Garry Abel Diaraja H

1103190147

TK-42-pil

WEEK 6 CASPER PoS

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 (Mendeteksi validator aman atau melanggar aturan)
- Dynamic validator (pemeriksaan setiap set validator yang 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.)
- Modulator overlay Desain Casper sebagai overlay membuatnya lebih mudah untuk diterapkan sebagai peningkatan ke POW chain.

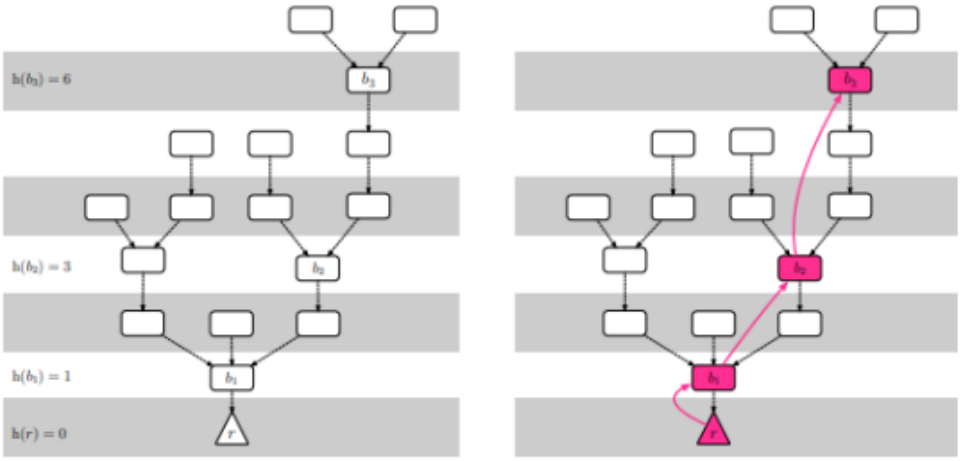
Cara Kerja Casper

Transisi dari Ethereum 1.0 ke 2.0 dijuluki sebagai pembaruan “Serenity”. Ini terdiri dari 3 tahap. Pada tahap awal (Phase 0), sebuah blockchain baru yang disebut Beacon Chain akan diluncurkan. Aturan-aturan Casper FFG akan mengendalikan mekanisme konsensus dari blockchain baru berbasis PoS ini.

Tidak seperti penambangan PoW, dimana para penambang menjalankan mesin khusus yang mahal untuk menghasilkan dan memvalidasi blok-blok dari transaksi, implementasi Casper akan menghapus proses penambangan dari Ethereum. Dengan kata lain, kemampuan voting dari masing-masing validator akan ditentukan oleh jumlah ETH yang mereka taruh.

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.

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.

Sebagai contoh, seseorang yang sudah mendeposit 64 ETH akan memiliki kemampuan voting dua kali lebih besar dibandingkan dengan orang lain yang hanya mendeposit sejumlah nilai staking minimum. Untuk menjadi validator blok pada tahap pertama Serenity, pengguna harus menaruh minimum 32 ether (ETH) - dideposit ke sebuah smart contract khusus yang didasarkan pada blockchain Ethereum sebelumnya (1.0). Kalau ini berjalan lancar, komite validator akan dilipih secara acak untuk mengajukan blok-blok baru dan nantinya mereka akan menerima upah blok atas kegiatan ini. Upah blok kemungkinan besar hanya terdiri dari biaya-biaya transaksi karena tidak ada subsidi blok. Bagaimanapun, perlu dicatat bahwa setiap implementasi PoS dapat menyajikan pendekatan yang berbeda, dengan model upah yang berbeda. Model Casper masih dalam pengembangan, dan banyak rincian tentang ini belum ditentukan.

Manfaat Casper

Salah satu manfaat Casper dalam membuat staking menjadi hal yang mungkin, adalah membantu Ethereum menjadi ramah lingkungan. Jika berbicara tentang sumber daya listrik dan komputasi, sistem berbasis PoW sangat merepotkan. Sebaliknya, model PoS jauh lebih gampang. Ketika nantinya sebuah model yang sepenuhnya PoS diimplementasikan ke dalam Ethereum, para penambang tidak lagi dibutuhkan untuk mengamankan blockchain, sehingga sumber daya yang diminta mejadi jauh lebih sedikit.

Manfaat potensial Casper lainnya adalah terkait keamanan. Pada intinya, Casper akan digunakan sebagai penyeleksi, bertugas untuk mengatur rantai pada blok-blok. Pada dasarnya, Casper akan bertindak sebagai akuntan pada buku besar (ledger) Ethereum 2.0. Jadi jika validator bertindak mencurigakan, mereka akan dihapus secepatnya dan dihukum. Hukuman terhadap pelanggaran aturan adalah stake (dalam ETH) milik validator tersebut, yang berarti pelanggaran jaringan sangat mahal. Namun, para developer masih mendiskusikan kemungkinan-kemungkinan 51% serangan.

Yang terakhir, beberapa orang berpendapat bahwa Casper akan menyumbangkan tingkat desentralisasi yang sangat besar kepada Ethereum. Sampai saat ini, mereka yang paling kuat di jaringan adalah mereka yang memiliki sumber daya untuk menjalankan operasi penambangan. Di masa depan, setiap orang yang dapat membeli sejumlah ether yang cukup akan mampu untuk membantu mengamankan blockchain.