Nama : Putri Mellia Zahrani

NIM : 1103190143

Summarized Self Mining

1. **Pengertian Self Mining**

   Self Mining atau Penambangan egois adalah strategi penambangan cryptocurrency yang menipu di mana satu penambang atau kelompok memecahkan hash, membuka blok baru, dan menahannya dari blockchain publik. Self Mining ini termasuk serangan karena di lakukan perubahan dengan sengaja dari blockchain sehingga dapat meningkatkan hadiah penambang atau sekelompok penambang. Tindakan ini menciptakan garpu, yang kemudian ditambang untuk maju dari blockchain publik.

   Jika blockchain grup berada di depan blockchain yang jujur, ia dapat memperkenalkan blok terbarunya ke jaringan. Jaringan diarahkan untuk mengenali blok terbaru, sehingga garpu grup akan menimpa blockchain asli. Para penambang dapat secara efektif mencuri cryptocurrency dari pengguna lain dengan mengubah blockchain.

2. **Cara Kerja Self Mining**

   "Mining" adalah proses di mana node di jaringan blockchain memvalidasi dan mengkonfirmasi transaksi. Penambang mendapatkan token yang baru dicetak sebagai imbalan atas upaya komputasi mereka. Dengan penambangan yang egois, kartel mengaburkan blok yang baru dibuat dari rantai utama, mengungkapkannya di lain waktu.

   Self Mining ini pertama kali diidentifikasi oleh peneliti Cornell Emin Gün Sirer dan Ittay Eyal dalam makalah tahun 2013.1 Mereka membuktikan bahwa sangat mungkin untuk mendapatkan lebih banyak bitcoin dengan menyembunyikan blok yang baru dibuat dari blockchain utama, menciptakan garpu blockchain. Secara teoritis, para penambang dapat memperkenalkannya ke jaringan pada waktu yang tepat dan mengubah blockchain.

   Bitcoin dan jaringan cryptocurrency lainnya yang menggunakan mekanisme konsensus proof-of-work bergantung pada penambang yang perangkat lunak penambangannya menemukan solusi untuk nomor hash terenkripsi yang dibuat secara acak. Ketika hash dipecahkan, blok baru terbuka di blockchain, dan penambang yang memecahkannya menerima biaya transaksi dan hadiah. Dalam makalah mereka tahun 2013, Sirer dan Eyal menunjukkan bahwa penambang dapat meningkatkan keseluruhan bagi hasil mereka dengan menyembunyikan blok baru dan membuatnya tersedia untuk sistem dalam jaringan pribadi mereka. Praktik ini mempercepat proses penemuan dan mengatasi masalah infrastruktur yang terkait dengan penambangan, seperti latensi jaringan dan biaya listrik.

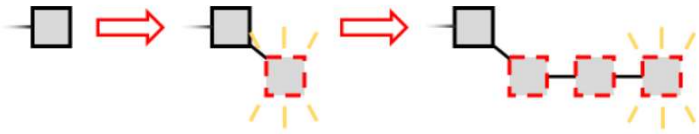
   Awalnya, blockchain bercabang akan lebih pendek dari blockchain publik. Rantai pribadi menambang blok baru di dalam kumpulannya dan menyembunyikan blok yang baru dibuat. Proses penambangan diulang sampai blockchain pribadi mencapai ketinggian blok yang lebih besar dari pada blockchain publik.

Self Mining kemudian secara strategis mengatur waktu pengenalan blok baru mereka ke blockchain yang jujur sehingga blockchain publik bergabung dengan rantai yang baru diperkenalkan. Jaringan publik menambang blockchain baru, dan Self Mining menerima hadiah cryptocurrency dan biaya transaksi untuk blok mereka yang baru diterima.

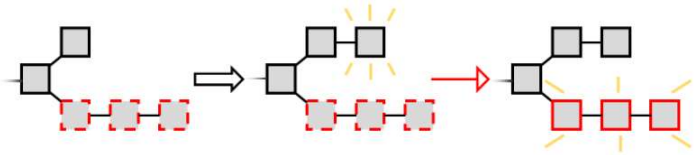
Sirer dan Eyal menganalisis sumber daya yang terbuang untuk kedua rantai tersebut. Mereka mendalilkan bahwa Self Mining memiliki keunggulan kompetitif atas penambang di blockchain publik karena imbalan mereka relatif lebih besar setelah memperhitungkan sumber daya yang terbuang.

3. Algoritma Selfish Mining

Pertama, selfish miner mencoba memperpanjang rantai terpanjang, seperti yang seharusnya. Namun, begitu dia membuat blok, dia merahasiakannya daripada menerbitkannya, dan kemudian mencoba memperluasnya lebih jauh, membentuk cabang rahasia.

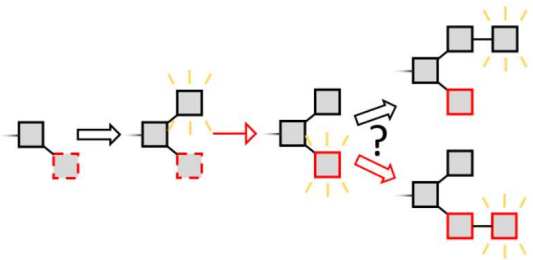


Sementara itu, miner lain memperpanjang rantai publik, yang pada akhirnya akan menjadi lebih panjang (dengan probabilitas 1) karena mereka adalah mayoritas. Penambang egois terus memperluas cabang rahasianya sampai rantai publik selangkah di belakang. Kemudian dia menerbitkan rantai rahasianya.

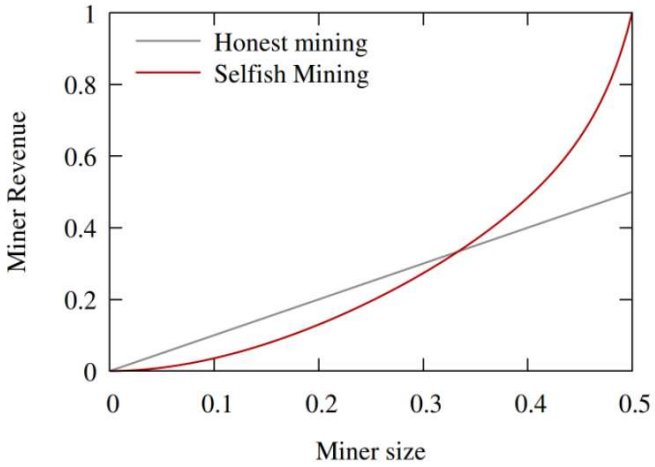


Karena rantai rahasia lebih panjang, pihak lain menganggapnya sebagai rantai utama, jadi sekarang semua orang mengikuti blok penambang yang egois. Blok yang dihasilkan oleh penambang lain dengan demikian dipangkas - diabaikan dan tidak memberikan hadiah kepada pembuatnya.

Tapi ada peringatan untuk strategi ini - ketika pertama kali membentuk rantai rahasianya, penambang egois mengambil risiko. Jika dia membuat blok rahasia pertama dan kemudian penambang lain membuat blok, dia tidak dapat mempublikasikan blok rahasianya dan memiliki rantai terpanjang; sebaliknya, itu akan menjadi perlombaan antara dua cabang panjang satu.



Selfish Miner akan mencoba untuk memperpanjang cabangnya sendiri, dan untuk kesederhanaan mari kita asumsikan bahwa semua penambang lain akan mencoba untuk memperpanjang cabang lainnya. Jika dia menang, dia menerbitkan bloknya, yang merupakan rantai terpanjang, dan serangan dimulai kembali di akhir rantai terpanjang ini. Jika penambang lain menang, penambang egois dirugikan (cabang lebih pendek). Dalam hal ini dia menyerah upaya serangan dan mulai lagi. Dia tidak memperoleh pendapatan dari blok rahasianya yang sebelumnya dipangkas.



Dari gambar di atas kita dapat melihat bahwa penambang egois yang lebih besar dari 1/3 kekuatan penambangan akan meningkatkan pendapatannya dengan menyimpang dari protokol yang ditentukan dan melakukan Penambangan Egois.