Nama : Asep Irawan

NIM : 1103190112

Dirty Pool
A Full-fledged Simulation for Selfish Mining in Bitcoin

A. Selfish Mining

Pada tahun 2010, seorang pengguna bernama RHorning mendeskripsikan sebuah ide "*selfish mining*" pada forum Bitcoin **bitcointalk**. Pengguna dari forum ini menyediakan simulasi akan hasil dari serangan, yang pada saat itu disebut dengan *mining cartel attack.* Nantinya pada taun 2013 istilah *selfish mining* dan penjelasan formalnya diperkenalkan oleh peneliti Cornel Emin Gun Sirer dan Ittay Eyal dalam tulisan "Majority is not enough :Bitcoin mining is vulnerable".

Singkatnya *selfish mining attack* adalah metode untuk *mining pools* untuk meningkatkan umpan balik dengan bermain tidak adil. Seorang *selfish miner* akan terus menambang block berikutnya namun tidak menyebarkan informasinya. Mereka akan terus mempertahankan kepastian mereka. Dengan ini akan ada suatu garpu tersembunyi pada blockchain yang hanya dapat dilihat oleh *selfish* blockchain. Ketika jaringan yang lainnya akan menyusul dengan *selfish miner*, *selfish miner* akan meluncurkan sebagian dari blocks yang di selesaikan kedalam blockchain. Hasilnya ialah *chain* dan *proof of work* mereka lebih panjang dan lebih sulit , sehingga jaringan lainnya mengadopsi blocks mereka dan menuntut hadiah blocknya.

B. Stubborn Mining

Setelah diperkenalkannya *selfish mining* penelitian lebih lanjut menunjukan stratregi *selfih mining* yang lebih general dan lebih menguntungkan. Contohnya "Theoretical Bitcoin Attack with less than half of the computational power (Draft)" dan lebih pentinya "Stubborn Mining : Generalizing Selfish Mining dan Combining an Eclipse Attack". Hal tersebut mnyediakan sebuah pemahaman akan penyamarataan akan *selfish mining* dan juga pengenalan akan nama-nama yang berbeda untuk setiap variasinya sendiri.

Lead Stubborn Mining Strategy

Miner ini menunggu miner jujur untuk menyusul mereka sebelum melakukan penyebaran akan semua block tersembunyi tentangan dari miner egois yang tidak mau mengambil resiko agar tidak tertangkap oleh miner jujur, dan menyebarkan block dia jika kecepatan dan kemajuan dia mengecil hingga satu block.

J-Trail Stubborn Mining Strategy

Trail Stubborn Mining ini merupakan sebuah perbaikan dari Lead Stubborn Mining. Saat Chain bribadi milik Trail Stubborn Miner tertinggal Chain publik, mereka mungkin akan memutuskan untuk terus menambang saja, dengan harapan untuk dapat menyusul.

Equal Fork Stubborn Mining Strategy

Sebuah Equal Fork Stubborn Mining Strategy menunggu blockchain resmi untuk mengetahui rahasia garpunya dari satu block. Dia hanya dapat menyerah disaat panjang dari blockchain resmi sama dengan fork rahasia dia.