Highway: Efficient Consensus with Flexible Finality

Abstrak

Kami mengusulkan Highway, protokol kesepakatan baru yang aman dan hidup dalam model BFT sinkron parsial klasik, sementara pada saat yang sama menawarkan peningkatan praktis atas solusi yang ada. Secara khusus, finalitas blok di **Highway** bukanlah biner tetapi dinyatakan oleh fraksi node yang perlu melanggar aturan protokol agar blok dapat dikembalikan. Selama periode partisipasi yang jujur, finalitas blok mungkin mencapai lebih dari 1/3 (seperti yang akan menjadi maksimum untuk protokol klasik), hingga genap 1 (kepastian lengkap).

pengantar

Sejak diperkenalkannya Bitcoin dan konsep database yang terdesentralisasi dan anti-rusak database – sebuah blockchain – sejumlah paradigma yang berbeda telah dikembangkan untuk merancang database tersebut. Baru-baru ini, gagasan untuk membangun sistem semacam itu berdasarkan PoS (Proof of Stake) telah mendapatkan popularitas yang signifikan. Sementara dalam mekanisme PoW (Proof of Work, seperti yang digunakan dalam Bitcoin) asli yang digunakan untuk mendorong partisipasi dan mengamankan sistem, kekuatan suara seorang peserta sebanding dengan jumlah kekuatan komputasi yang dimiliki, dalam PoS kekuatan suara proporsional.

Pertimbangan Praktis

- Panjang Putaran Dinamis
  Saat mendefinisikan versi dasar dari protokol kami, kami membagi waktu menjadi putaran yang panjangnya tetap.
- Era
  Karena protokol Highway dimaksudkan untuk membuat dan memelihara blockchain, setelah dijalankan (diinisialisasi) seharusnya berjalan selamanya, tanpa henti. Akibatnya, validator terpaksa menyimpan seluruh DAG, bahkan unit yang dibuat pada awal eksekusi protokol. Menghapus bagian "lama" dari DAG tidak aman, karena validator (kemungkinan tidak jujur) mungkin langsung mengutip di unit terbaru mereka beberapa unit yang sangat tua.
- Mengirim Lebih Sedikit Pengesahan
  Ingatlah bahwa strategi pengesahan awal yang kami perkenalkan di Bagian 3.6.1 sangat sederhana: setelah melihat ekivokasi, dukung setiap unit oleh validator non-equivocate. Meskipun memungkinkan argumen yang cukup sederhana bahwa keaktifan dipertahankan, ini juga memperkenalkan overhead yang tidak dapat diabaikan jika terjadi keragu-raguan terdeteksi di era tertentu.
- Konsensus Tertimbang
  Selama ini dianggap bahwa pendapat setiap validator sama pentingnya dalam proses mencapai mufakat. Dalam subbagian ini, menjelaskan modifikasi yang memungkinkan protokol Highway dijalankan dalam skenario di mana setiap validator memiliki bobot bilangan bulat terkait, sesuai dengan kekuatan votingnya – versi yang berguna misalnya saat membuat blockchain Proof of Stake.