Summary Incentive On Casper

Kontribusi dari penelitian ini adalah sebagai berikut. Penelitian ini pertama-tama memberikan gambaran umum tentang protokol Casper FFG dan menjelaskan fungsi inti dari protokol tersebut. Untuk alasan yang berkaitan tentang liveness dan keselamatan, penelitian ini mengembangkan kerangka matematika untuk skema insentif, kondisi pemotongan, dan aturan pilihan fork. Hasil teoritis pertama penelitian ini adalah bahwa dengan skema hadiah yang diimplementasikan, Casper skema pemeriksaan α-live, untuk setiap $\alpha \in (0, 1]$, yaitu, validator online yang mengendalikan fraksi apa pun $\alpha \in (0, 1]$ dari saham pada akhirnya dapat menyelesaikan pos pemeriksaan. Pos pemeriksaan Casper Protokol memprioritaskan keselamatan dalam jangka pendek, tetapi liveness dalam jangka panjang, dan karenanya mencapai keseimbangan antara protokol yangbaik selalu memprioritaskan liveness (misalnya, rantai PoW yang mendasari) atau safety (misalnya, Tendermint).

Protokol Casper dimaksudkan untuk menawarkan jaminan finalitas yang lebih kuat daripada PoW di kedua hybrid PoW / PoS dan pada akhir dalam pengaturan PoS murni. Wawasan utama yang dimaksud adalah bahwa dalam PoS, node harus melakukan deposit untuk menjadi Validator dan pesan mereka yang akan muncul di blockchain, karena hal tersebut dapat dikaitkan dengan setoran. Jika pengguna terlibat dalam perilaku buruk yang jelas, misalnya, dengan memilih pos pemeriksaan yang saling bertentangan, maka mereka dapat dihukum dengan memotong simpanan yang mereka miliki. Isi gagasan yang setara di PoW adalah perangkat keras pada penambangan punya penambang musuh akan dihancurkan. Dalam pengaturan penelitian ini yang terburuk adalah kasus perilaku buruk dalam memilih pos pemeriksaan yang saling bertentangan. Jika ada dua dari tiga validator yang menempatkan taruhan mereka di belakang suara mereka untuk pos pemeriksaan, maka dua dari tiga validator lain menempatkan taruhannya di belakang pos pemeriksaan yang kontradiktif, maka itu harus menyiratkan bahwa hal tersebut adalah persimpangan, yaitu setidaknya satu dari tiga validator, telah mendukung kedua pos pemeriksaan yang saling bertentangan. Penelitian ini masih tidak dapat menjamin finalitas absolut – jika pos pemeriksaan yang saling bertentangan diselesaikan karena perilaku validator, maka rantai fork permanen atau beberapa mekanisme tata kelola off-chain digunakan untuk memutuskan mendukung satu cabang, dengan mengorbankan yang lainnya.

Dalam penelitian ini menganalisis kontrak Casper FFG yang dievaluasi pada testnet Ethereum khusus. Penelitian ini menjelaskan mekanisme inti dan menunjukkan bahwa skema insentifnya memastikan liveness sambil memberikan safety terhadap finalisasi sejarah yang saling bertentangan, yaitu, pos pemeriksaan. Sebagai protokol finalitas yang dapat dilapisi pada blockchain PoW dan PoS, hibrid Casper FFG dapat menarik bagi khalayak luas dalam ekosistem blockchain. Temuan kami tentang liveness, safety, insentifkompatibilitas, dan implementasi tetap sangat relevan untuk transisi Ethereum ke desain yang terpecah di manaFilosofi Casper FFG terbawa.