Name : Gihon Godwin Silitonga

Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack

Decentralized cryptocurrencies like Bitcoin and other altcoins have captured the public's interest, and have been much more successful than any prior incarnations of electronic cash. Many would call the rise of these electronic currencies a technological revolution, and the "wave of the future".

There is Modeling of Bitcoin Mining:

- Defining Key Parameters
  We represent the attacker and the rest of the network only in aggregate; our model does not distinguish between the various separate entities (e.g., mining pools, industrial mining operations) that constitute the network.
- Markov Chain Model of Mining
  Model Bitcoin mining using a Markov decision process, where the state captures relevant aspects of the information available to Alice and Bob, and the transitions occur when Alice or Bob find a new block.
- Expressing Honest and Selfish Mining
  The net effect of selfish mining is to "waste" mining power on blocks that eventually get discarded. Sometimes Alice spends effort to no avail and her private chain falls behind Bob's; on other occasions, Bob wastes work while Alice is already ahead.
- Revenue Gain
  The relative gain of selfish mining (SM) strategy compared to a honest strategy (H) is defined as: relative gain(SM, H) = gainSM − α α More generally, given strategies X and Y , the relative gain of X over Y is defined as: relative gain(X, Y) = gainX − gainY α.
- Plausible Choices of α and γ
  Plausible values for α. As mentioned earlier, α is the fraction of the attacker's hashpower relative to the entire network. Meanwhile, Plausible values for α. As mentioned earlier, α is the fraction of the attacker's hashpower relative to the entire network.

  Detecting and inferring attacks. Eclipse attacks and stub□born mining can likely be detected if they occur in practice. One way is by observing the stale block rate – a stale block is one that has valid transactions and proof-of-work, but is ultimately excluded from the main chain