INCENTIVE ON CASPER

Seperti Bitcoin [31], [32], mekanisme proposal blok EthereumDidasarkan pada konsep Proof-of-Work (PoW). Dalam PoW, peserta jaringan menggunakan kekuatan komputasi untuk memenangkan hak.untuk menambahkan blok ke blockchain. Namun, konsumsi energi global yang mengkhawatirkan dari blockchain berbasis PoW telah membuatkonsep yang semakin kontroversial [22], [45], [65]. Salah satu alternatif utama untuk PoW adalah penambangan virtual atau Proof-of-Stake.(PoS) [1], [5], [46], [55]. Di PoS, hak untuk mengusulkan blok diperoleh dengan mengunci – atau menyetor – token di blockchain,yang tidak memiliki biaya energi yang melekat.

Sebagai bagian dari tujuan jangka panjangnya untuk beralih dari PoW ke PoS, Ethereum merancang protokol PoS penuh yang disebut Casper [15], [57],[58]. Untuk memastikan transisi yang mulus dengan dampak minimal pada penggunanya dan harga Ether (cryptocurrency asli Ethereum[41]), Ethereum menyebarkan dan menguji versi hibrida, Casper the Friendly Finality Gadget atau Casper FFG, sebagai kontrak cerdaspada testnet khusus [26], [53], [54].

Kontribusi dari makalah ini adalah sebagai berikut. Kami pertama-tama memberikan gambaran umum tentang protokol Casper FFG dan menjelaskannya fungsi inti. Untuk alasan tentang liveness dan keselamatan, kami mengembangkan kerangka matematika untuk skema insentif,kondisi pemotongan, dan aturan pilihan fork. Hasil teoritis pertama kami adalah bahwa dengan skema hadiah yang diimplementasikan, Casper'sSkema pemeriksaan α-live, untuk setiap $\alpha \in (0, 1]$, yaitu, validator online yang mengendalikan fraksi apa pun $\alpha \in (0, 1]$ dari saham akanakhirnya 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).

Agar tetap kompatibel dengan evolusi Ethereum menuju desain yang terpecah dan karenanya lebih terukur [13], [27], [58],spesifikasi Casper FFG terus diperbarui [11], [15]. Namun, takeaways utama dan temuan utama dari pengujianCasper FFG sebagai kontrak cerdas dalam pengaturan hibrida terbawa ke desain rantai PoS utama yang saat ini dikembangkan, yang disebutRantai Suar [10], [15], yang akan mengoordinasikan konsensus di antara beberapa rantai samping atau pecahan. Meskipun kami fokus untuk menggabungkan Casper FFG denganRantai PoW Ethereum, protokol dapat dilapisi di atas blockchain berbasis rantai – PoW atau PoS – dan mungkinoleh karena itu menjadi kepentingan yang lebih luas bagi komunitas blockchain.

Ethereum berfungsi sebagai komputer global yang operasinya direplikasi di seluruh jaringan peer-to-peer. Peserta dalamjaringan disebut node – mereka biasanya berinteraksi dengan seluruh jaringan melalui aplikasi perangkat lunak yang disebut klien. Siklien berinteraksi dengan blockchain Ethereum melalui transaksi. Ada tiga jenis transaksi utama: Token transfers, Contract creations, Contract calls. In hybrid Casper FFG, some nodes assume the role of validators. Nodes can become validators by locking/staking tokens on the PoW chain, thus creating a deposit. Peran utama validator adalah untuk memilih pos pemeriksaan [60]. Pos pemeriksaan adalah blok apa pun dengan bloknomor $i \cdot l$, di mana saya $\in \{0, 1, . .\}$

dan $l \in N$ menunjukkan panjang zaman: sebuah zaman didefinisikan sebagai urutan bersebelahan dariblok antara dua pos pemeriksaan, termasuk yang pertama tetapi tidak yang terakhir.

Protokol Casper dimaksudkan untuk menawarkan jaminan finalitas yang lebih kuat daripada PoW di kedua hybrid PoW / PoS dan akhirnya dalam pengaturan PoS murni. Wawasan utama adalah bahwa dalam PoS, node harus melakukan deposit untuk menjadiValidator, dan pesan mereka yang muncul di blockchain karena itu dapat dikaitkan dengan setoran tersebut. Jika pengguna terlibatdalam perilaku buruk yang jelas, misalnya, dengan memilih pos pemeriksaan yang saling bertentangan, maka mereka dapat dihukum dengan memotong simpanan mereka. Sigagasan yang setara di PoW adalah bahwa perangkat keras penambangan penambang musuh dihancurkan. Dalam pengaturan kami, yang terburukkasus perilaku buruk adalah memilih pos pemeriksaan yang saling bertentangan. Jika 2/3 validator menempatkan taruhan mereka di belakang suara merekauntuk pos pemeriksaan, maka jika 2/3 validator lain menempatkan taruhannya di belakang pos pemeriksaan yang kontradiktif, maka itu harusmenyiratkan bahwa persimpangan, yaitu setidaknya 1/3 dari validator, telah mendukung kedua pos pemeriksaan yang saling bertentangan. Kami masihtidak dapat menjamin finalitas absolut – jika pos pemeriksaan yang saling bertentangan diselesaikan karena perilaku validator, maka rantaifork permanen atau beberapa mekanisme tata kelola off-chain digunakan untuk memutuskan mendukung satu cabang, dengan mengorbankan yang lain.

Pada bagian ini kami menyelidiki bagaimana mekanisme insentif Casper mempengaruhi sifat fundamental dari konsensus keseluruhan.protokol, yaitu, pada mekanisme proposal blok yang mendasari dikombinasikan dengan skema pos pemeriksaan Casper FFG. Kami melanjutkan dengan menganalisis fundamental properti liveness dan safety di Bagian III-B dan III-C, masing-masing. Kami fokus pada jenis liveness dan safety berikutkesalahan untuk protokol pemeriksaan.

Liveness faults: pos pemeriksaan tidak diselesaikan selama satu atau lebih zaman berturut-turut.
Safety faults: dua atau lebih pos pemeriksaan yang saling bertentangan diselesaikan pada zaman yang sama atau berbeda. (Bagaimanapun, ini juga akanmengarah ke fork permanen, atau setidaknya satu simpul harus membalikkan pos pemeriksaan yang diselesaikan melalui reset manual.)

Akhirnya, kami mempelajari kompatibilitas insentif (yaitu, apakah validator diberi insentif untuk mengikuti protokol) di Bagian III-D.

Kami menyimpulkan bagian tentang liveness dengan diskusi tentang implikasi dariBeberapa asumsi teorema 4. Pertama, teorema menyatakan bahwa liveness dipulihkan dalam sejumlah zaman yang terbatas,tetapi durasi waktu zaman tersebut tergantung pada mekanisme proposal blok yang mendasarinya.

Setelah inisiasi dari fork, validator yang terus memberikan suara di cabang atas tahu bahwa mereka akan dapat mulai menyelesaikan terlebih dahulu, karena merekamembentuk mayoritas kapan saja. Validator di cabang yang lebih rendah juga akan dapat menyelesaikan pos pemeriksaan, namun ini akan ambil waktu lebih lama. Dalam hal ini, pos pemeriksaan yang saling bertentangan akan diselesaikan dan klien mengetahui salah satu dari pos pemeriksaan tidak akan mau mengembalikannya (di bawah aturan pilihan fork Casper). Dengan kata lain,

bahkan jika acara finalitas ganda memang terjadi, pengguna tidak dipaksa untuk menerima klaim yang memiliki lebih banyak saham di belakangnya; sebaliknya, pengguna akan dapat secara manual pilih fork mana yang harus diikuti, dan tentu saja dapat dengan mudah memilih "yang datang lebih dulu". Serangan yang sukses di Casper terlihat lebih seperti hard-fork daripada pengembalian, dan komunitas pengguna di sekitar aset on-chain cukup bebas untuk hanya menerapkan akal sehat untuk menentukan fork mana yang bukan serangan dan benar-benar mewakili hasil transaksi yang Awalnya disepakati sebagai finalisasi.

Saat ini, insentif untuk pengusul blok pada rantai PoW mirip dengan yang ada di Bitcoin, yangtelah ditunjukkan dalam [30], [38], [62] menjadi ekuilibrium Nash untuk mengikuti protokol bagi siapa saja yang mengendalikan kurang dari kira-kira13dari kekuatan pertambangan. Mekanisme checkpointing memiliki dampak kecil pada profitabilitas penambangan egois karenamemberlakukan batasan pada berapa banyak blok yang dapat dikembalikan dan kapan. Lagi pula, aturan pilihan fork baru lebih memilih blok yang memilikipos pemeriksaan tertinggi yang dibenarkan, yang berarti bahwa tidak mungkin bagi penambang egois untuk meyakinkan node lain untuk menjatuhkan blok yangmelampaui pos pemeriksaan terakhir yang dibenarkan. Validator adalah kelas node baru yang diperkenalkan oleh Casper FFG. Tindakan mereka yang paling penting adalah memilih, jadikami akan mempertimbangkan dampak pada simpanan mereka untuk menghasilkan suara yang sah atau tidak.

Dalam makalah ini, kami menganalisis kontrak Casper FFG yang dievaluasi pada testnet Ethereum khusus. Kami menjelaskannyamekanisme 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, hibrida 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.