Summary Blockchain Mining with Multiple Selfish Miners

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. 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.

Setelah kita mengetahi apa itu penambang egois, kita perlu solusi untuk mencegah adanya penambang egois. 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 yangmembutuhkan indeks objektif. 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*.