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

makalah ini, 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.

2. ForkDec: Accurate Detection for Selfish Mining Attacks

Bitcoin pada dasarnya adalah buku besar publik yang terdesentralisasi dan terdistribusi, yang memungkinkan siapa saja untuk berpartisipasi dalam menerbitkan transaksi. Transaksi akan dikumpulkan oleh peserta (disebut penambang) di jaringan dan kemudian ditambahkan ke buku besar melalui protokol konsensus. Mekanisme insentif adalah inti dari fungsionalitas Bitcoin, yang menjamin keamanan dan keaktifan Bitcoin dengan mendorong sejumlah besar penambang jujur untuk berpartisipasi dalam proses consensus. Menerapkan ForkDec ke set tes untuk evaluasi. Hasil evaluasi menunjukkan bahwa ForkDec dapat mencapai akurasi 99,03% untuk mendeteksi penambangan egois di Bitcoin. ForkDec hanya bisa mendeteksi adanya serangan tetapi tidak bisa mengidentifikasi miner yang melancarkan serangan.

3. ON PROFITABILITY OF SELFISH MINING

Pada paper on profitablity of selfish mining membahas tentang selfish mining strategy dalam Bitcoin network dan mengevaluasi dengan benar biaya serangan dan profitabilitasnya Yang diharapkan durasi serangan telah diabaikan dalam literatur tetapi sangat penting. Dalam paper ini membuktikan bahwa strategi tersebut hanya dapat menguntungkan setelah penyesuaian kesulitan. Karena itu serangan terhadap algoritma penyesuaian kesulitan. Serta dalam paper ini mengusulkan perbaikan protokol Bitcoin mebuatnya kebal terhadap serangan penambangan yang egois. Selfish Mining merupakan strategi penambang menyimpangan yang dijelaskan dalam operator penambangan besar menahan blok

yang ditambang dan melepaskannya dengan strategi tepat waktu untuk membatalkan jumlah maksimum blok yang ditambang oleh sisa jaringan.

4. Majority is not Enough: Bitcoin Mining is Vulnerable

Pada paper ini menunjukkan bahwa protokol Bitcoin tidak kompatibel dengan insentif. paper menghadirkan serangan penambang yang berkolusi memperoleh pendapatan yang lebih besar daripada bagian mereka yang adil/jujur. Ide kunci di balik strategi serangan ini disebut Selfish Mining, selfish mining adalah kolam untuk menjaga blok yang ditemukan tetap pribadi, sehingga dengan sengaja memotong rantai publik. Ketika cabang publik mendekati cabang kolam pribadi, para penambang egois mengungkapkan blok dari rantai pribadi mereka ke publik. Paper ini mengusulkan perubahan sederhana yang kompatibel dengan protokol Bitcoin untuk mengatasi masalah ini dan meningkatkan ambang batas ketika seorang penambang belajar cabang yang bersaing dengan panjang yang sama, itu harus menyebarkan semuanya, dan pilih yang mana untuk ditambang secara seragam secara acak.

5. Blockchain Mining with Multiple Selfish Miners

Keamanan blockchain seperti Bitcoin didirikan oleh rantai teka-teki Hash kriptografi, yang ditangani oleh jaringan besar peserta pseudonim yang disebut penambang. Memecahkan teka-teki Hash dianggap sebagai cara untuk menghasilkan Proof-of-Work (PoW) untuk mencapai consensus global. PoW Bitcoin menuntut perhitungan intensif, sehingga mengkonsumsi banyak energi. Penyesuaian kesulitan seperti bitcoin adalah Inti dari penambangan Bitcoin adalah untuk memecahkan teka-teki kriptografi. Header blok terutama mencakup Hash dari blok sebelumnya, Hash root Merkle transaksi, waktu awal menghitung hash header, nBits yang digunakan untuk menghasilkan kesulitan target dan NONCE.

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

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. Pekerjaan kita membuka tantangan berikut:

a. karakterisasi yang lebih lengkap dari strategi komplek ruang dan metode analitis untuk menurunkan dan membuktikan strategi optimal yang diberikan pilihan parameter apa pun; dan
b. merancang protokol konsensus aman yang dapat dibuktikan yang keamanan secara formal didasarkan pada asumsi rasionalita daripada mayoritas yang jujur. Dengan membuka kompleksit ruang strategi, pekerjaan kami menunjukkan bahwa untuk mencapa tujuan ini mungkin menantang terutama jika formal model juga perlu menangkap prop- tingkat jaringan yang realisti agasi.