Pada paper on profitablity of selfish mining membahas tentang selfish mining strategy dalam Bitcoin network dan mengevaluasi dengan benar biaya serangan dan profitabilitasnya Yang diharapkan durasi serangan telah diabaikan dalam literatur tetapi sangat penting. Dalam paper ini membuktikan bahwa strategi tersebut hanya dapat menguntungkan setelah penyesuaian kesulitan. Karena itu serangan terhadap algoritma penyesuaian kesulitan. Serta dalam paper ini mengusulkan perbaikan protokol Bitcoin mebuatnya kebal terhadap serangan penambangan yang egois.

Selfish Mining merupakan strategi penambang menyimpangan yang dijelaskan dalam operator penambangan besar menahan blok yang ditambang dan melepaskannya dengan strategi tepat waktu untuk membatalkan jumlah maksimum blok yang ditambang oleh sisa jaringan.

Pada paper ini menjelaskan selfish mining attack mulai dari validasi dan blok nya tidak di broadcast kemudian melajutkan penambang secara diam-diam pada atas blok ini. Selanjutnya dia melanjutkan proses berikut :

1. Jika selfish miner hanya sama 1 blok dan honest miner menemukan blok kemudian selfish mining segera menyebarkan blok dia tealh menambang secara diam-diam.
2. Jika selfish miner adalah 2 blok dan honest miner menemukan satu blok, lalu selfish miner segera menyiarkan dua blok yang dia miliki ditambang secara rahasia. Kemudian, seluruh jaringan berganti
3. Jika selfish miner lebih besar dari 2 maka selfish miner melepaskan blok segra setelah honest miner menemukannya.
4. Dalam kasus lain, selfish miner terus menambang secara diam diam.

Selfish miner merupakan trik yang memperlambat jaringan dan mengurangi penambang kesulitan. Serangan itu mengrangi profitablitas penambang yang jujur dan salah satu dari selfish miner sebelum penyesuaian kesulitan. Selfish miner hanya menjadi menguntungkan setelah menurunkan tingkat kesulitan. Cara lain untuk mencapainya adalah dengan memundurkan dari jaringan dan mulai menambang cryptocurrency lain dengan hashing uang sama fingsi.

Ther origin of problem : Pada dasarnya, Serangan itu memanfaatkan hukum penyesuaian kesulitan.

Formula penyesuaian kesulitan baru. Untuk mengurangi serangan ini, idenya adalaha untuk memasukan jumlah blok dalam rumus penyesuaian kesulitan

$$D_{\text{new}} = D_{\text{old}} \cdot \frac{(n_0 + n')\tau_0}{S_{n_0}}$$