Nama : Weni Wilman Putri

NIM : 1103184134

Casper Protokol

Didalam Ethereum, mekanisme proposal pada awalnya akan menjadi POW chain, menjadikan versi pertama Casper sebagai sistem POW atau POS. Di masa depan, mekanisme proposal POW akan diganti dengan yang lebih efisien. Misalnya, kita dapat mengkonversi proposal blok menjadi semacam skema blok POS Round-Robin.

Dalam versi casper yang sederhana, ada seperangkat validator dan mekanisme proposal yang tetap yang menghasilkan child block dari block yang ada, membentuk block yang terus berkembang. Dalam keadaan normal, diharapkan mekanisme proposal akan mengusulkan blok satu demi satu dalam daftar tertaut. Tetapi dalam kasus latensi jaringan atau serangan yang disengaja, mekanisme proposal terkadang akan menghasilkan banyak child dari parent yang sama. Tugas Casper adalah memilih satu child dari setiap parent, sehingga memilih satu chain kanonik dari pohon balok.

Casper hanya mempertimbangkan subtree dari pos pemeriksaan membentuk pos pemeriksaan. Blok genesis adalah pos pemeriksaan, dan setiap blok yang tingginya di pohon blok (atau nomor blok) adalah kelipatan tepat 100 juga merupakan pos pemeriksaan. "Tinggi pos pemeriksaan" dari balok dengan tinggi balok$100 * k$ secara sederhana k; ekuivalen, tinggi h (c) dari sebuah pos pemeriksaan c adalah jumlah elemen dalam rantai pos pemeriksaan yang membentang dari c (non-inklusif) ke root di sepanjang tautan induk.

Setiap validator deposit; ketika validator bergabung, depositnya adalah jumlah koin yang disimpan. Setelah bergabung, setoran masing-masing validator naik dan turun dengan hadiah dan penalti. Bukti keamanan pasak berasal dari ukuran setoran, bukan jumlah validator, jadi kami mengatakan “2 per 3validator”, kami adalah mengacu pada setoranpecahan; yaitu, satu set validator yang jumlah jumlah depositnya sama dengan 2 per 3 dari total ukuran deposit dari seluruh set validator.

Pembuktian Keamanan

Kami membuktikan dua sifat dasar Casper:keamanan yang akuntabel dan keaktifan yang masuk akal. Keamanan yang akuntabel berarti bahwa dua pos pemeriksaan yang bertentangan tidak dapat diselesaikan keduanya kecuali $\geq 1/3$ validator melanggar (1/3 dari total deposit hilang. Keaktifan yang masuk akal berarti bahwa, terlepas dari setiap peristiwa sebelumnya (misalnya, peristiwa tebasan, blok tertunda, serangan sensor, dll.), jika $\geq 2/3$ validator mengikuti protocol. maka selalu mungkin untuk menyelesaikan pos pemeriksaan baru tanpa validator yang melanggar kondisi pemotongan.

Aturan Casper’s Fork

Casper lebih rumit daripada desain PoW standar. Dengan demikian, pilihan garpu harus disesuaikan. Aturan pilihan garpu yang dimodifikasi harus diikuti oleh semua pengguna, validator, dan bahkan mekanisme proposal blok yang mendasarinya. Jika pengguna, validator, atau pengusul blok malah mengikuti aturan pilihan garpu PoW standar "selalu membangun di atas rantai terpanjang", ada skenario patologis di mana Casper "terjebak" dan blok apa pun

yang dibangun di atas rantai terpanjang tidak dapat diselesaikan (atau bahkan dibenarkan) tanpa beberapa validator secara altruistik mengorbankan deposit mereka. Untuk menghindari hal ini, kami memperkenalkan sebuah novel, benar dengan konstruksi, pilihan fork.

Menghentikan Serangan

Ada dua serangan terkenal terhadap sistem POS :: long range revisions dan catastrophic crashes.

1. Long Range Revisions Dalam istilah sederhana, serangan jarak jauh dicegah oleh aturan pilihan garpu untuk tidak pernah mengembalikan blok yang telah diselesaikan, serta harapan bahwa setiap klien akan "masuk" dan mendapatkan tampilan lengkap terkini dari rantai di beberapa frekuensi reguler (misalnya, sekali per 1-2 bulan). Garpu "revisi jarak jauh" yang menyelesaikan blok yang lebih lama dari itu.
2. Catastrophic Crashes
   Algoritma yang tepat untuk pulih dari berbagai serangan ini tetap menjadi masalah terbuka. Untuk saat ini, kami menganggap validator dapat mendeteksi perilaku yang jelas-jelas tidak sesuai (misalnya, tidak menyertakan bukti) dan secara manual membuat "garpu lunak minoritas". Garpu minoritas ini dapat dilihat sebagai blockchain dalam dirinya sendiri yang bersaing dengan rantai mayoritas di pasar, dan jika rantai mayoritas benar-benar dioperasikan oleh penyerang jahat yang berkolusi maka kita dapat berasumsi bahwa pasar akan menyukai garpu minoritas.