Casper the Friendly Finality Gadget

Penelitian ini memperkenalkan Casper, bukti sistem finalitas berbasis pasak yang menutupi bukti yang ada dari kerja blockchain. Casper adalah mekanisme konsensus parsial yang menggabungkan bukti algoritma taruhan penelitian dan teori konsensus toleransi kesalahan Bizantium. Penelitian ini memperkenalkan sistem Penelitian ini, buktikan beberapa fitur yang diinginkan, dan menunjukkan pertahanan terhadap revisi jarak jauh dan kecelakaan besar. Lapisan luar Casper menyediakan hampir semua bukti rantai kerja dengan perlindungan tambahan terhadap blokir pengembalian.

Selama beberapa tahun terakhir telah ada banyak penelitian tentang blockchain berbasis “bukti kepemilikan” (PoS) algoritma konsensus. 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 (atau "taruhan") 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. Penelitian ini mempresentasikan Casper, bukti baru dari sistem pasak yang berasal dari literatur toleransi kesalahan Bizantium. Casper tetap tidak sempurna. Misalnya, mekanisme proposal blok yang sepenuhnya dikompromikan akan mencegah Casper dari menyelesaikan blok baru. Casper adalah peningkatan keamanan ketat berbasis PoS untuk hampir semua rantai PoW. Itu masalah yang tidak sepenuhnya diselesaikan Casper, terutama yang terkait dengan serangan 51%, masih dapat diperbaiki menggunakan garpu lunak yang diaktifkan pengguna. Sistem Casper saat ini dibangun berdasarkan bukti mekanisme proposal blok kerja. Kami berharap untuk mengubah mekanisme proposal blok menjadi bukti kepemilikan. Kami ingin membuktikan keamanan yang akuntabel dan masuk akal keaktifan bahkan ketika bobot set validator berubah dengan hadiah dan penalti.