Nama : Aflah Naufal Afii
NIM : 1103183203

Dirty Pool Full-fledged Simulation for Selfish Mining in Bitcoin

➢ Selfish Mining

Pada tahun 2010, pengguna RHorning menggambarkan ide penambangan egois di forum Bitcoin, bitcointalk . Pengguna forum memberikan hasil simulasi untuk serangan itu, yang pada saat itu disebut serangan kartel penambangan. Kemudian pada tahun 2013 istilah penambangan egois dan deskripsi formalnya diperkenalkan oleh peneliti Cornell Emin Giin Sirer dan lttay Eyal dalam makalah Mayoritas tidak cukup: Penambangan Bitcoin Rentan
Penambang egois terus menambang blok berikutnya tetapi tidak menyiarkannya. Mereka terus melakukannya mempertahankan keunggulan mereka. Dengan cara ini akan ada garpu tersembunyi di blockchain yang hanya bisa dilihat oleh penambang yang egois. Ketika sisa jaringan akan mengejar penambang egois maka penambang egois melepaskan bagian mereka dari blok yang diselesaikan ke dalam blockchain.

Serangan penambangan egois adalah metode untuk kumpulan penambangan untuk meningkatkan pengembaliannya dengan tidak bermain adil. Hasilnya adalah rantai dan bukti kerja mereka lebih panjang dan lebih sulit sehingga jaringan lainnya mengadopsi solusi blok mereka dan mereka mengklaim hadiah blok.

Ada juga penyerangan Eclipse, yaitu kondisi saat seorang penyerang memonopoli koneksi keluar masuk blok, sehingga akan terjadi isolasi pada user yang ada pada jaringan tersebut. Terlebih lagi, apabila blok ini memiliki kunci yang strategis terhadap mayoritas blok lainnya, user akan membutuhkan lebih banyak daya komputasi yang pada akhirnya akan digunakan untuk membantu kebutuhan si penyerang ini. Serangan seperti ini juga memiliki konsep yang sama dengan Selfish dan Stubborn mining yaitu penyerangan dari salah satu user untuk kepentingan pribadi.

➢ Stubborn Mining

Setelah memperkenalkan penambangan egois, beberapa penelitian lebih lanjut menunjukkan bahwa strategi penambangan egois yang lebih umum bisa lebih menguntungkan. Misalnya Serangan Bitcoin Teoretis dengan Kurang dari Setengah Kekuatan Komputasi (draft) dan khususnya Penambangan Keras Kepala: Menggeneralisasi Penambangan Egois dan Menggabungkan dengan Serangan Eclipse memberikan generalisasi komprehensif penambangan egois dan juga memperkenalkan nama yang berbeda untuk setiap variasinya:

- Lead Stubborn Mining Strategy

Penambang Keras Kepala menunggu sampai penambang jujur mengejarnya untuk menyiarkan semua blok rahasianya sebagai lawan dari penambang egois yang tidak mengambil risiko ditangkap oleh penambang jujur dan menyiarkan bloknya jika kemajuannya menyusut menjadi satu blok.

- J-Trail Stubborn Mining Strategy

trail Stubborn Mining merupakan perbaikan dari Lead Stubborn Mining. Ketika jejak rantai pribadi Penambang Keras berada di belakang rantai publik, mereka mungkin memutuskan untuk terus menambangnya, dengan harapan bisa menyusul. Kami mempertimbangkan keluarga strategi keras kepala jejak yang diparameterisasioleh ambang j, sehingga penambang keras kepala aj-trail menerima blockchain publik hanya ketika rantai pribadi mereka berada di belakang rantai publik dengan j + 1 blok). Jadi menurut defmisi, penambangan keras kepala I-trail sama dengan

penambangan keras kepala timah. Di sini kami hanya mempelajari penambangan keras kepala 2-trail,3-trail dan 4-trail karena strategi keras kepala trail lainnya dapat dengan mudah didominasi oleh strategi lain.

- Equal Fork Stubborn Mining Strategy

Penambang Keras Garpu Setara menunggu blockchain resmi untuk mengatasi garpu rahasianya dengan satu blok. Dia hanya menyerah ketika panjang blockchain resmi sama dengan panjang garpu rahasianya ditambah satu.