Sutan Faiz Rasyid
1103183160

TK-42-PIL

Week 5

Blockchain

Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack

Kami memperluas ruang strategi penambangan untuk termasuk strategi "stubborn" baru yang, untuk sejumlah besar parameter, dapatkan penambang lebih banyak pendapatan. Akibatnya, kita menunjukkan bahwa serangan penambangan egois tidak (secara umum) optimal. Selanjutnya, kami menunjukkan bagaimana penambang dapat lebih meningkatkan keuntungannya dengan membuat serangan penambangan yang tidak sepele dengan tingkat jaringan serangan gerhana. Kami menunjukkan, secara mengejutkan, bahwa mengingat penyerang strategi terbaik, dalam beberapa kasus korban serangan gerhana dapatbenar-benar mendapat manfaat dari gerhana!

Cryptocurrency terdesentralisasi seperti Bitcoin, strategi penambangan membentuk ruang yang rumit, dan ini ruang dapat diperluas lebih lanjut dengan menggabungkan serangan penambangan dan serangan tingkat jaringan dengan cara yang tidak mudah. Pekerjaan kita membuka tantangan berikut:

1) karakterisasi yang lebih lengkap dari strategi kompleks ruang dan metode analitis untuk menurunkan dan membuktikan strategi optimal yang diberikan pilihan parameter apa pun; dan

2) merancang protokol konsensus aman yang dapat dibuktikan yang keamanan secara formal didasarkan pada asumsi rasionalitas daripada mayoritas yang jujur. Dengan membuka kompleksitas ruang strategi, pekerjaan kami menunjukkan bahwa untuk mencapai tujuan ini mungkin menantang terutama jika formal model juga perlu menangkap propagasi tingkat jaringan yang realistis.