Casper Pos

Nama : Ryndam Putra Anugera

AsmoroNim : 1103184020

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 atacks 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 sebagaipeningkatan ke POW chain.**

Casper Protokol

Didalam Ethereum, mekanisme proposal pada awalnya akan menjadi POW chain, menjadikan versi pertamaCasper sebagai sistem POW atau POS. Di masa depan, mekanisme proposal POW akan diganti dengan yang lebihefisien. 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 menghasilkanchild 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 pemeriksan