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

Penambang egois adalah serangan terkenal di mana penambang egois, di bawah kondisi tertentu, dapat memperoleh bagian hadiah yang tidak proporsional menyimpang dari perilaku jujur. Dalam makalah ini, penelitian ini memperluas ruang strategi penambangan untuk termasuk strategi "keras kepala" baru yang, untuk sejumlah besar parameter, dapatkan penambang lebih banyak pendapatan. Akibatnya, kita menunjukkan bahwa serangan penambangan egois tidak (secara umum) optimal. Selanjutnya, penelitian ini menunjukkan bagaimana penambang dapat lebih meningkatkan keuntungannya dengan membuat serangan penambangan yang tidak sepele dengan tingkat jaringan *Eclipse Attack*. Penelitian ini menunjukkan, secara mengejutkan, bahwa mengingat penyerang strategi terbaik, dalam beberapa kasus korban *Eclipse Attack* dapat benar-benar mendapat manfaat dari gerhana.

Penelitian ini menunjukkan bahwa dalam 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 sepele. Dari perkerjaan tersebut membuka tantangan lain yaitu, karakterisasi yang lebih lengkap dari strategi kompleks ruang dan metode analitis untuk menurunkan dan membuktikan strategi optimal yang diberikan pilihan parameter apa pun. Serta tantangan lainnya adalah 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 penelitian ini menunjukkan bahwa untuk mencapai tujuan ini mungkin menantang terutama jika formal model juga perlu menangkap propagasi tingkat jaringan yang realistis.