Nama : Hanif Shafwan Mahib

NIM : 1103194150

Kelas : TK-43-02

Tugas 5 Blockchain

I. Summary

1. Eclipse Attack

Cryptocurrency terdesentralisasi seperti Bitcoin dan altcoin lainnya telah menarik minat publik, dan telah jauh lebih berhasil daripada inkarnasi uang elektronik sebelumnya. Banyak yang akan menyebut kebangkitan mata uang elektronik ini sebagai revolusi teknologi, dan "gelombang masa depan". Cryptocurrency yang muncul ini mewujudkan teknologi blockchain baru, di mana penambang mencapai konsensus tentang sejarah transaksi dan status buku besar. Analisis awal keamanan Bitcoin bergantung pada asumsi bahwa sebagian besar jaringan, yang diukur dengan sumber daya komputasi, akan secara jujur menjalankan klien referensi default. Segera menjadi jelas bahwa asumsi ini harus dibenarkan dengan pertimbangan insentif pengguna atau penyerang untuk menyimpang.

Menunjukkan bahwa dalam cryptocurrency terdesentralisasi seperti Bitcoin, strategi penambangan membentuk ruang yang rumit, dan ruang ini dapat diperluas lebih lanjut dengan menggabungkan serangan penambangan dan serangan tingkat jaringan dengan cara yang tidak sepele. Pekerjaannya membuka tantangan berikut:

1) Karakterisasi yang lebih lengkap dari ruang strategi yang kompleks dan metode analitik untuk menurunkan dan membuktikan strategi optimal yang diberikan pilihan parameter apa pun.
2) Merancang protokol konsensus aman yang dapat dibuktikan yang keamanannya secara formal didasarkan pada asumsi rasionalitas daripada mayoritas yang jujur.

2. ForkDec

Dalam karya ini, mengusulkan sistem deteksi untuk egois serangan penambangan di Bitcoin, yang disebut ForkDec, sistem e adalah berdasarkan model klasifikasi pembelajaran mesin untuk mewujudkan deteksi cerdas serangan. Untuk memastikan bahwa ForkDec memiliki akurasi deteksi tinggi, kami membuat kumpulan data yang berisi sekitar 200.000 sampel garpu Bitcoin untuk pelatihan model. Kami kemudian terapkan ForkDec ke set tes untuk evaluasi. hasil evaluasi menunjukkan bahwa ForkDec dapat mencapai akurasi 99,03% untuk mendeteksi penambangan egois di Bitcoin.

Yang perlu jelas adalah bahwa ForkDec hanya bisa mendeteksi adanya serangan tetapi tidak dapat mengidentifikasi penambang yang melancarkan serangan. Di pekerjaan mendatang, kami akan menganalisis lebih lanjut strategi penyerang dan meningkatkan ForkDec untuk secara akurat menemukan penyerang. Selain itu, blockchain juga berlaku di bidang perlindungan privasi dan data ketertelusuran. Penyerang dapat menggunakan metode lain untuk menyerang rantai blok. Oleh karena itu, kita juga harus mempelajari penerapan ForkDec untuk mendeteksi serangan lain, misalnya serangan pengeluaran ganda, serangan bandit waktu, dan serangan DoS blockchain.

3. Majority is not Enough

   Keamanannya bitcoin sangat bergantung pada distribusi protokol yang memelihara blockchain, protokol tersebut dijalankan oleh pekerja yang disebut penambang. 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.

4. 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 untuk menemukan blok yang valid. Penambang egois biasanya tidak ingin menghancurkan konsensus PoW blockchain, tetapi untuk memanfaatkannya. Rasio minimum kekuatan Hash yang membawa lebih banyak hadiah bagi penambang egois daripada rasio ini secara konvensional disebut ambang menguntungkan.

5. On Selfish Mining 20

   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. 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.

6. Selfish and Stubborn

   Bitcoin dan Ethereum adalah dua cryptocurrency teratas berbasis blockchain baik dari kapitalisasi pasar cryptocurrency atau popularitas. Namun, mereka rentan terhadap penambangan yang egois dan penambangan yang keras kepala karena keduanya mengadopsi mekanisme konsensus Proof-of-Work.

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.