

Proof of Stake Made Simple with Casper

Sebagian besar blockchain publik seperti Bitcoin dan mengandalkan bukti kerja untuk mencapai mufakat. Peserta, yang disebut penambang, bersaing untuk memecahkan teka-teki kriptografi untuk tambahkan blok baru dan terima hadiah. arena biaya modal awal yang tinggi dan skala ekonomi, penambang menjadi lebih besar dan sistem menjadi lebih terpusat. Akhirnya, satu-satunya cara bukti kerja mencegah penyerang melanggar konsensus adalah dengan menghabiskan banyak upaya komputasi pada perangkat utama blockchain: untuk bertahan melawan penyerang, jaringan harus mengeluarkan uang sebanyak penyerang. Proof of stake menggunakan seperangkat validator untuk mencapai konsensus pada rantai utama. Validator ini menyeter sejumlah cryptocurrency blockchain dan memberikan suara yang ditimbang berdasarkan saham mereka. Tidak perlu listrik dikonsumsi, dan sistem sepenuhnya terdesentralisasi karena tidak ada skala ekonomi. Itu keuntungan terbesar dari bukti kepemilikan seperti Casper adalah penyerang dapat diidentifikasi dan deposit mereka dapat segera dihancurkan. Sebagai bukti kerja, Anda tidak dapat menghancurkan perangkat keras penyerang setelah serangan. Tujuan penelitian ini adalah untuk menjelaskan secara detail apa itu proof of stake dan apa itu Casper. Penelitian ini menggambarkan protokol, peran validator, dan cara menyelesaikan blok. Penelitian ini kemudian membuktikan bahwa Casper menjamin keamanan yang akuntabel dan kehidupan yang masuk akal. Kontribusi utama Penelitian ini adalah merilis basis kode sederhana untuk bereksperimen dengan algoritma konsensus.

Penelitian ini telah merinci dan mudah-mudahan membuatnya lebih mudah untuk memahami bagaimana Casper berhasil mencapai konsensus menggunakan bukti kepemilikan. Implementasi Casper Penelitian ini memungkinkan siapa saja yang memiliki pengetahuan dasar tentang python untuk memahami detail protokol dan memvisualisasikan apa yang terjadi di dalam jaringan. Dengan plot blockchain seperti yang terlihat oleh masing-masing validator, kita dapat lebih memahami bagaimana latensi memengaruhi penyebaran blok dan jumlah pos pemeriksaan yang dibenarkan atau diselesaikan. Penelitian ini telah bereksperimen dengan berbagai parameter untuk Casper dan menemukan bahwa konsensus dapat dicapai bahkan dalam kondisi yang merugikan. Algoritme ini secara mengejutkan kuat untuk node yang terputus dan akan andal mencapai konsensus bahkan dengan latensi tinggi.