# BLOCKCHAIN

## WEEK 6 CASPER POS

Nama : Raudhatul Rafiqah

NIM : 1103180225

### Pendahuluan

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). Casperbertanggung 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 danmengetahui 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 diterapkansebagai 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.

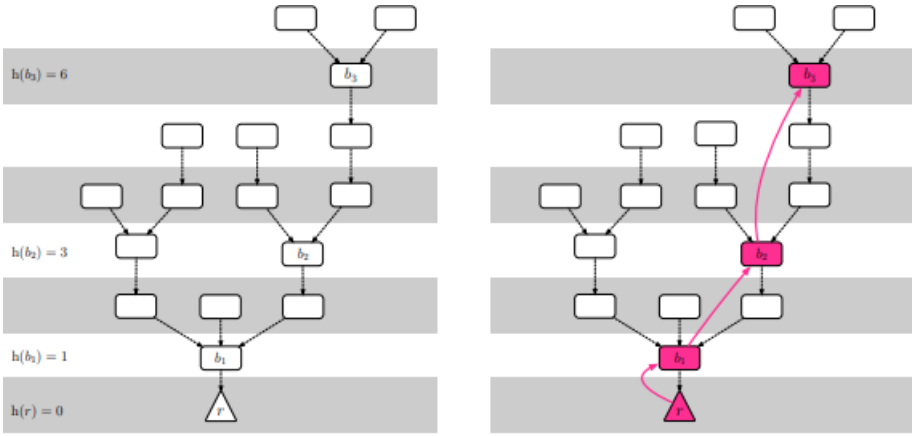
Dalam keadaan normal, diharapkan mekanisme proposal akan mengusulkan blok satu demi satu dalam daftar tertaut. Tetapi dalam kasus latensi jaringan atau serangan yang disengaja, mekanisme proposal terkadang akan menghasilkan banyak child dari parent yang sama. Tugas Casper adalah memilih satu child dari 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 $\nu$’s private key |




(b) The height function (c) The justified chain $r \to b_1 \to b_2 \to b_3$

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.

**Pembuktian Keamanan**

Kami membuktikan dua sifat dasar Casper:keamanan yang akuntabel dan keaktifan yang masuk akal. Keamanan yang akuntabel berarti bahwa dua pos pemeriksaan yang bertentangan tidak dapat diselesaikan keduanya kecuali ≥ 1/3 validator melanggar (1/3 dari total deposit hilang. Keaktifan yang masuk akal berarti bahwa, terlepas dari setiap peristiwa sebelumnya (misalnya, peristiwa tebasan, blok tertunda, serangan sensor, dll.), jika ≥ 2/3 validator mengikuti protocol. maka selalu mungkin untuk menyelesaikan pos pemeriksaan baru tanpa validator yang melanggar kondisi pemotongan.

**Aturan Casper’s Fork**

Casper lebih rumit daripada desain PoW standar. Dengan demikian, pilihan garpu harus disesuaikan. Aturan pilihan garpu yang dimodifikasi harus diikuti oleh semua pengguna, validator, dan bahkan mekanisme proposal blok yang mendasarinya. 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 (atau bahkan dibenarkan) tanpa beberapa validator secara altruistik mengorbankan deposit mereka. Untuk menghindari hal ini, kami memperkenalkan sebuah novel, benar dengan konstruksi, pilihan fork.

**Mengaktifkan Set Dynamic Validator**

Himpunan validator harus dapat berubah. Validator baru harus dapat bergabung, dan validator yang ada harus dapat keluar. Untuk mencapai ini, kami mendefinisika dinasti dari sebuah blok. Dinasti blok *b* adalah jumlah pos pemeriksaan akhir dalam rantai dari root ke induk blok *b*. Ketika calon validator pesan setoran termasuk dalam blok dengan dinasti *d*, maka validator akan bergabung dengan set validator di blok pertama dengan dinasti d+2. Kami memanggil d+2 validator ini memulai dinasti, DS(v). Untuk meninggalkan set validator, validator harus mengirim pesan "tarik". Jika pesan penarikan validator termasuk dalam blok dengan dinasti *d*, juga meninggalkan set validator di blok pertama dengan dinasti d+2; Kami memanggil d+2 milik sang validator akhir dinasti, DE(v). Jika pesan penarikan belum disertakan, maka DE(v) =∞. Setelah validator meninggalkan set validator, kunci publik validator selamanya dilarang untuk bergabung kembali dengan set validator. Ini menghilangkan kebutuhan untuk menangani beberapa dinasti awal/akhir untuk satu pengenal.

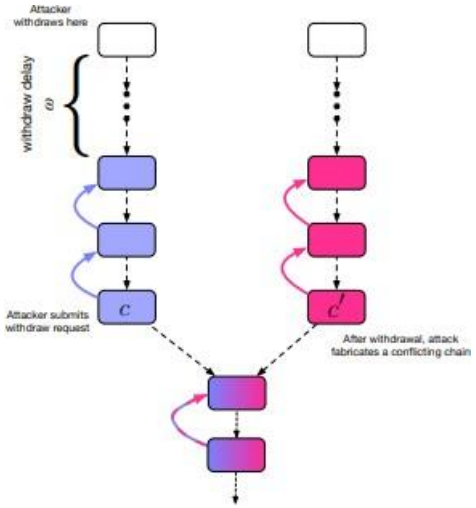
Pada awal dinasti akhir, deposit validator dikunci untuk jangka waktu yang lama, yang disebut penundaan penarikan (kira-kira “blok senilai empat bulan”), sebelum deposit ditarik. Jika, selama penundaan penarikan, validator melanggar perintah apa pun, setoran dipotong.

**Menghentikan Serangan**

Ada dua serangan terkenal terhadap sistem POS : : long range revisions dan catastrophic crashes.

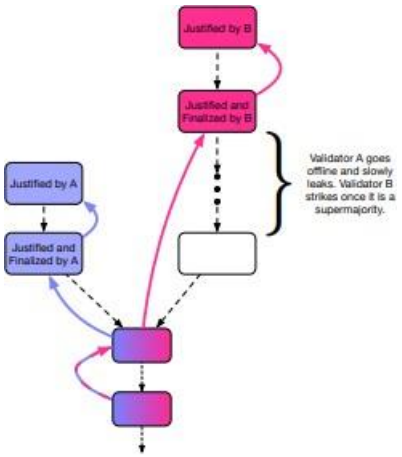
1. Long Range Revisions
   Dalam istilah sederhana, serangan jarak jauh dicegah oleh aturan pilihan garpu untuk tidak pernah mengembalikan blok yang telah diselesaikan, serta harapan bahwa setiap klien akan "masuk" dan mendapatkan tampilan lengkap terkini dari

frekuensi reguler (misalnya, sekali per 1-2 bulan). Garpu "revisi jarak jauh" yangmenyelesaikan blok yang lebih lama dari itu.




Kami juga dapat menghindari masalah batas waktu penyertaan bukti dengan secara informal menyatakan bahwa serangan akan berumur pendek, karena validator akan melihat rantai yang berjalan lama tanpa menyertakan pemotongan bukti sebagai serangan dan beralih ke cabang lain yang didukung oleh minoritas validator yang jujur. yang bukan bagian dari serangan sehingga menghentikan serangan dan menebas penyerang

2. Catastrophic Crashes
   Algoritma yang tepat untuk pulih dari berbagai serangan ini tetap menjadi masalah terbuka. Untuk saat ini, kami menganggap validator dapat mendeteksi perilaku yang jelas-jelas tidak sesuai (misalnya, tidak menyertakan bukti) dan secara manual membuat"garpu lunak minoritas". Garpu minoritas ini dapat dilihat sebagai blockchain dalam dirinya sendiri yang bersaing dengan rantai mayoritas di pasar, dan jika rantai mayoritas benar-benar dioperasikan oleh penyerang jahat yang berkolusi maka kita dapat berasumsi bahwa pasar akan menyukai garpu minoritas.




**Kesimpulan**

Kami mempresentasikan Casper, bukti baru dari sistem pasak yang berasal dari literatur toleransi kesalahan Bizantium. Casper termasuk: dua kondisi pemotongan, aturan pilihan garpu yang benar

berdasarkan konstruksi yang terinspirasi oleh [11], dan set validator dinamis. Akhirnya kami memperkenalkan ekstensi ke Casper (tidak mengembalikan pos pemeriksaan akhir dan kebocorantidak aktif) untuk bertahan melawan dua serangan umum.

Casper tetap tidak sempurna. Misal seperti wholly compromised block proposal mechanism akan mencegah Casper dari menyelesaikan blok baru. Casper adalah peningkatan keamanan ketat berbasis PoS untuk hampir semua rantai PoW. Masalah yang tidak sepenuhnya diselesaikan Casper, terutama yang terkait dengan serangan 51%, masih dapat diperbaiki menggunakan garpu lunak yangdiaktifkan pengguna.

Perkembangan di masa depan tidak diragukan lagi akan meningkatkan keamanan Casper dan mengurangi kebutuhan akan garpu lunak yang diaktifkan pengguna. Pekerjaan masa depan.Sistem Casper saat ini bdibangun di atas bukti mekanisme usulan blok kerja. Kami berharap untuk mengubah mekanisme proposal blok menjadi bukti kepemilikan. Kami ingin membuktikan keamanan yang dapat dipertanggungjawabkan dan keaktifan yang masuk akal bahkan ketika bobot set validator berubah dengan hadiah dan penalti. Masalah lain untuk pekerjaan di masa depan adalah spesifikasi formal dari aturan pilihan garpu dengan mempertimbangkan serangan umum pada proof of stake.
Kertas kerja masa depan akan menjelaskan dan menganalisis insentif keuangan dalam Casper dan konsekuensinya. Masalah ekonomi tertentu yang terkait dengan strategi otomatis untuk memblokir penyerang membuktikan batas atas rasio antara tingkat ketidaksepakatan antara klien yang berbedadan biaya yang dikeluarkan oleh penyerang.