Keamanan blockchain seperti Bitcoin didirikan oleh rantai teka-teki Hash kriptografi, yang ditangani oleh jaringan besar peserta pseudonim yang disebut *penambang.* Memecahkan teka-teki Hash dianggap sebagai cara untuk menghasilkan Proof-of-Work (PoW) untuk mencapai consensus global. PoW Bitcoin menuntut perhitungan intensif, sehingga mengkonsumsi banyak energi. Setiap penambang bersaing untuk "permainan" ini, dan dihargai oleh mata uang crypto (yaitu bitcoin) jika dia adalah penambang pertama yang diakui
untuk menemukan blok yang valid. Penambang egois biasanya tidak ingin menghancurkan konsensus PoW blockchain , tetapi untuk memanfaatkannya. Rasio minimum kekuatan Hash yang membawa lebih banyak hadiah bagi penambang egois daripada rasio ini secara konvensional disebut *ambang menguntungkan*. Eyal dan Sirer memperkenalkan skema penambangan egois pertama (yaitu penambangan egois dasar,BSM) dan menunjukkan bahwa ambang batas BSM yang menguntungkan adalah 25% dari total kekuatan Hash [2]. Nayak dkk. [9] mengusulkan penambangan keras kepala yang meningkatkan pendapatan penambang egois sebesar 13,94% dibandingkan dengan BSM. Sebagai trik utama dari skema keras kepala, penambang egois bersikeras untuk forking jika rantai pribadinya sedikit tertinggal di belakang rantai publik.

penambangan egois adalah serangan terhadap algoritma penyesuaian kesulitan konsensus blockchain [32]. Baru-baru ini, banyak upaya telah dikhususkan untuk serangan majemuk penambangan egois dengan serangan menahan block [14] [34], serangan penyuapan [15], serangan gerhana dan serangan pengeluaran ganda [22]

hasil dari pengamatannya di dapatkan bahwa:

1. BSM. Ambang batas kekuatan Hash yang menguntungkan di bawah 21,48% dengan dua penyerang BSM simetris, dibandingkan dengan 25% dengan penyerang BSM tunggal dan 23,21% dengan penyerang optimal tunggal. Lebih banyak blok yang diizinkan untuk dipegang secara pribadi atau lebih banyak penyerang akan secara dramatis mengurangi ambang batas ini. Ketika kekuatan Hash dari dua penyerang asimetris, ambang menguntungkan dari satu penyerang akan berkurang terlebih dahulu dan kemudian meningkat ketika power Hash penyerang lainnya meningkat (yaitu tidak monoton).
2. POMDP. Kebijakan pertambangan POMDP membawa lebih banyak pendapatan bagi penambang strategis daripada BSM dan pertambangan jujur , dan mendekati kinerja kebijakan penambangan MDP dengan informasi yang lengkap. Ketika penyerang BSM (Bob) memiliki kekuatan Hash 34%, ambang menguntungkan penyerang lain (Alice) menurun dari 29,44% menjadi sekitar 2% jika
   dia memilih POMDP daripada BSM. Algoritma online yang dirancang dapat dengan cepat dan efektif menghitung tindakan yang hampir optimal di bawah information yang dapat diamati saat ini.
3. Penundaan yang menguntungkan. Seorang penambang BSM menerima pendapatan yang kurang absolut daripada penambangan jujur pada periode penyesuaian kesulitan pertama bahkan jika kekuatan Hash-nya berada di atas ambang batas yang menguntungkan, dan keuntungannya dicapai di periode mendatang. BSM adalah after yang menguntungkan 51 putaran penyesuaian kesulitan (yaitu 714 hari dalam Bitcoin) jika kekuatan Hash dari dua penambang egois simetris adalah 22%. Penundaan ini menurun menjadi 5 putaran (yaitu 70 hari dalam Bitcoin) karena kekuatan Hash mereka bertambah menjadi 33%, yang masih cukup lama

Pada mode penambangan egois Alice mempertahankan rantai pribadi, begitu juga Bob, sementara Henry beroperasi pada rantai publik. Alice dan Bob tidak menyadari peran masing-masing, bahkan kehadiran satu

sama lainPanjang rantai pribadi disimpan sebagai informasi pribadi oleh Alice dan Bob, dan Panjang rantai publik diamati oleh mereka semua.

Prosedur penambangan terdiri dari dua kasus sebagai berikut.
• *(Kasus penambangan rantai publik)* Henry selalu menambang setelah rantai publik. Alice atau Bob juga menambang di rantai publik jika lebih panjang dari rantai pribadinya.
• *(Kasus penambangan rantai swasta)* Alice (resp. Bob) terus menambang rantai pribadinya (resp. nya) jika dia (resp. dia) menemukan blok baru dan rantai pribadi sekarang lebih panjang than rantai publik. *Prosedur pelepasan* lebih rumit daripada prosedur penambangan. Henry menyiarkan blok yang ditambang segera setelah ditemukan, sementara Alice dan Bob akan memutuskan apakah akan melepaskan blok yang ditambang tergantung pada panjang rantai publik.
• *(Kasus hangus)* Alice (resp. Bob) meninggalkan rantai pribadinya (resp. nya) dan sesuai dengan penambangan setelah rantai publik jika yang terakhir lebih panjang. Henry juga meninggalkan rantai publiknya jika Alice atau Bob menerbitkan rantai yang lebih panjang.
• *(Kasus pelepasan yang menghindari risiko)* Alice (resp. Bob) melepaskan bloknya (resp. nya) yang ditambang secara pribadi ke publik karena takut kehilangan jika blok baru ditambang oleh yang lain dan keuntungan utama dari rantai pribadinya tidak lebih dari dua blok.
• *(Kasus reaksi berantai)* Ketika Alice (resp. Bob) melepaskan bloknya (resp. nya) ke rantai publik dan memperbarui panjangnya, pelepasan blok pribadi Bob (resp. Alice) dipicu segera.

Definisi dasar dari selfish mining sendiri terdapat dua definisi:

Definisi pertama(pendapatan realtif) *Biarkan Ra, Rb dan Rh menjadi jumlah yang diharapkan dari blok yang valid yang ditambang oleh Alice, Bob dan Henry di putaran penambangan, masing-masing. Pendapatan relatif seorang penambang,* Rˆi*, dinyatakan sebagai:*

$$\hat{R}_i = \frac{R_i}{R_a + R_b + R_h}, \qquad i \in \{a, b, h\}$$

Perlu ditekankan bahwa blok yang valid adalah blok yang dikonfirmasi dalam rantai longest. Profitabilitas penambangan egois tidak mengacu pada surplus bahwa hadiah blok mengurangi biaya perhitungan kriptografi. Bahkan, ini adalah ukuran kontras dengan penambangan jujur yang membutuhkan indeks objektif.

Definisi Kedua (profitability) *Penambangan egois atau strategis yang dilakukan oleh Alice (resp. Bob) dianggap*
menguntungkan jika pendapatan relatif lebih tinggi dari kekuatan Hash yang dinormalisasi, yaitu Rˆa *> α* 1 *(resp.* Rˆb > α 2).

Penyesuaian kesulitan seperti bitcoin adalah Inti dari penambangan Bitcoin adalah untuk memecahkan
teka-teki kriptografi. Header blok terutama mencakup Hash dari blok sebelumnya, Hash root Merkle transaksi, waktu awal menghitung hash header, nBits yang digunakan untuk menghasilkan kesulitan target dan *NONCE*.