

Nama : Muhamad Fauzan Anshori

NIM : 1103190035

Kelas : TK-42-PIL

Summary Paper POS Casper

Casper merupakan sistem proof of stake yang dikembangkan dari literatur toleransi kesalahan bizantium dengan menggabungkan mekanisme algoritma penelitian konsensus proof of stake dan teori toleransi kesalahan bizantium consensus. Casper terdiri dari dua kondisi berupa aturan pilihan correct-by-construction fork dan set validator dinamis. Casper tetap tidak sempurna, pada kasus mekanisme proposal blok yang dikompromikan secara penuh dapat mencegah Casper untuk menyelesaikan blok-blok baru. Casper adalah peningkatan keamanan berbasis proof of stake untuk setiap chain proof of stake. Beberapa permasalahan yang tidak sepenuhnya Casper dapat atasi yang berkaitan dengan sekitar 51% serangan yang terjadi masih dapat dikoreksi dengan menggunakan soft fork yang dikendalikan pengguna. Tentunya di pengembangan kedepannya akan meningkatkan tingkat keamanan Casper dan mengurangi penggunaan soft fork yang dikendalikan pengguna.

Sistem Casper saat ini dibangun berdasarkan mekanisme block proposal proof of work yang kedepannya akan dikembangkan menjadi mekanisme block proposal proof of stake. Keamanan perlu dikembangkan menjadi keaktifan yang masuk akan dan keamanan yang dapat dipertanggung jawabkan bahkan ketika bobot set validator berubah dengan reward dan penalties. Selain itu permasalahan pada pengembangan kedepannya yaitu spesifikasi formal dari aturan pilihan fork dengan mempertimbangkan serangan umum pada proof of stake dan para pengembang perlu dapat menjelaskan dan menganalisis keuangan insentif dalam Casper dan konsekuensinya. Beberapa permasalahan tertentu seperti strategi otomatis untuk menghalangi penyerang membuktikan batas atas biaya yang dikeluarkan oleh penyerang dan antara rasio ketidak sepakatan yang terjadi diantara para klien.