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

Mengembangkan model Markov baru, yang dapat mempelajari penambangan egois dan tujuh jenis penambangan keras kepala di Bitcoin dan Ethereum. Hasil analisis kuantitatif dapat membantu penambang jujur dalam mendeteksi apakah ada penambang jahat dalam sistem dan menetapkan ambang batas hash power node penambangan di untuk mencegah penambang jahat menghasilkan keuntungan melalui penambangan yang egois dan keras kepala. kemudian mendapatkan hadiah, beberapa penambang dapat membentuk kumpulan penambangan penambangan blok biasanya disesuaikan untuk mengurangi dampak dari kekuatan hash yang bervariasi 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 pembelanjaan ganda , serangan gerhana dan serangan penambangan egois Ethereum Classic menderita penambangan egois di Makalah ini berfokus pada dua jenis penambangan berbahaya, yaitu penambangan egois dan keras kepala yang dirinci tipe sebelumnya selalu mengadopsi strategi penambangan yang jujur untuk bercabang dan menerbitkan blok segera setelah menjadi simpul, yang merupakan penambang individu atau kumpulan penambangan). contoh untuk menggambarkan rantai blok ketika MP menggunakan strategi penambangan yang berbahaya dan jujur di Bitcoin, masing-masing. strategi jahat, cabang dengan tiga blok semuanya diproduksi oleh Blok-blok yang dihasilkan oleh rantai utama yang jujur), yang berarti bahwa kekuatan hash dari strategi penambangan penambang yang jujur Penambangan yang jujur (100%, berlawanan dengan 60% untuk penambangan yang jujur) dengan menggunakan Namun , strategi penambangan yang berbahaya tidak selalu membawa lebih banyak pendapatan relatif ke MP daripada strategi penambangan yang jujur mendapatkan pendapatan yang lebih rendah daripada strategi penambangan yang jujur. hanya mempelajari pendapatan relatif dari penambang jahat atau mengabaikan dampak penambangan berbahaya pada blockchain penambangan yang egois dan keras kepala tidak hanya pada pendapatan penambangan untuk menyelidiki delapan jenis penambangan berbahaya di Bitcoin Penambang berbahaya 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. 2.

Kami memperoleh formula untuk menghitung pendapatan relatif untuk penambang jujur dan penambang jahat di Bitcoin dan pendapatan penambangan Ethereum terdiri dari tiga jenis hadiah, tetapi strategi penambangan optimal penambangan Bitcoin untuk penambang jahat dan dua penambangan di cabang pribadi ketika dua blok diterbitkan secara bersamaan dan kekuatan hash penambang jahat di Bitcoin dan Ethereum, masing-masing. pedoman untuk penambang yang jujur tentang pengaturan ambang batas kekuatan hash node penambangan untuk mencegah penambang jahat mengambil untung dengan penambangan yang egois dan keras kepala. rasio blok, transaksi per detik, dan resistensi dapat mengevaluasi dampak penambangan berbahaya pada sistem blockchain dan membantu penambang yang jujur mendeteksi bahwa kami adalah yang pertama mengevaluasi dampak penambangan keras kepala pada kinerja dan keamanan Bitcoin dan Ethereum. model Markov dimensi yang dapat menggambarkan penambangan egois penambangan egois pada Bitcoin dan kinerja sistem Ethereum penambangan berbahaya pada keamanan blockchain, kami mempertimbangkan skenario yang dianggap penambangan egois. Jumlah rata-rata blok paman yang dibuat dalam a Jumlah blok reguler s yang dibuat dalam jumlah rata-rata blok reguler yang dibuat oleh sistem dengan serangan pengeluaran ganda selain penambang jujur Grup 1 (G1) terdiri dari penambang jujur dan MP, dan menunjukkan probabilitas blok yang dihasilkan oleh G1 Sebelum presentasi perilaku penambang jujur dan MP, Di Ethereum, blok paman hanya dapat direferensikan oleh satu Perilaku penambang jujur penambang mengendalikan sebagian besar kekuatan hash di blockchain Penambang jujur mengadopsi strategi penambangan jujur:

Penambang yang jujur selalu menambang blok di rantai terpanjang yang blok diproduksi; dan di Ethereum, penambang jujur merujuk jika ada dua blok (dilambangkan sebagai BA dan BB) yang diterbitkan hampir bersamaan, sebagian penambang jujur menerima BA terlebih dahulu dan menambangnya, dan sisanya menambang blok di blok MP dapat mengadopsi strategi penambangan yang jujur atau strategi penambangan egois yang berbahaya yang diberikan di 3 Contoh bahwa menggunakan strategi penambangan yang keras kepala lebih baik daripada penggunaan strategi penambangan yang egois.