Nama : Weni Wilman Putri

NIM : 1103184134

Pendahuluan

Cryptocurrency terdesentralisasi seperti Bitcoin dan coin lainnya telah menarik minat publik, dan telah jauh lebih sukses 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.

Karena cryptocurrency membawa nilai moneter, mereka secara alami menjadi target serangan yang berharga. Secara intuitif, untuk cryptocurrency yang dirancang dengan aman, penyerang mengendalikan α sebagian kecil dari sumber daya komputasi jaringan seharusnya hanya dapat diperolehα sebagian kecil dari hadiah penambangan. Namun, penyerang dapat menggunakan berbagai jenis serangan untuk mendapatkan bagian yang tidak adil dari hadiah penambangan. Kami menyebut serangan seperti itu secara umum sebagai serangan penambangan. Di antara yang paling terkenal adalah serangan gaya selfish mining yang mengeksploitasi kelemahan dalam protokol konsensus terdistribusi dan dan serangan tingkat jaringan yang berusaha membuat partisi jaringan antara kekuatan penambangan, disebut sebagai eclipse attack.

Selfish Mining dan Eclipse Attack

Selfish mining tidak optimal untuk ruang parameter yang besar. Ada strategi yang dapat dijadikan alternatif, yaitu stubborn mining yang menggeneralisasi dan mengungguli serangan selfish mining. Untuk sebagian besar ruang parameter yang menarik, strategi baru kami secara signifikan meningkatkan pendapatan penyerang. Bergantung pada parameter lingkungan, strategi penambangan yang keras kepala dapat mengalahkan penambangan yang egois hingga 25% (bahkan tanpa memanfaatkan serangan tingkat jaringan apa pun). Bergantung pada parameternya, dan pada harga selama penulisan, ini dapat menghasilkan keuntungan tambahan $73K per hari dibandingkan dengan penambang yang egois. Kami menunjukkan bahwa dalam beberapa kasus, strategi yang keras kepala dapat menghasilkan 13%keuntungan dibandingkan dengan non-trail-stubborn.

Selfish miners juga dapat mengeksploitasi serangan tingkat jaringan untuk lebih meningkatkan keuntungannya. Secara khusus, dengan kesukesesan eclipse attack, penyerang mengisolasi korban dari rekan-rekannya yang lain di tingkat jaringan, dengan mengontrol koneksi masuk dan keluarnya. Bergantung pada parameternya, strategi ini terkadang dapat menghasilkan 30% keuntungan dibandingkan dengan penggunaan naif dari node yang hilang. Kami juga menunjukkan bahwa secara mengejutkan, dalam beberapa rentang parameter, strategi terbaik penyerang sebenarnya membantu node eclipse, maka korban mungkin memiliki sedikit insentif untuk mencegah, mendeteksi, atau bereaksi terhadap serangan tersebut. Tidak

ada strategi tunggal yang merupakan strategi optimal “satu ukuran untuk semua”. Sebaliknya, penyerang harus memilih strateginya berdasarkan parameter yang diperkirakan termasuk jumlah daya komputasi yang dapat digunakannya, fraksi jaringan yang berpotensi dikalahkan, dan fraksi jaringan tersisa yang dapat dipengaruhinya.

Hasil Temuan

Pertama, kami menunjukkan bahwa ruang strategi penambangan yang layak itu rumit, dan selfish mining secara umum tidak optimal. Kedua, kami menunjukkan bahwa kemungkinan menggabungkan serangan penambangan dengan serangan tingkat jaringan semakin memperumit ruang kemungkinan strategi. Tantangan penting yang kami ajukan adalah tugas merancang protokol konsensus yang keamanannya terjamin.

Implementasi referensi Bitcoin mengamanatkan bahwa, setiap kali beberapa penambang menghasilkan blok yang valid, ia mendistribusikannya ke seluruh jaringan. Eyal dan Sirer menunjukkan selfish miners dapat memperoleh bagian yang tidak adil dari hadiah blok dengan menyimpang dari klien referensi. Secara khusus, seorang penambang dengan lebih dari 33% daya komputasi dapat mencapai keuntungan yang tidak proporsional dengan mempertahankan blockchain pribadi dan menahan blok yang telah ditambang. Ini memaksa penambang yang jujur untuk melakukan perhitungan yang sia - sia di cabang publik yang basi. Penambangan yang egois berhasil karena penambang yang jujur dipaksa untuk menghabiskan sebagian siklus komputasi mereka pada blok yang ditakdirkan untuk tidak berada di chain publik. Berbagai serangan lain telah dipelajari. Misalnya, anggota kumpulan penambangan dapat meluncurkan serangan penahan blok terhadap kumpulan itu sendiri. Hal ini merugikan kumpulan korban dan anggota lainnya, tetapi sebenarnya meningkatkan pendapatan jaringan lainnya.

Pemodelan Penambangan Bitcoin

Menentukan Parameter Kunci Hashpower penyerang yaitu, Alice: bagian dari total hashpower jaringan yang dikendalikan oleh penyerang, selanjutnya disebut sebagai "Alice" Hashpower dari publik yang jujur yaitu, Bob: bagian dari hashpower dari jaringan yang tersisa, selanjutnya disebut sebagai “Bob”. Pengaruh jaringan Alice: sebagian kecil dari jaringan Bob (dalam hal kekuatan hash) yang akan menambang di blok Alice (yaitu, penyerang) ketika Alice dan Bob telah melepaskan blok pada (kurang lebih) pada waktu yang sama sehingga menghasilkan fork dengan panjang yang sama. Jika penambang yang jujur menemukan sebuah blok, ia akan segera menerbitkan blok tersebut.

Pendapatan

Pendapatan pertambangan. Setiap kali seorang penambang menemukan sebuah blok, dia mendapatkan hadiah berupa Bitcoin yang baru dicetak. Saat ini, dan dalam waktu dekat, hadiah ini adalah 25 BTC per blok (yaitu, pada saat penulisan≈ $6000USD per blok). Namun, hanya blok dirantai utamamenghitung pendapatan mereka. Misalnya, setiap kali ada garpu (dua balok dengan panjang yang sama, yaitu,memimpin=0kan), salah satu dari dua blok pada akhirnya akan dibuang

Stubborn Mining

Stubborn mining secara ketat menggeneralisasi dan meningkatkan yang diketahui sebelumnya seperti strategi selfish mining. Strategi penambangan mendefinisikan mesin state,

di mana setiap state mewakili lead rantai blok pribadi Alice di atas rantai blok publik Bob dan apakah ada percabangan. Ada dua jenis transisi status di mesin status ini:

1) Status transisi yang terjadi ketika Bob menemukan blok baru. Dalam hal ini, Bob selalu mengumumkan blok baru dengan segera. Pada titik ini, Alice memiliki kebebasan untuk melakukan tindakan berikut:
    a. jika rantai pribadi Alice memimpin, Alice dapat memutuskan apakah dan berapa banyak blok yang akan diungkapkan dari rantai pribadinya kepada Bob; dan
    b. jika rantai pribadi Alice cukup berada di belakang rantai Bob, Alice dapat memilih untuk meninggalkan penambangan di rantai pribadinya dan menerima rantai Bob. Keputusan Alice dalam kasus ini akan menentukan bagaimana rantai Markov akan bertransisi ketika Bob menambang blok berikutnya.
2) Status transisi yang terjadi ketika Alice menemukan blok baru. Dalam kasus terakhir, yaitu, ketika Alice menambang blok berikutnya, kami berasumsi bahwa Alice dapat terus menambang di rantai pribadinya sendiri. Apakah Alice segera mengungkapkan blok barunya kepada Bob tergantung pada strategi dan keadaan saat ini.