Nama : Firstasgi Qiyadh Darmawan

NIM : 1103194103

Summary Paper

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.

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

penambangan egois adalah serangan terhadap algoritma penyesuaian kesulitan konsensus blockchain [32]. Baru-baru ini, banyak upaya telah dikhususkan untuk serangan majemuk penambangan egois dengan serangan menahan block [14] [34], serangan penyuapan [15], serangan gerhana dan serangan pengeluaran ganda [22]

hasil dari pengamatannya di dapatkan bahwa:

1. BSM. Ambang batas kekuatan Hash yang menguntungkan di bawah 21,48% dengan dua penyerang BSM simetris, dibandingkan dengan 25% dengan penyerang BSM tunggal dan 23,21% dengan penyerang optimal tunggal. Lebih banyak blok yang diizinkan untuk dipegang secara pribadi atau lebih banyak penyerang akan secara dramatis mengurangi ambang batas ini. Ketika kekuatan Hash dari dua penyerang asimetris, ambang menguntungkan dari satu penyerang akan berkurang terlebih dahulu dan kemudian meningkat ketika power Hash penyerang lainnya meningkat (yaitu tidak monoton).
2. POMDP. Kebijakan pertambangan POMDP membawa lebih banyak pendapatan bagi penambang strategis daripada BSM dan pertambangan jujur , dan mendekati kinerja kebijakan penambangan MDP dengan informasi yang lengkap. Ketika penyerang BSM (Bob) memiliki kekuatan Hash 34%, ambang menguntungkan penyerang lain (Alice) menurun dari 29,44% menjadi sekitar 2% jika

   dia memilih POMDP daripada BSM. Algoritma online yang dirancang dapat dengan cepat dan efektif menghitung tindakan yang hampir optimal di bawah information yang dapat diamati saat ini.

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:*

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. 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*.

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.

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 jumlah blok dalam rumus penyesuaian kesulitan

$$D_{\text{new}} = D_{\text{old}} \cdot \frac{(n_0 + n')\tau_0}{S_{n_0}}$$

Majority is not Enough: Bitcoin Mining is Vulnerable INTRO

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.

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.

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.

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

Kami memperoleh formula untuk menghitung pendapatan relatif untuk penambang jujur dan penambang jahat di Bitcoin dan pendapatan penambangan Ethereum terdiri dari tiga jenis hadiah, tetapi strategi penambangan optimal penambangan Bitcoin untuk penambang jahat dan dua penambangan di cabang pribadi ketika dua blok diterbitkan secara bersamaan dan kekuatan hash penambang jahat di Bitcoin dan Ethereum, masing-masing.

Model Markov dimensi yang dapat menggambarkan penambangan egois penambangan egois pada Bitcoin dan kinerja sistem Ethereum penambangan berbahaya pada keamanan blockchain, kami mempertimbangkan skenario yang dianggap penambangan egois. Jumlah rata-rata blok paman yang dibuat dalam a Jumlah blok reguler s yang dibuat dalam jumlah rata-rata blok reguler yang dibuat oleh sistem dengan serangan pengeluaran ganda selain penambang jujur Grup 1 (G1) terdiri dari penambang jujur dan MP, dan menunjukkan probabilitas blok yang dihasilkan oleh G1 Sebelum presentasi perilaku penambang jujur dan MP, Di Ethereum, blok paman hanya dapat direferensikan oleh satu Perilaku penambang jujur penambang mengendalikan sebagian besar kekuatan hash di blockchain Penambang jujur mengadopsi strategi penambangan jujur: \