan yang diterapkan. Ethereum berfungsi sebagai komputer global yang operasinya direplikasi di jaringan peer-to-peer. Partisipan dalam jaringan disebut node – mereka biasanya berinteraksi dengan jaringan lainnya melalui aplikasi perangkat lunak yang disebut klien. Klien berinteraksi dengan blockchain Ethereum melalui transaksi. Ada tiga jenis transaksi utama: Transfer token menyediakan fungsionalitas inti yang sama dengan Bitcoin dengan mengizinkan node untuk bertukar token digital. Pembuatan kontrak mengunggah potongan kode, yang disebut kontrak (pintar), ke blockchain.

6. Incentives in Ethereum’s Hybrid Casper Protocol

Ethereum berfungsi sebagai komputer global yang operasinya direplikasi di jaringan peer-to-peer. Peserta dalam jaringan disebut node - mereka biasanya berinteraksi dengan sisa jaringan melalui aplikasi perangkat lunak yang disebut klien. Itu klien berinteraksi dengan blockchain Ethereum melalui transaksi. Ada tiga jenis utama transaksi: Transfer token menyediakan fungsionalitas inti yang sama dengan Bitcoin dengan memungkinkan node untuk bertukar token digital. Pembuatan kontrak mengunggah potongan kode, yang disebut kontrak (pintar), ke blockchain. Kontrak dieksekusi menggunakan runtime lingkungan yang disebut Ethereum Virtual Machine (EVM).1 Dua bahasa tingkat tinggi terkenal yang dikompilasi ke dalam EVM adalah Solidity dan Vyper yang masing-masing didasarkan pada bahasa JavaScript dan Python. Vyper sangat relevan untuk kertas ini seperti yang digunakan untuk kontrak Casper. Kontrak tipikal akan mencakup satu atau lebih fungsi yang dapat dipanggil oleh node.

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

Struktur ini mengelompokkan transaksi ke dalam blok yang divalidasi oleh kelompok pengguna blockchain. Dalam tra- blockchains tradisional, misalnya, Bitcoin, pengguna bersaing satu sama lain-lain dalam memecahkan masalah kriptografi/matematis yang sulit lem yang mudah diverifikasi. Proses ini disebut ''menambang,'' dan pemenangnya mendapatkan koin baru sebagai hadiah untuknya jasa. Oleh karena itu, blockchain ini didasarkan pada kon- kecuali Proof of Work (PoW). Secara praktis, kami menganggap pengguna dapat dipercaya karena dia menghabiskan banyak uang upaya komputasi untuk memverifikasi beberapa transaksi. Pada sebaliknya, dalam protokol Proof of Stake (PoS), pengguna yang validasi transaksi yang dipilih berdasarkan kekayaan (stake).

8. Proof of Stake Made Simple with Casper

Sebagian besar blockchain publik seperti Bitcoin (Nakamoto [2008]) dan Ethereum (Wood [2014]) mengandalkan bukti kerja untuk mencapai mufakat. Peserta, yang disebut penambang, bersaing untuk memecahkan teka-teki kriptografi untuk tambahkan blok baru dan terima hadiah. Semua perhitungan ini membutuhkan banyak energi untuk dijalankan, dan Bitcoin pada Desember 2017 menghabiskan listrik sebanyak Denmark Karena 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.