Casper Pos

Nama : Tegar Pandji Asmoro

Nim : 1103194006

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 adalah overlay diatas mekanisme proposal (proposal yang mengusulkan blok). Casper bertanggung jawab untuk menyelesaikan blok – blok ini. Pada dasarnya memilih chain unik yang mewakili transaksi kanonik dari ledger. 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 teteapi penyerang dapat mencegah Casper menyelesaikan pos pemeriksaan di masa mendatang.

Fitur Casper yang belum tentu didukung oleh algoritma BFT :

- *Accountability,* Jika validator melanggar aturan, casper dapat mendeteksi pelanggaran dan mengetahui validator mana yang melanggar aturan.
- *Dynamic validator,* Setiap set validator berubah seiring berjalannya waktu
- *Defenses,* pertahanan terhadap long range revision attacks serta serangan dimana lebih dari sepertiga validator offline, dengan biaya tradeoff synchronicity assumption sangat lemah.
- *Modular overlay,* Desain Casper sebagai overlay membuatnya lebih mudah untuk diterapkan sebagai peningkatan ke POW chain.

Casper Protokol

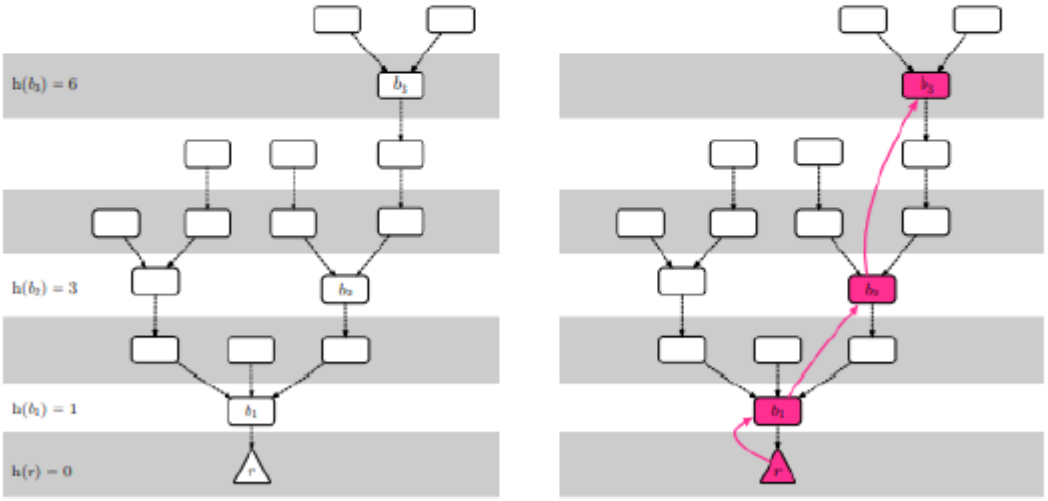
Didalam Ethereum, mekanisme proposal pada awalnya akan menjadi POW chain, menjadikan versi pertama Casper sebagai sistem POW atau POS. Di masa depan, mekanisme proposal POW akan diganti dengan yang lebih efisien. Misalnya, kita dapat mengkonversi proposal blok menjadi semacam skema blok POS Round-Robin. 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 balok100 $*$ 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 3 validator”, 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.

Validator dapat menyiarkanPilihpesan yang berisi empat informasi: dua pos pemeriksaan s dan t bersama dengan tinggi badan mereka h (s) dan h (t). Kami membutuhkan itu s menjadi nenek moyang t di pohon pos pemeriksaan, jika tidak, suara dianggap tidak sah. Jika kunci publik validator tidak ada dalam set validator, suara dianggap tidak sah. Bersama dengan tanda tangan validator, kami akan menulis suara ini dalam form (v, s, t, h(s), h(t)).

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 $r \rightarrow b_1 \rightarrow b_2 \rightarrow b_3$

Figure 1: Illustrating a checkpoint tree, the height function, and a justified chain within the checkpoint tree.