Tugas Minggu 6

Fajri Nurfauazan | 1103180184 | TK-42-PIL

Selama beberapa tahun terakhir telah ada banyak penelitian tentang blockchain berbasis "*proof of stake*" (PoS). Dalam sistem PoS, blockchain menambahkan dan menyetujui blok baru melalui proses di mana jumlah koin (atau "*stake*") yang dimilikinya. Ini adalah alternatif yang jauh lebih efisien dari pada "*mining*" proof of work (PoW). Ada dua aliran pemikiran utama dalam desain PoS. Proof of stake pertama, berbasis rantai, meniru bukti mekanik kerja dan menampilkan rantai blok dan mensimulasikan penambangan dengan memberikan hak semu secara acak untuk membuat blok baru untuk pemangku kepentingan. Sekolah lain, Byzantine Fault Toleran (BFT) based proof of stake, didasarkan pada tubuh berusia tiga puluh tahun meneliti algoritma konsensus BFT seperti PBFT. Algoritme BFT biasanya telah terbukti secara matematis blok. Penggunaan kembali algoritma BFT untuk proof of stake pertama kali diperkenalkan oleh Tendermint, dan memiliki Casper yang mengikuti tradisi BFT ini, meskipun dengan beberapa modifikasi.

Casper adalah mekanisme konsensus parsial yang menggabungkan bukti penelitian algoritma pasak dan teori konsensus toleransi kesalahan Bizantium. Overlay Casper menyediakan hampir semua bukti rantai kerja dengan perlindungan tambahan terhadap pembalikan blok. 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 yang dimilikinya.

Work Casper the Friendly Finality Gadget kami 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 mekanisme proposal yang dipilih. Artinya, jika penyerang sepenuhnya mengontrol mekanisme proposal, Casper melindungi dari penyelesaian dua pos pemeriksaan yang saling bertentangan, tetapi penyerang dapat mencegah Casper menyelesaikan pos pemeriksaan di masa mendatang. Akuntabilitas memungkinkan kami untuk menghukum validator yang salah, memecahkan masalah "Tidak ada yang dipertaruhkan" yang mengganggu PoS berbasis rantai. Hukuman karena melanggar aturan adalah seluruh deposit validator. Fungsionalitas ini memiliki peran yang mirip dengan abstraksi umum "Pemilihan pemimpin" yang digunakan dalam algoritme BFT tradisional, tetapi disesuaikan untuk mengakomodasi konstruksi Casper sebagai overlay finalitas di atas blockchain yang ada.

Desain Casper sebagai overlay membuatnya lebih mudah untuk diterapkan sebagai peningkatan ke bukti rantai kerja yang ada dan menjelaskan Casper secara bertahap, dimulai dengan versi sederhana dan kemudian secara bertahap menambahkan perubahan set validator dan akhirnya pertahanan terhadap serangan. Protokol Casper Di dalam Ethereum, mekanisme proposal awalnya akan menjadi bukti rantai kerja yang ada, menjadikan versi pertama Casper sebagai sistem PoW/PoS hybrid. Kita dapat membayangkan mengubah proposal blok menjadi semacam skema penandatanganan blok round-robin PoS.

Dalam versi Casper yang sederhana ini, kami mengasumsikan ada seperangkat validator dan mekanisme proposal yang menghasilkan blok anak dari blok yang ada, membentuk pohon blok yang terus tumbuh. Tugas Casper adalah memilih satu anak dari setiap orang tua, sehingga memilih satu rantai kanonik dari pohon balok. Daripada berurusan dengan pohon blok penuh, untuk tujuan efisiensi2 Casper hanya mempertimbangkan subpohon dari pos pemeriksaan yang membentuk pohon pos pemeriksaan. Properti Casper yang paling menonjol adalah tidak mungkin untuk menyelesaikan dua pos pemeriksaan yang bertentangan kecuali 13 validator melanggar salah satu dari dua4 Perintah Casper/kondisi pemotongan.

Jika validator melanggar salah satu kondisi pemotongan, bukti pelanggaran dapat dimasukkan ke dalam blockchain sebagai transaksi, di mana seluruh deposit validator diambil dengan "biaya Finder" kecil yang diberikan kepada pengirim bukti transaksi. Di Ethereum saat ini, menghentikan penegakan kondisi tebasan membutuhkan serangan 51% yang berhasil pada pengusul blok proof-of-work Ethereum.

Sekarang anggaplah konflik am dan bn, dan tanpa kehilangan keumuman $h(am) < h(bn) = h(bn)$, maka jelas bahwa 13 validator melanggar kondisi I). Biarkan r b1 b2 bn menjadi rantai pos pemeriksaan, sehingga ada 4 Casper versi sebelumnya memiliki dua jenis pesan dan empat kondisi pemotongan , tetapi kami telah

menguranginya menjadi satu jenis pesan dan dua kondisi pemotongan. Aturan Pilihan Garpu Casper Casper lebih rumit daripada desain PoW standar.

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 tanpa beberapa validator secara altruistik mengorbankan deposit mereka.

Kesimpulan mempresentasikan Casper, bukti baru dari sistem pasak yang berasal dari literatur toleransi kesalahan Bizantium. Casper mencakup: dua kondisi pemotongan, aturan pilihan garpu konstruksi yang benar yang terinspirasi oleh , dan set validator dinamis. Akhirnya memperkenalkan ekstensi ke Casper untuk bertahan melawan dua serangan umum. Mekanisme proposal blok yang sepenuhnya dikompromikan akan mencegah Casper menyelesaikan blok baru. Casper adalah peningkatan keamanan ketat berbasis PoS untuk hampir semua rantai PoW.

Perkembangan di masa depan tidak diragukan lagi akan meningkatkan keamanan Casper dan mengurangi kebutuhan akan garpu lunak yang diaktifkan pengguna. Sistem Casper saat ini dibangun di atas bukti proposal blok kerja.