Nama : Delatifa Putri Sugandi

NIM : 1103194080

Summary of Casper POS Papers

Casper adalah mekanisme konsensus parsial yang menggabungkan proof of stake algorithma research dan Byzantine fault tolerant consensus theory. Dalam sistem PoS, blockchain menambahkan dan menyetujui blok baru melalui proses di mana siapa pun yang memegang koin di dalam sistem dapat berpartisipasi, dan pengaruh yang dimiliki agen sebanding dengan jumlah koin yang dimilikinya. Ini adalah alternatif yang jauh lebih efisien untuk penambangan proof of work (PoW) dan memungkinkan blockchain untuk beroperasi tanpa biaya perangkat keras dan listrik penambangan yang tinggi.

Terdapat dua aliran pemikiran utama dalam desain PoS. *Chain-based proof of stake*, meniru bukti mekanisme kerja dan menampilkan rantai blok dan mensimulasikan penambangan dengan secara acak memberikan hak untuk membuat blok baru untuk pemangku kepentingan. Ini termasuk karya Peercoin, Blackcoin, dan Iddo Bentov. *Byzantine fault tolerant* (BFT) berdasarkan bukti pasak, didasarkan pada tubuh berusia tiga puluh tahun penelitian algoritma konsensus BFT seperti PBFT [6]. Algoritma BFT biasanya telah terbukti secara matematis properti; misalnya, seseorang biasanya dapat membuktikan secara matematis bahwa selama $> \frac{2}{3}$ peserta protokol adalah mengikuti protokol dengan jujur, maka, terlepas dari latensi jaringan, algoritma tidak dapat menyelesaikan konflik blok.

Casper memperkenalkan beberapa fitur baru yang belum tentu dapat digunakan pada algoritma BFT:

- Accountability, Jika validator melanggar aturan, kami dapat mendeteksi pelanggaran dan mengetahui validator mana melanggar aturan.
- Dynamic validators, cara aman untuk set validator untuk berubah seiring waktu.
- Defenses, pertahanan terhadap serangan revisi jarak jauh serta serangan di mana lebih dari $\frac{1}{3}$ 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 POW Chain.

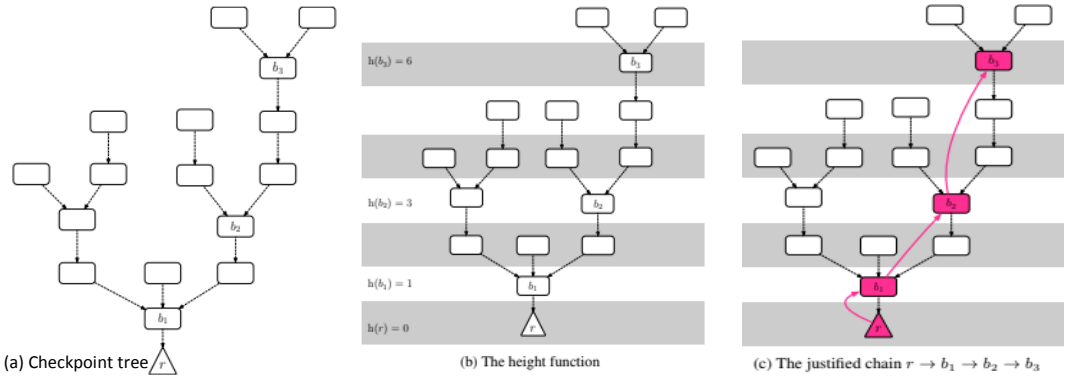
Casper Protokol

Pada ethereum, mekanisme proposal pada awalnya akan menjadi POW chain, yang membuat versi pertama casper sebagai sistem POW dan POS. Dalam versi casper yang sederhana, ada seperangkat validator dan mekanisme proposal yang tetap 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 dftar tertaut. Tetapi dalam kasus latensi jaringan atau serangan yang disengaja, mekanisme proposal terkadang akan menghasilka 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 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 rantai pos pemeriksaan yang membentang dari c (non-inklusif) ke akar di sepanjang tautan induk.

Validator dapat menyiarkan pesan suara yang berisi empat informasi, 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 (v, s, t, h(s), h(t)).

Notasi	Deskripsi
s	Hash dari setiap justified checkpoint (sumber)
t	Setiap checkpoint hash yang merupakan keturunan dari s ("target")
h(s)	the height of checkpoint s in the checkpoint tree
h(t)	The height of checkpoint t in the checkpoint tree
S	Signature of (s, t, h(s), h(t)) dari kunci privat validator



- 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.

Proving Safety and Plausible Liveness

Kami membuktikan dua sifat dasar Casper: Proving Safety and Plausible Liveness. 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. Plausible Liveness, Tautan supermayoritas selalu dapat ditambahkan untuk menghasilkan pos pemeriksaan baru yang diselesaikan, asalkan ada anak-anak yang memperpanjang rantai yang sudah selesai.

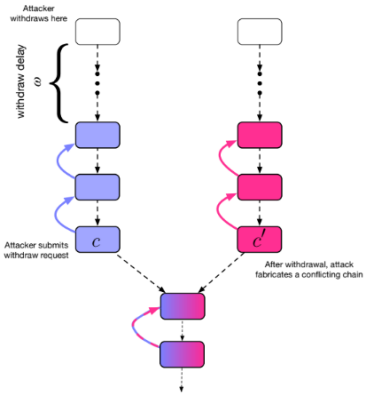
Aturan Casper's Fork

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.

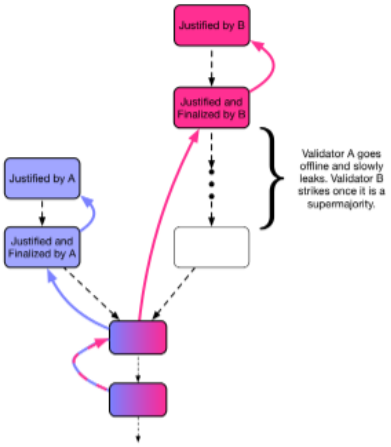
Stopping Attacks

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

- Long Range Revisions
  Setelah koalisi validator menarik simpanan mereka, jika koalisi itu memiliki lebih dari $\frac{2}{3}$ dari simpanan lama di masa lalu, mereka dapat menggunakan supermayoritas historis mereka untuk menyelesaikan pos pemeriksaan yang saling bertentangan tanpa takut disayat (karena uangnya sudah ditarik). Inilah yang disebut 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 rantai di beberapa frekuensi reguler (misalnya, sekali per 1-2 bulan). Garpu "revisi jarak jauh" yang menyelesaikan blok yang lebih lama dari itu.



- 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 kebocoran tidak 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 yang diaktifkan 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 berbeda dan biaya yang dikeluarkan oleh penyerang.