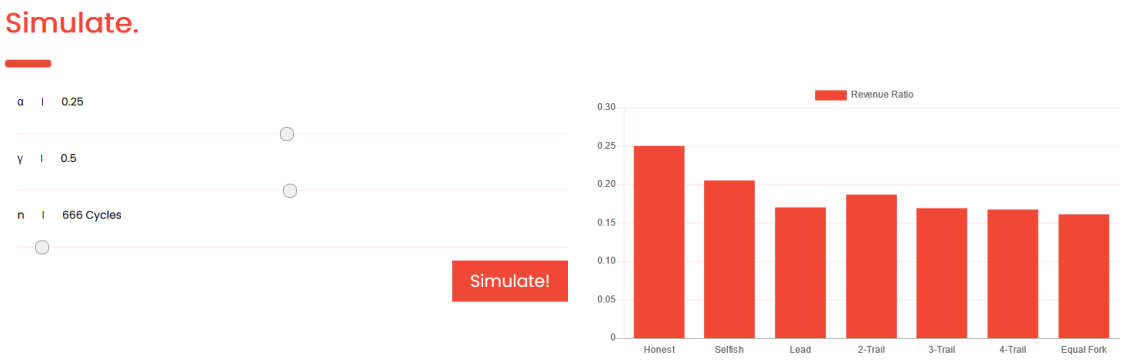
Praktek :



Summery :

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.

Pada paper ini menjelaskan selfish mining attack mulai dari validasi dan blok nya tidak di broadcast kemudian melajutkan penambang secara diam-diam pada atas blok ini. Selanjutnya dia melanjutkan proses berikut :

1. Jika selfish miner hanya sama 1 blok dan honest miner menemukan blok kemudian selfish mining segera menyebarkan blok dia tealh menambang secara diam-diam.
2. Jika selfish miner adalah 2 blok dan honest miner menemukan satu blok, lalu selfish miner segera menyiarkan dua blok yang dia miliki ditambang secara rahasia. Kemudian, seluruh jaringan berganti
3. Jika selfish miner lebih besar dari 2 maka selfish miner melepaskan blok segra setelah honest miner menemukannya.
4. Dalam kasus lain, selfish miner terus menambang secara diam diam.

Selfish miner merupakan trik yang memperlambat jaringan dan mengurangi penambang kesulitan. Serangan itu mengrangi profitablitas penambang yang jujur dan salah satu dari selfish miner sebelum penyesuaian kesulitan. Selfish miner hanya menjadi menguntungkan setelah menurunkan tingkat kesulitan. Cara lain untuk mencapainya adalah dengan memundurkan dari jaringan dan mulai menambang cryptocurrency lain dengan hashing uang sama fingsi.

Ther origin of problem : Pada dasarnya, Serangan itu memanfaatkan hukum penyesuaian kesulitan.

Formula penyesuaian kesulitan baru. Untuk mengurangi serangan ini, idenya adalaha untuk memasukan jumalh blok dalam rumus penyesuaian kesulitan.

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. Setiap penambang bersaing untuk "permainan" ini, dan dihargai oleh mata uang crypto (yaitu bitcoin) jika dia adalah penambang pertama yang diakui.

Prosedur penambangan terdiri dari dua kasus sebagai berikut.

1. (Kasus penambangan rantai publik) Henry selalu menambang setelah rantai publik. Alice atau Bob juga menambang di rantai publik jika lebih panjang dari rantai pribadinya.
2. (Kasus penambangan rantai swasta) Alice (resp. Bob) terus menambang rantai pribadinya (resp. nya) jika dia (resp. dia) menemukan blok baru dan rantai pribadi sekarang lebih panjang than rantai publik. Prosedur pelepasan lebih rumit daripada prosedur penambangan. Henry menyiarkan blok yang ditambang segera setelah ditemukan, sementara Alice dan Bob akan memutuskan apakah akan melepaskan blok yang ditambang tergantung pada panjang rantai publik.
3. (Kasus hangus) Alice (resp. Bob) meninggalkan rantai pribadinya (resp. nya) dan sesuai dengan penambangan setelah rantai publik jika yang terakhir lebih panjang. Henry juga meninggalkan rantai publiknya jika Alice atau Bob menerbitkan rantai yang lebih panjang.
4. (Kasus pelepasan yang menghindari risiko) Alice (resp. Bob) melepaskan bloknya (resp. nya) yang ditambang secara pribadi ke publik karena takut kehilangan jika blok baru ditambang oleh yang lain dan keuntungan utama dari rantai pribadinya tidak lebih dari dua blok.
5. (Kasus reaksi berantai) Ketika Alice (resp. Bob) melepaskan bloknya (resp. nya) ke rantai publik dan memperbarui panjangnya, pelepasan blok pribadi Bob (resp. Alice) dipicu segera

Definisi dasar dari selfish mining sendiri terdapat dua definisi:

Definisi pertama(pendapatan realtif) Biarkan Ra, Rb dan Rh menjadi jumlah yang diharapkan dari blok yang valid yang ditambang oleh Alice, Bob dan Henry di putaran penambangan, masing masing. Pendapatan relatif seorang penambang, Rˆi, dinyatakan sebagai:

$$\hat{R}_i = \frac{R_i}{R_a + R_b + R_h}, \qquad i \in \{a, b, h\}$$

Perlu ditekankan bahwa blok yang valid adalah blok yang dikonfirmasi dalam rantai longest. Profitabilitas penambangan egois tidak mengacu pada surplus bahwa hadiah blok mengurangi biaya perhitungan kriptografi. Bahkan, ini adalah ukuran kontras dengan penambangan jujur yang membutuhkan indeks objektif.

Definisi Kedua (profitability) Penambangan egois atau strategis yang dilakukan oleh Alice (resp. Bob) dianggap menguntungkan jika pendapatan relatif lebih tinggi dari kekuatan Hash yang dinormalisasi, yaitu Rˆa

> α 1 (resp. Rˆb > α 2).

Penyesuaian kesulitan seperti bitcoin adalah Inti dari penambangan Bitcoin adalah untuk memecahkan teka-teki kriptografi.

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

Secara kuantitatif menganalisis beberapa jenis strategi penambangan berbahaya dalam sistem Bitcoin dan Ethereum dengan membangun model Markov. Di Bitcoin, penambang bisa mendapatkan satu jenis hadiah penambangan (yaitu, hadiah blok statis), tetapi penambang di Ethereum bisa mendapatkan tiga jenis hadiah penambangan (yaitu, hadiah blok statis, hadiah paman, dan hadiah keponakan).

Salah satu arah kerja kami di masa depan adalah menerapkan model dan formula kami untuk mempelajari mata uang kripto yang bercabang dari Bitcoin dan Ethereum. Kami berencana untuk memperluas model dan formula kami ke jaringan yang tidak sempurna dan mengevaluasi dampak penundaan propagasi blok pada penambangan berbahaya. Analisis kuantitatif dari serangan-serangan itu juga merupakan arah pekerjaan kami di masa depan.

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.

Serangkaian penelitian terhadap perilaku penambangan yang egois, karya-karya ini memiliki keterbatasan tertentu: baik protokol yang ada perlu dimodifikasi atau efek deteksi untuk serangan tidak memuaskan. Kami mengusulkan ForkDec, sistem akurasi tinggi untuk deteksi penambangan egois berdasarkan jaringan saraf yang sepenuhnya terhubung, untuk tujuan mencegah penyerang egois secara efektif. Jaringan saraf berisi total 100 neuron (10 lapisan tersembunyi dan 10 neuron per lapisan), dipelajari pada set pelatihan yang berisi sekitar 200.000 sampel.

Sistem ini didasarkan pada model klasifikasi pembelajaran mesin untuk mewujudkan deteksi serangan yang cerdas. Untuk memastikan bahwa ForkDec memiliki akurasi deteksi yang tinggi, kami membuat kumpulan data yang berisi sekitar 200.000 sampel garpu Bitcoin untuk pelatihan model.

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.

Dalam pekerjaan di masa mendatang, kami akan menganalisis lebih lanjut strategi penyerang dan meningkatkan ForkDec untuk menemukan penyerang secara akurat.

Majority is not Enough: Bitcoin Mining is Vulnerable

Strategi ini membuat penambang jujur yang mengikuti protokol Bitcoin menjadi sia-sia sumber daya untuk menambang cryptopuzzles yang akhirnya tidak berguna. Analisis paper ini menunjukkan bahwa, sementara pihak yang jujur dan egois menyianyiakan beberapa sumber daya, penambang yang jujur membuang lebih banyak secara proporsional dan hadiah kumpulan penambang egois melebihi bagiannya dari kekuatan penambangan jaringan, hal tersebut memberi penambang egois keuntungan kompetitif dan memberi insentif kepada penambang rasional untuk bergabung dengan kumpulan penambangan yang egois.

Serangan ini dapat memiliki konsekuensi yang signifikan untuk Bitcoin:

1. Penambang rasional akan lebih suka bergabung dengan penambang egois, dan kelompok yang berkolusi akan bertambah besar sampai menjadi mayoritas.
2. 2.Pada ini titik, sistem Bitcoin tidak lagi menjadi mata uang yang terdesentralisasi.
3. Penambangan yang egois dapat dilakukan untuk semua ukuran kelompok penambang yang berkolusi

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. Setiap penambang yang menerapkan perubahan akan mengurangi kemampuan kumpulan penambang egois untuk meningkatkan nilai Y melalui kontrol propagasi data, Peningkatan ini bersifat independen adopsi perubahan di penambang lain, oleh karena itu tidak memerlukan "hard fork", Perubahan kami secara eksplisit mengacak pilihan sewenang-wenang ini, dan karena itu tidak memperkenalkan kerentanan baru.