Nama : Hanif Shafwan Mahib

NIM : 1103194150

Kelas : TK-43-02

Tugas 6 Blockchain

I. Summary

1. EBB and Flow Protocol

Teorema CAP mengatakan bahwa tidak ada blockchain yang dapat hidup di bawah partisipasi dinamis dan aman di bawah sementara partisi jaringan. Untuk mengatasi dilema ketersediaan-finalitas ini, kami merumuskan kelas baru protokol konsensus fleksibel, protokol dan-aliran, yang mendukung sepenuhnya tersedia secara dinamis buku besar bersama dengan buku besar awalan yang telah diselesaikan. yang diselesaikan buku besar jatuh di belakang buku besar ketika partisi jaringan tetapi mengejar ketika jaringan sembuh.

Untuk inspirasi cara mengatasi dilema ini, mari kita meninjau kembali aspek penting lain dari Nakamoto's terpanjang protokol rantai: aturan konfirmasi k-deep. Dalam protokol ini, semua penambang bekerja pada rantai terpanjang, tetapi klien yang berbeda dapat memilih nilai k yang berbeda untuk menentukan seberapa dalam a blok harus berada di rantai terpanjang untuk mengonfirmasinya. Seorang klien yang memilih nilai k yang lebih besar adalah yang lebih konservatif klien, percaya pada penyerang yang lebih kuat atau menginginkan lebih reliabel, dan buku besarnya adalah awalan dari klien yang lebih agresif yang memilih nilai k yang lebih kecil.

2. EBB Flow

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 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.

3. POS Attacks 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.

4. POS Casper

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.

5. POS Highway

Kami mengusulkan Highway, protokol kesepakatan baru yang aman dan hidup dalam model BFT sinkron parsial klasik, sementara pada saat yang sama menawarkan peningkatan praktis atas solusi yang ada. Secara khusus, finalitas blok di Highway bukanlah biner tetapi dinyatakan oleh fraksi node yang perlu melanggar aturan protokol agar blok dapat dikembalikan. Selama periode partisipasi yang jujur, finalitas blok mungkin mencapai lebih dari 1/3 (seperti yang akan menjadi maksimum untuk protokol klasik), hingga genap 1 (kepastian lengkap).

Sejak diperkenalkannya Bitcoin dan konsep database yang terdesentralisasi dan anti-rusak database – sebuah blockchain – sejumlah paradigma yang berbeda telah dikembangkan untuk merancang database tersebut. Baru-baru ini, gagasan untuk membangun sistem semacam itu berdasarkan PoS (Proof of Stake) telah mendapatkan popularitas yang signifikan. Sementara dalam mekanisme PoW (Proof of Work, seperti yang digunakan dalam Bitcoin) asli yang digunakan untuk mendorong partisipasi dan mengamankan sistem, kekuatan suara seorang peserta sebanding dengan jumlah kekuatan komputasi yang dimiliki, dalam PoS kekuatan suara proporsional.

6. POS Incentive on Casper

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.

7. POS Long Range Attacks

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. 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).

Tindakan pencegahan dapat memberikan perlindungan penuh dari semua ancaman. 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.

8. POS Make 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.

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.