Qorio Surya Akbar

1103180038

TK-42-PIL

Blockchain

Casper adalah finalitas POS yang melapisi POW blockchain. Casper adalah mekanisme consensus yang menggabungkan algoritma POS dan teori kesalahan Byzantine. Sistem ini membuktikan beberapa fitur yang dibutuhkan dan pertahanan jarak jauh serta kesalahan besar. 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 dipilihmekanisme. 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.

Fitur Casper:

- Accountability, Jika validator melanggar aturan, kami dapat mendeteksi pelanggaran dan mengetahui validator mana melanggar aturan.
- Dynamic validators, untuk set validator untuk berubah seiring waktu
- Defenses. serangan revisi jarak jauh serta serangan di mana lebih dari 1/3 validator drop offline, dengan biaya asumsi sinkronisitas tradeoff yang sangat lemah.
- Modular overlay, Desain Casper sebagai overlay membuatnya lebih mudah untuk diterapkan sebagai peningkatan ke bukti rantai kerja yang ada

Casper Protocol

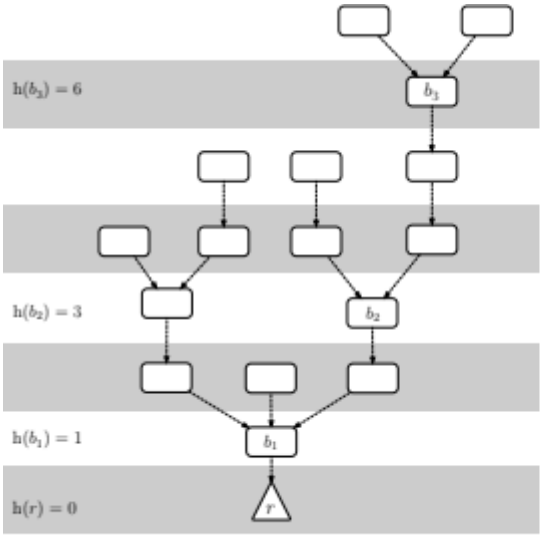
Di dalam Ethereum, mekanisme proposal pada awalnya akan menjadi bukti rantai kerja yang ada, menjadikannya yang pertama versi Casper sistem PoW/PoS hybrid. Di versi mendatang, mekanisme proposal PoW akan diganti dengan sesuatu yang lebih efisien. Misalnya, kita dapat membayangkan mengubah proposal blok menjadi semacam Skema penandatanganan blok round-robin PoS.

Dalam keadaan normal, kami berharap mekanisme proposal biasanya akan mengusulkan blok satu setelah lainnya dalam daftar tertaut (yaitu, setiap blok "induk" memiliki tepat satu blok "anak"). Tetapi dalam kasus jaringan latensi atau serangan yang disengaja, mekanisme proposal pasti kadang-kadang akan menghasilkan banyak anak dari orang tua yang sama. Tugas Casper adalah memilih satu anak dari setiap orang tua, sehingga memilih satu rantai kanonik dari pohon blok.

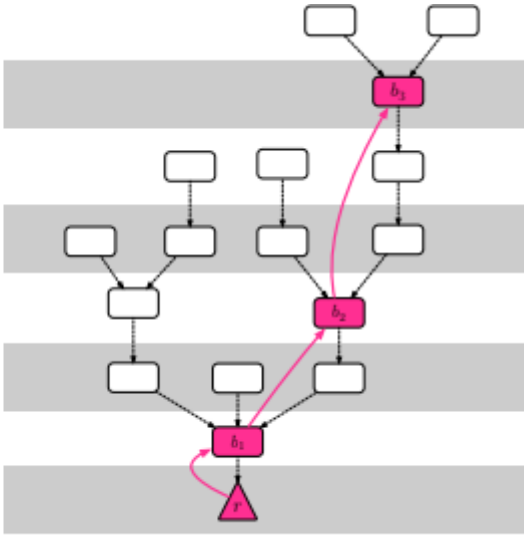
Daripada berurusan dengan pohon blok penuh, untuk tujuan efisiensi2 Casper hanya mempertimbangkan subpohon dari pos pemeriksaan membentuk pohon pos pemeriksaan. Blok genesis adalah pos pemeriksaan, dan setiap blok yang tingginya di pohon blok (atau nomor blok) adalah kelipatan tepat dari 100 juga merupakan pos pemeriksaan. "Tinggi pos pemeriksaan" dari sebuah blok dengan tinggi balok 100 k hanyalah k; ekuivalen, tinggi h(c) dari pos pemeriksaan c adalah jumlah elemen dalam.

Validator dapat menyiarkan pesan suara yang berisi empat informasi (Tabel 1): dua pos pemeriksaan s dan t bersama-sama dengan tinggi mereka h(s) dan h(t). Kami mengharuskan s menjadi nenek moyang t di pohon pos pemeriksaan, jika tidak pemungutan suara dianggap tidak sah. Jika kunci publik validator tidak ada dalam set validator, voting dianggap tidak sah. Bersama dengan tanda tangan dari validator, kami akan menulis suara ini dalam bentuk hν, s, t, h(s), h(t)i. rantai pos pemeriksaan yang membentang dari c (non-inklusif) ke akar di sepanjang tautan induk.

Notation	Description
s	the hash of any justified checkpoint (the "source")
t	any checkpoint hash that is a descendent of s (the "target")
$\mathrm{h}(s)$	the height of checkpoint s in the checkpoint tree
$\mathrm{h}(t)$	the height of checkpoint t in the checkpoint tree
$\mathcal{S}$	signature of $\langle s, t, \mathrm{h}(s), \mathrm{h}(t)\rangle$ from the validator ν's private key



(b) The height function



(c) The justified chain $r \rightarrow b_1 \rightarrow b_2 \rightarrow b_3$

- Supermajority link adalah sepadang pos pemeriksaan (a,b), juga ditulis a → b, sehingga setidaknya 2 per 3 validator (dari deposito) telah menerbitkan suara dengan sumber a dan target b. Supermajority link dapat melewati pos pemeriksaan, dan ini tidak masalah untuk h(b) > h(a) + 1. Gambar 1c menunjukan supermajority link berwarna merah: r → b1, b1 → b2, and b2 → b3
- Dua pos a dan b disebut bertentangan jika dan hanya jika mereka adalah nodes di cabang yang berbeda yaitu, tidak ada ancestor atau descendant yang lain.
- Checkpoint dibenarkan jika (1) adalah akarnya, atau (2) ada supermajority link c' → c dimana checkpoint c' dibenarkan. Gambar 1c menunjukkan chain dari 4 blok yang dibenarkan. Checkpoint yang disebut finalisasi jika (1) adalah akar (2) dibenarkan dan ada supermajority link c → c' dimana c' adalah child langsung dari c.