Nama : Asep Irawan
NIM : 1103190112

Casper the Friendly Finality Gadget

A. Introduction

Dalam beberapa tahun terakhir dilakukan sebuah penelitian terhadap blockchain dengan algoritma dasar "Proof of stake" (PoS). Dalam sebuah PoS sistem, sebuah blockchain menambahkan dan menyetujui akan block baru melalui sebuah proses dimana siapapun yang memegang koin di dalam sistem dapat ikut menyertainya, dan pengaruh dari seorang agen tergantung akan proposi dari jumlah koin yang dipegangnya. Hal ini dpaat dikatakan lebih efisien dibandingkan dengan PowW atau *Mining* dan memungkinkan blockchain agar dapat beroperasi tanpa *mining* yang memerlukan *hardware* tingkat tinggi dan listrik yang besar.

B. The Casper Protocol

Di dalam sebuah ethereum, mekanisme yang diketahui akan memiliki permulaan dengan adanya PoW atau *Proof Of Work* chain, membuat versi pertama dari *Casper a hybrid PoW/PoS System.* Di masa depan versi dari mekanisme proposal PoW akan digantikan dengan suatu yang lebih efisien . Sebagai contohnya, kita dapat membayangkan akan proposal block diubah menjadi suatu PoS round-robin block rencana petanda.

Pada veri sederhananya Casper, kita mengasumsikan akan adanya jumlah tetap akan pengesah dan mekanisme proposal yang akan menghasilkan anak block dari block yang ada, dan akan menghasilkan *block tree* yang kana terus bertumbuh. Dan akar dari pohon terebut khasnya disebut dengan "genesis block".

Dalam situasi normal, kita mengharapkan mekanisme proposal akan menghasilkan block dan block di dalam sebuah daftar gabungan. Namun dalam situasi jaringan tersembunyi , mekanisme proposal akan menghasilkan banyak anak dalam satu orang tua. Tugas dari Casper adalah memilih satu anak dari setiap orang tua, dan akhirnya memilih satu buah rantai besambungan dari *block tree*.

Daripada mengatasi *block tree* sepenuhnya, dengan tujuan efisiensi Casper hanya menganggap *subtree* dari *chekspoints* membentuk *checkpoints tree*. *Genesis block* adalah sebuah *checkpoint*, dan setiap block yang memiliki tinggi dalam *block tree* memiliki jumlah yang tetap kelipatan dari 100 juga merupakan *checkpoint*.

Setiap pengesah memiliki deposit, ketika sebuah pengesah bergabung, dia mendepositkan sejumlah koin. Setelah bergabung, setiap pemasukan pengesah akan naik dan turun dengan kelebihan dan kekurangan. Keamanan *Proof of Stake* terbedakan dari ukuran pemasukan dan bukan dari jumlah pengesah, sehingga ketika dalam sebuah pencatatan tertulis "$\frac{2}{3}$ of validator", yang dimaksud adalah bagian dari berat pemasukannya.