Nama : Delatifa Putri Sugandi

NIM : 1103194080

Selfish Minning Attacks Summarize

Pada tahun 2013, Selfish mining beserta deskripsinya diperkenalkan oleh peneliti yang bernama Cornell Emin Gun Sirer dan Ittay Eyal. Serangan Selfish Mining adalah metode untuk meningkatkan pengembaliannya dengan tidak bermain adil. Serangan Selfish Mining juga dikenal sebagai serangan pemotongan blok, menggambarka upaya jahat untuk mendiskreditkan integrasi jaringan blockchain.

Pertama kali diusulkan oleh peneliti Cornell pada tahun 2013, Selfish Mining mendefinisikan mekanisme bagi penambang untuk bekerja sama dan meningkatkan keuntungan mereka dengan membuat garpu terpisah dan tidak mengungkapkan blok yang ditambang ke seluruh jaringan. Ini berdampak pada kesehatan protokol secara keseluruhan, karena kolusi meningkatkan risiko sentralisasi. Penambangan Bitcoin bergantung pada sejumlah faktor, termasuk, namun tidak terbatas pada, efisiensi mesin penambangan, biaya listrik, dan daya hash yang disumbangkan ke jaringan . Desainnya memastikan desentralisasi dengan memberikan hadiah kepada penambang individu di blockchain, yang merupakan salah satu alasan popularitas kumpulan penambangan karena memungkinkan penambang untuk menerima hadiah yang berkelanjutan dan konsisten.

Namun, penambang dapat sangat mengoptimalkan penambangan dan meningkatkan hasil dengan terlibat dalam penambangan yang egois. Jika mereka berhenti mendeklarasikan blok baru ke jaringan publik, itu dapat membuat proses berjalan lebih cepat dan mengurangi pemborosan sumber daya.

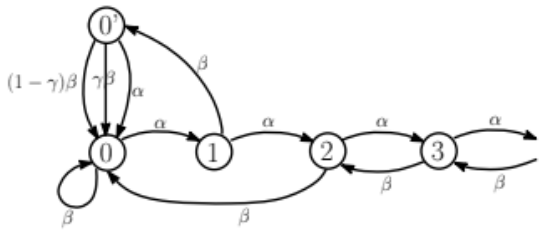
❖ The Selfish Mining Strategy

Strategy selfish mining mengikuti honest mining yaitu :

- Ketika lead = 2 dan Bob menambang blok berikutnya: Ungkapkan seluruh private chain Alice kepada Bob (menghasilkan lead = 0).
- Saat lead = 00 dan Alice menambang blok berikutnya: Tunjukkan rantai pribadi Alice ke Bob (menghasilkan lead = 0).
- Ketika lead = 0 atau lead > 0 dan Alice menambang blok yang berikutnya : Jangan ungkapkan private chain Alice
- Alice selalu menerima rantai terpanjang.

Efek dari Selfish mining adalah "membuang" penambangan daya pada blok yang akhirnya dibuang. Kadang-kadang Alice menghabiskan upaya tanpa hasil dan rantai pribadinya jatuh di belakang Bob; pada kesempatan lain, Bob menyia-nyiakan pekerjaan sambil Alice sudah di depan. Hasil yang mengejutkan adalah bahwa untuk banyak nilai dan, strategi ini menyebabkan Bob menyia-nyiakan lebih banyak pekerjaan daripada Alice. Setelah jaringan menyesuaikan

teka-teki kesulitan untuk mengkompensasi blok yang dibuang (yang tidak berkontribusi pada rantai utama), Alice memperoleh lebih banyak pendapatan daripada jika dia menambang dengan jujur.



Selfish Mining strategy digunakan untuk menjaga blok yang ditemukan tetap pribadi, sehingga dengan sengaja memotong rantai. Honest node terus menambang di rantai publik, sementara kumpulan menambang dicabang swasta sendiri. Jika kumpulan menemukan lebih banyak blok, itu mengembangkan keunggulan yang lebih lama di rantai publik, dan terus merahasiakan blok baru ini. Ketika cabang publik mendekati cabang pool pribadi, para selfish miner mengungkapkan blok dari rantai pribadi mereka ke publik.

Selfish-Mine memungkinkan kumpulan ukuran yang cukup untuk mendapatkan pendapatan yang lebih besar darinya rasio kekuatan pertambangan. Untuk penyederhanaan, dan tanpa kehilangan keumuman, kita asumsikan bahwa penambang dibagi menjadi dua kelompok, kelompok minoritas yang berkolusi yang mengikuti strategi penambangan yang egois, dan mayoritas yang mengikuti strategi penambangan yang jujur. Tidak penting apakah penambang yang jujur beroperasi sebagai kumpulan kelompok, atau individu.

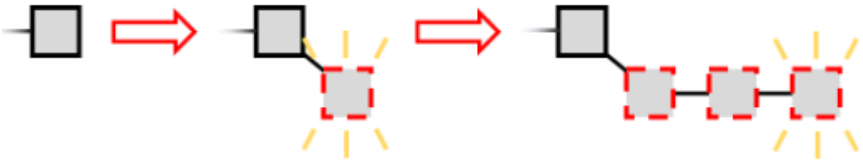
Serangan penambang egois dimulai dengan memvalidasi dan tidak menyiarkan blok, lalu melanjutkan penambangan secara diam-diam pada atas blok ini. Kemudian dia melanjutkan sebagai berikut:

1. Jika uang muka penambang egois hanya sama dengan 1 blok dan penambang jujur menemukan blok kemudian penambang egois segera menyiarkan blok dia telah menambang secara diam-diam. Sebuah kompetisi kemudian mengikuti. Penambang egois adalah diasumsikan cukup terhubung dengan baik dengan sisa jaringan sehingga pecahan 0 γ 1 dari jaringan yang jujur menerima proposal bloknya dan mulai menambang di atasnya.
2. Jika kemajuan penambang egois adalah 2 blok dan penambang jujur menemukan satu blok, lalu penambang egois segera menyiarkan dua blok yang dia miliki ditambang secara rahasia. Kemudian, seluruh jaringan beralih ke garpunya.
3. Jika kemajuan penambang egois lebih besar dari 2, maka penambang egois melepaskan blok segera setelah penambang jujur menemukannya.
4. Dalam kasus lain, penambang yang egois terus menambang secara diam-diam di atas garpunya.

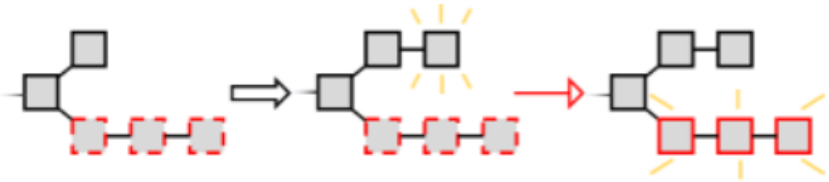
❖ Algoritma Selfish Mining

Selfish Mining adalah algoritma penambangan strategis yang menunjukkan bahwa protokol yang ditentukan bukanlah keseimbangan bagi penambang minoritas pada umumnya.

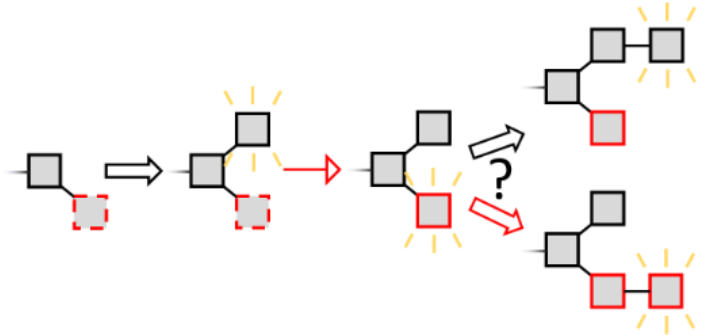
Pertama, penambang egois mencoba memperpanjang rantai terpanjang, seperti yang seharusnya. Namun, begitu dia membuat blok, dia merahasiakannya daripada menerbitkannya, dan kemudian mencoba memperluasnya lebih jauh, membentuk cabang rahasia.



Sementara itu, penambang 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.



Stubborn Minning Attacks Summarize

Lead Stubborn Mining Strategy

A Lead Stubborn Miner waits until the honest miners catch up with him to broadcast all of his secret blocks as opposed to the selfish miner who does not take the risk of being caught by the honest miners and broadcasts his blocks if his advance shrinks to one block.

j–Trail Stubborn Mining Strategy

trail Stubborn Mining is an amelioration of Lead Stubborn Mining. When a trail Stubborn Miner's private chain falls behind the public chain, they may decide to continue mining on it anyway, in the hope of catching up. We consider a family of trail stubborn strategies parameterized by a threshold j, such that a j–trail stubborn miner accepts the public blockchain only when their private chain falls behind the public chain by j + 1 blocks). So by definition the 1–trail stubborn mining is the same as lead stubborn mining. Here we study only 2–trail, 3–trail and 4–trail stubborn mining since the other trail stubborn strategies can be easily dominated by other strategies.

Equal Fork Stubborn Mining Strategy

An Equal Fork Stubborn Miner waits for the official blockchain to overcome his secret fork by one block. He/she only gives up when the length of the official blockchain is equal to the length of his secret fork plus one.

Stubborn Mining Strategies

As we can see, when lead = 2 and if Bob finds the next block and closes the gap by 1, the selfish miner would immediately reveal her private chain to guarantee that the network chooses her private chain over Bob’s. Therefore, the state transitions to lead = 0. In lead-stubborn mining, instead of revealing her entire private chain, Alice reveals the next block on her private chain only, to match the length of the public chain. In this case, γ fraction of Bob will mine on Alice’s private chain, and $1 - \gamma$ fraction mines on Bob’s fork; and the state transitions to lead = 10. This has pros and cons for the attacker Alice: if the $(1 - \gamma)$ fraction of Bob succeeds in advancing Bob’s chain, Alice may risk losing her private chain. However, if Alice or the γ fraction of Bob advances Alice’s fork, then Alice has successfully diverted a part of Bob, $(1 - \gamma)$ fraction, to do useless work. Moreover, when lead = k for some k > 2, and if Bob finds the next block, the selfish miner does not reveal her private chain, and thus the state machine transition to lead = $k - 1$. However, the lead-stubborn miner would again, immediately reveal one more block on her private fork, and the state thus transitions to lead = $(k - 1)$.