Nama : Hamzah Fatihulhaq

NIM : 110319213

SUMMARIZE

SELFISH MINING

Apa Itu *Selfish Mining*?

Serangan *Selfish Mining*, juga dikenal sebagai serangan pemotongan blok(*withholding attack*), menggambarkan upaya jahat untuk mendiskreditkan integritas jaringan blockchain. *Selfish Mining* adalah Serangan penambangan yang egois terjadi ketika seorang individu di kumpulan penambangan mencoba untuk menahan blok yang berhasil divalidasi agar tidak disiarkan ke seluruh jaringan kumpulan penambangan. Setelah penambang egois menahan blok mereka yang berhasil ditambang dari grup, mereka terus menambang blok berikutnya, sehingga penambang egois telah menunjukkan lebih banyak bukti kerja dibandingkan dengan penambang lain di kumpulan penambangan. Tindakan ini menciptakan *fork*, yang kemudian ditambang untuk menjadi yang terdepan di 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.

Cara Kerja *Selfish Mining*

"*Mining*" atau “Penambang” 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.

Penambangan egois pertama kali diidentifikasi oleh peneliti Cornell Emin Gün Sirer dan Ittay Eyal dalam makalah tahun 2013. Mereka membuktikan bahwa memungkin untuk mendapatkan lebih banyak bitcoin dengan menyembunyikan blok yang baru dibuat dari blockchain utama, dengan membuat *fork* 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

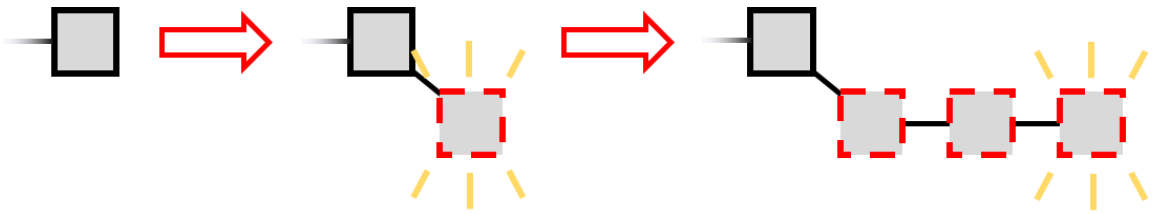
penambangan diulang sampai blockchain pribadi mencapai ketinggian blok yang lebih besar dari pada blockchain publik.

Penambang egois 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 penambang egois menerima hadiah cryptocurrency dan biaya transaksi untuk blok mereka yang baru diterima.

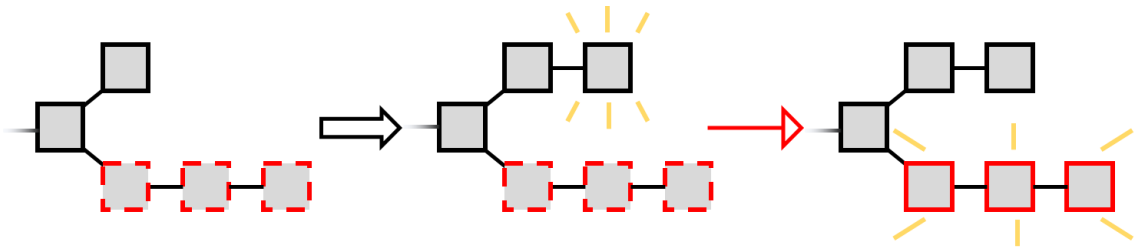
Sirer dan Eyal menganalisis sumber daya yang terbuang untuk kedua rantai. Mereka mendalilkan bahwa penambang egois memiliki keunggulan kompetitif atas penambang di blockchain publik karena imbalan mereka relatif lebih besar setelah memperhitungkan sumber daya yang terbuang.

Algoritma *Selfish Mining*

Selfish Mining (SM) adalah algoritma penambangan strategis yang menunjukkan bahwa protokol yang ditentukan bukanlah keseimbangan bagi penambang minoritas pada umumnya. Awalnya, penambang egois mencoba memperpanjang rantai terpanjang, seperti yang seharusnya. Namun, begitu penambang membuat blok, penambang akan merahasiakannya daripada menerbitkannya, dan kemudian mencoba memperluasnya lebih jauh, membentuk **cabang rahasia**.

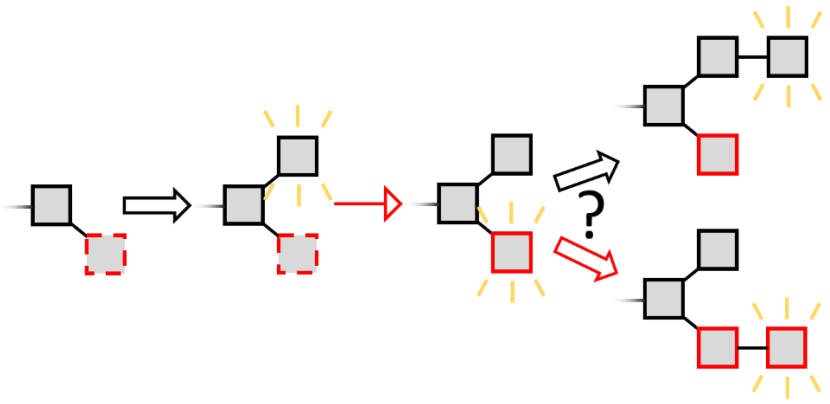


Sementara itu, penambang lain memperpanjang rantai publik, yang pada akhirnya akan menjadi lebih panjang (dengan probabilitas 1) karena mereka adalah mayoritas. Penambang egois terus memperluas cabang rahasianya sampai rantai publik selangkah di belakang. Kemudian dia menerbitkan rantai rahasianya.



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 dan diabaikan dan tidak memberikan hadiah kepada pembuatnya.

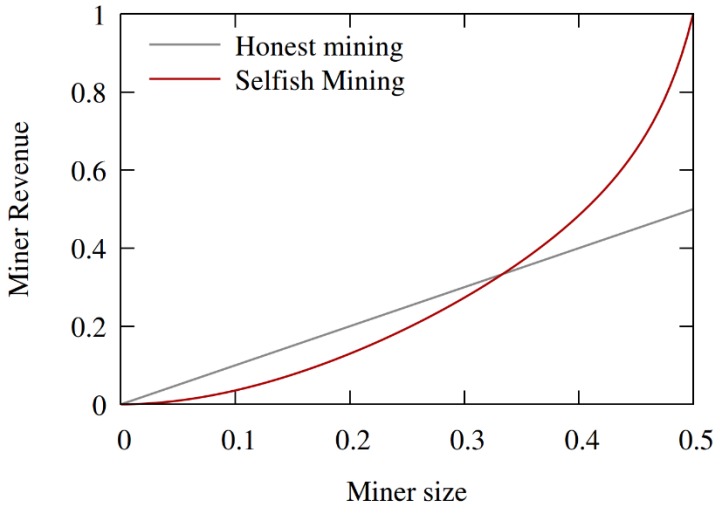
Tetapi ada peringatan untuk strategi ini, ketika pertama kali membentuk rantai rahasianya, penambang yang egois mengambil risiko. Jika penambang egois membuat blok rahasia pertama dan kemudian penambang lain membuat blok, dia tidak dapat mempublikasikan blok rahasianya dan memiliki rantai terpanjang. Sebagai gantinya, ini akan menjadi perlombaan antara dua cabang yang panjangnya satu.



Penambang yang egois akan mencoba untuk memperpanjang cabangnya sendiri, dan untuk kesederhanaan, diasumsikan bahwa semua penambang lain akan mencoba untuk memperpanjang cabang lainnya. Jika pengambang egois menang, penambang egois akan 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.

Analisis Penambangan Egois

Sepintas mungkin tampak serangan itu tidak akan berhasil dan penambang minoritas akan kehilangan lebih banyak balapan yang dia menangkan. Namun, analisis yang cermat menunjukkan hal ini tidak terjadi secara umum. Hal ini dapat digambarkan secara alami sebagai Rantai Markov. Dengan menghitung setiap blok dari penambang yang egois dan dari penambang lainnya, kita dapat menghitung rasio blok penambang yang egois dan pendapatannya dari semua blok sebagai fungsi dari ukurannya.



Dapat dilihat penambang egois yang lebih besar dari 1/3 kekuatan penambangan akan meningkatkan pendapatannya dengan menyimpang dari protokol yang ditentukan dan melakukan Penambangan Egois.

STUBBORN MINING

Stubborn Mining

Penambangan egois memberikan wawasan tentang serangan yang mengubah strategi penambangan. Pada tahun 2015, Neyak dkk, mengusulkan strategi alternatif yang disebut penambangan keras kepala. Dalam penambangan yang keras kepala, penyerang tidak akan mudah menyerah bahkan ketika cabang pribadinya tertinggal rantai utama dan tidak akan dengan mudah melepaskan cabang pribadi untuk mengklaim kemenangan saat itu sedang memimpin kompetisi. Strategi penambangan yang membandel dapat dikategorikan menjadi tiga macam, lead stubborn, equal fork stubborn and trail stubborn (Tj -stubborn) depending on

Lead Stubborn Mining Strategy

Lead Stubborn Mining 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 diparameterisasi oleh ambang j, sehingga penambang keras kepala j-trail menerima blockchain publik hanya ketika rantai pribadi mereka berada di belakang rantai publik dengan j + 1 blok). Jadi menurut definisi, penambangan keras kepala 1-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

Equal Fork Stubborn Mining menunggu blockchain resmi untuk mengatasi fork rahasianya dengan satu blok. Dia hanya menyerah ketika panjang blockchain resmi sama dengan panjang fork rahasianya ditambah satu.

Solusi

Dua solusi yang mungkin telah diusulkan untuk mencegah serangan penambangan egois terjadi di jaringan blockchain. Yang pertama adalah secara acak menugaskan penambang ke cabang-cabang blockchain ketika fork terjadi, dan yang kedua adalah menetapkan batas ambang batas untuk kumpulan penambangan di jaringan yang akan mencegah penambang egois mendapatkan keuntungan yang signifikan dibandingkan penambang lain yang beroperasi di jaringan.