Nama : Muh Nardika

NIM : 1103184124

Kelas : TK-42-PIL

ON PROFITABILITY OF SELFISH MINING

Selfish Mining

Selfish Mining is a method for increase the upgrade by not playing fair. Selfish Mining attack too known as a slashing attack, depicting a malicious attempt to discredit network integration blockchain.

Selfish Mining defines a mechanism for miners to cooperate and increase their profits by creating separate forks and not revealing mined blocks throughout network. This has an impact on overall health protocols, due to collusion increase the risk of centralization. Bitcoin mining is based on a number of factors, including, but not limited to, mining machine efficiency, electricity costs and hash power donated to the network. Its design ensures decentralization by providing rewards for individual miners on the blockchain, which is one of the reasons mining pool popularity because it allows miners to receive ongoing and consistent reward.

However, miners can greatly optimize mining and increase yield by engaging in selfish mining. If they stop declaring blocks new to the public network, it can make the process run faster and reduce resource wasting day

Basic Selfish Mining

The mining procedure consists of two cases as follows.

• (Public-chain mining case) Henry always mines after the public chain. Alice or Bob also mines on the public chain if it is longer than his private chain.

• (Private-chain mining case) Alice (resp. Bob) continues to mine on her (resp. his) private chain if she (resp. he)

discovers a new block and the private chain is now longer
than the public chain. The release procedure is more complicated than the mining procedure. Henry broadcasts his mined block as soon as it is discovered, while Alice and Bob will decide whether to release their mined blocks depending on the length of the public chain.

• (Forfeit case) Alice (resp. Bob) abandons her (resp. his) private chain and conforms to mining after the public chain if the latter is longer. Henry also abandons his public chain if Alice or Bob publishes a longer chain.

• (Risk-avoiding release case) Alice (resp. Bob) releases her (resp. his) privately mined blocks to the public because of the fear of loss if the new block is mined by the others and the leading advantage of her private chain is no more than two blocks.

• (Chain reaction case) When Alice (resp. Bob) releasesher (resp. his) blocks to the public chain and updates its length, the release of Bob's (resp. Alice's) private blocksis triggered immediately.

Proposition to Prevent Selfish Mining

a. ***The origin of the problem***.
   Basically, the attack took advantage of justice law. The protocol underestimates the actual hashing power on the network because only the blocks that are on the (official) blockchain are taken into account. That the number of orphan blocks increases in the face of selfish and significant miners the honest amount of hashrate is gone. Average time it takes the network to validate block increases. After the 2016 block, the adjustment of the adjustment is done automatically Improve orphan block production. despite the fact that the total hashing the network remains the same, the new difficulty of the power is lower than it should be, and block validation time is reduced. So income per unit time from egoist miners upgrade and make the attack profitable.

b. ***Difficulty Adjusment Formula***.
   To mitigate this attack, the idea is to incorporate the count of orphan blocks in the difficulty adjustment formula. This can be implemented with miners indicating the presence of "uncles' in the blocks they mine by including their header and peers relaying this data. Nodes would not need to broadcast whole orphan blocks but only their headers. It is possible to incentive miners to include proofs of existence of uncles in their blocks by including a rule that, in case of competition between two blocks with the same height, nodes should always broadcast the block with the most proof-of-work i.e.,

Conclusion

Selfish mining is an attack on the Bitcoin protocol, but the arguments present in the literature do not properly justify the attack. They lack of a correct evaluation of the cost of the attack and a proper analysis of profit and loss per unit of time. To compare the profitability of different mining strategies one needs to compute the average length of their cycles and their profitability ratio, that is a new notion introduced in this article.