Garry Abel Diaraja H

1103190147

TK-42-pil

Dirty Pool Full-fledged Simulation for Selfish Mining in Bitcoin

Selfish Mining dan Eclipse Attack

Selfish mining tidak optimal untuk ruang parameter yang besar. Ada strategi yang dapat dijadikan alternatif, yaitu stubborn mining yang menggeneralisasi dan mengungguli serangan selfish mining. Untuk sebagian besar ruang parameter yang menarik, strategi baru kami secara signifikan meningkatkan pendapatan penyerang. Bergantung pada parameter lingkungan, strategi penambangan yang keras kepala dapat mengalahkan penambangan yang egois hingga 25% (bahkan tanpa memanfaatkan serangan tingkat jaringan apa pun). Bergantung pada parameternya, dan pada harga selama penulisan, ini dapat menghasilkan keuntungan tambahan $73K per hari dibandingkan dengan penambang yang egois. Kami menunjukkan bahwa dalam beberapa kasus, strategi yang keras kepala dapat menghasilkan 13%keuntungan dibandingkan dengan non-trail-stubborn. Selfish miners juga dapat mengeksploitasi serangan tingkat jaringan untuk lebih meningkatkan keuntungannya. Secara khusus, dengan kesukesesan eclipse attack, penyerang mengisolasi korban dari rekan-rekannya yang lain di tingkat jaringan, dengan mengontrol koneksi masuk dan keluarnya. Bergantung pada parameternya, strategi ini terkadang dapat menghasilkan 30% keuntungan dibandingkan dengan penggunaan naif dari node yang hilang. Kami juga menunjukkan bahwa secara mengejutkan, dalam beberapa rentang parameter, strategi terbaik penyerang sebenarnya membantu node eclipse, maka korban mungkin memiliki sedikit insentif untuk mencegah, mendeteksi, atau bereaksi terhadap serangan tersebut. Tidak ada strategi tunggal yang merupakan strategi optimal “satu ukuran untuk semua”. Sebaliknya, penyerang harus memilih strateginya berdasarkan parameter yang diperkirakan termasuk jumlah daya komputasi yang dapat digunakannya, fraksi jaringan yang berpotensi dikalahkan, dan fraksi jaringan tersisa yang dapat dipengaruhinya.

Stubborn Mining

Setelah memperkenalkan penambangan egois, beberapa penelitian lebih lanjut menunjukkan bahwa strategi penambangan egois yang lebih umum bisa lebih menguntungkan.

misalnya Serangan Bitcoin Teoretis dengan Kurang dari Setengah Kekuatan Komputasi (draft)

dan khususnya Penambangan Keras Kepala: Menggeneralisasi Penambangan Egois dan Menggabungkan dengan Serangan Eclipse

memberikan generalisasi komprehensif penambangan egois dan juga memperkenalkan nama yang berbeda untuk setiap variasinya:

- Lead Stubborn Mining Strategy

Penambang Keras Kepala menunggu sampai penambang jujur mengejarnya untuk menyiarkan semua blok rahasianya sebagai lawan dari penambang egois yang tidak mengambil risiko ditangkap oleh penambang jujur dan menyiarkan bloknya jika kemajuannya menyusut menjadi satu blok

- J-Trail Stubborn Mining Strategy
  trail Stubborn Mining merupakan perbaikan dari Lead Stubborn Mining. Ketika jejak rantai pribadi Penambang Keras berada di belakang rantai publik, mereka mungkin memutuskan untuk terus menambangnya, dengan harapan bisa menyusul. Kami mempertimbangkan keluarga strategi keras kepala jejak yang diparameterisasi oleh ambang j, sehingga penambang keras kepala aj trailmenerima blockchain publik hanya ketika rantai pribadi mereka berada di belakang rantai publik dengan j + 1 blok). Jadi menurut definisi, penambangan keras kepala 1-trail sama dengan penambangan keras kepala timah. Di sini kami hanya mempelajari penambangan keras kepala 2-trail, 3-trail dan 4-trail karena strategi keras kepala trail lainnya dapat dengan mudah didominasi oleh strategi lain.
- Equal Fork Stubborn Mining Strategy
  Penambang Keras Garpu Setara menunggu blockchain resmi untuk mengatasi garpu rahasianya dengan satu blok. Dia hanya menyerah ketika panjang blockchain resmi sama dengan panjang garpu rahasianya ditambah satu.