Deep-Dive Analysis of Selfish and Stubborn Mining in Bitcoin and Ethereum

- Abstrak

Bitcoin dan Ethereum adalah dua cryptocurrency teratas berbasis blockchain baik dari kapitalisasi pasar cryptocurrency atau popularitas. Namun, mereka rentan terhadap penambangan yang egois dan penambangan yang keras kepala karena keduanya mengadopsi mekanisme konsensus Proof-of-Work.

- Pengantar

Bitcoin dan Ethereum sekarang menjadi dua cryptocurrency berbasis blockchain terbesar dan terpopuler di dunia, yang menggunakan mekanisme konsensus Proof-of-Work (PoW). Dalam sistem blockchain PoW, sejumlah besar penambang menambang blok dengan mencoba memecahkan teka-teki matematika dan penambang yang pertama kali memecahkan teka-teki memenangkan hak untuk menambahkan blok berikutnya ke blockchain.

Dalam sistem PoW, kesulitan menambang sebuah blok biasanya disesuaikan untuk mengurangi dampak dari berbagai kekuatan hash dan faktor lainnya pada waktu pembuatan blok reguler (10 menit di Bitcoin dan 13 detik di Ethereum). Blockchain PoW menghadapi banyak ancaman keamanan, seperti serangan pengeluaran ganda, serangan gerhana dan serangan penambangan egois.

Dalam pekerjaan kami, kami mengusulkan model Markov untuk mengevaluasi secara kuantitatif dampak penambangan yang egois dan keras kepala tidak hanya pada pendapatan penambangan penambang tetapi juga pada kinerja sistem dan keamanan di Bitcoin dan Ethereum. Kontribusi utama dari karya ini diringkas sebagai berikut.

1. Kami mengembangkan model Markov baru, yang dapat diterapkan untuk menyelidiki delapan jenis penambangan berbahaya di Bitcoin dan Ethereum. Penambang jahat dapat menggunakan strategi penambangan yang jujur atau strategi penambangan yang berbahaya, yang merupakan strategi penambangan yang egois atau salah satu dari tujuh jenis strategi penambangan yang keras kepala. Sejauh pengetahuan kami, model kami adalah model pertama yang dapat menganalisis delapan jenis strategi penambangan berbahaya di Bitcoin dan Ethereum.
2. Kami memperoleh formula untuk menghitung pendapatan relatif untuk penambang jujur dan penambang jahat di Bitcoin dan Ethereum, masing-masing. Pendapatan penambangan Ethereum terdiri dari tiga jenis hadiah, tetapi pendapatan penambangan Bitcoin hanya terdiri dari satu jenis hadiah. Analisis pendapatan relatif memiliki tiga manfaat utama:
    a. Memberikan hubungan kuantitatif antara strategi penambangan yang relatif-pendapatan-optimal untuk penambang jahat dan dua fitur penambang, termasuk rasio penambang jujur yang menambang di cabang pribadi ketika dua blok diterbitkan secara bersamaan dan kekuatan hash penambang jahat di Bitcoin dan Ethereum, masing-masing.
    b. Berikan panduan kepada penambang yang jujur tentang pengaturan ambang batas kekuatan hash node penambangan untuk mencegah penambang jahat mengambil untung dengan penambangan yang egois dan keras kepala.

c. Bantu penambang yang jujur merancang mekanisme hadiah untuk menolak penambangan berbahaya.

3. Kami memperoleh rumus untuk menghitung kinerja sistem dan metrik keamanan, termasuk rasio blok yang sudah usang, transaksi per detik, dan ketahanan terhadap serangan pengeluaran ganda. Dengan metrik ini, kami dapat mengevaluasi dampak penambangan berbahaya pada sistem blockchain dan membantu penambang jujur mendeteksi apakah ada penambang jahat dalam sistem. Penyelidikan kami terhadap literatur publik menunjukkan bahwa kami adalah yang pertama mengevaluasi dampak penambangan yang membandel pada kinerja dan keamanan Bitcoin dan Ethereum.

- Kesimpulan dan pekerjaan masa depan

  Secara kuantitatif menganalisis beberapa jenis strategi penambangan berbahaya dalam sistem Bitcoin dan Ethereum dengan membangun model Markov. Di Bitcoin, penambang bisa mendapatkan satu jenis hadiah penambangan (yaitu, hadiah blok statis), tetapi penambang di Ethereum bisa mendapatkan tiga jenis hadiah penambangan (yaitu, hadiah blok statis, hadiah paman, dan hadiah keponakan).

  Salah satu arah kerja kami di masa depan adalah menerapkan model dan formula kami untuk mempelajari mata uang kripto yang bercabang dari Bitcoin dan Ethereum. Kami berencana untuk memperluas model dan formula kami ke jaringan yang tidak sempurna dan mengevaluasi dampak penundaan propagasi blok pada penambangan berbahaya. Analisis kuantitatif dari serangan-serangan itu juga merupakan arah pekerjaan kami di masa depan.