SD5 Coalition Strategy Explanation

April 29 2021

Motivation

This strategy aims to abuse the bank's policy of accepting a miner's payment as soon as the spend operation is in the unique longest chain. This allows colluding miners to double spend all of their currency as quickly as every other new block by never mining on top of a chain where the coalition miners have spent their currency.

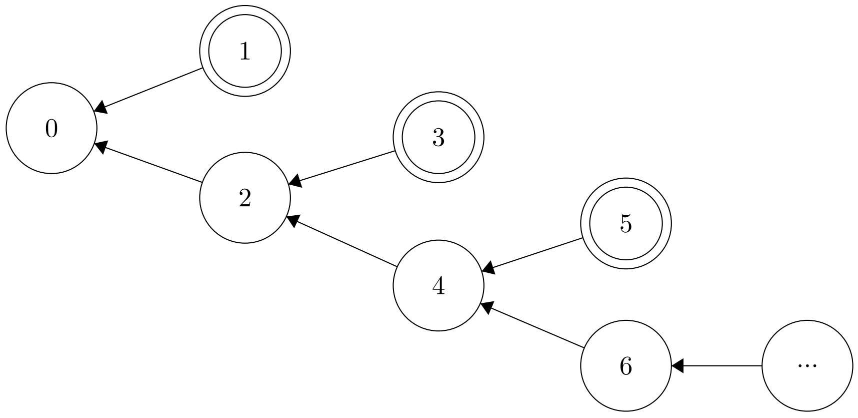
Example Trace

Assume all miners choose which block to mine on using the following protocol:

- Find the blocks where the miner has the most stake, not counting the most recent bribe
- Among those blocks, choose the highest block
- Earlier blocks win ties

Whenever the block chosen by the above protocol is a highest block, then the miners spend all of their available currency. Otherwise, they spend nothing. No bribes are used.

The first few rounds will produce blocks connected in the following fashion, with double circles indicating rounds on which the miners spend:



The production of an odd-numbered block B will give a unique longest chain, so all miners spend everything. This means that the previous block $P(B)$ will become the block with the highest stake that is the longest for all miners, so the next produced block with have the same height as B, but the miners will have at least their entire starting funds, so that new block will be mined on top of. The cycle continues indefinitely, allowing the miners the double spend every other round.

Exploitability

All miners using (essentially) the above strategy is a Nash equilibrium. There is clearly no profitable deviation from the spending habits, since the miners spend all currency exactly when the next block will temporarily be on the unique longest chain (odd-numbered rounds) and never spend currency when the next block will be on the longest chain at the end of the game (even-numbered rounds). In terms of mining during odd-numbered rounds, a miner only loses utility from mining on a different block by delaying the rounds until they are next able to double spend. This is because all other miners will spend all of their currency on the mined block, so none of the other miners will ever mine on top of that block for the rest of the game. For even-numbered rounds, the miner's block will become part of the eventual longest chain, and mining on top of a different block will not lead to the block being in the eventual longest chain, so the miner does not profit from deviating. This shows that if all other players are following the coalition strategy, the unique best response is to also follow the coalition strategy.

For the finite version of this game that ends on an even round, there is an issue that it is better for the final miner to mine of top of the previous odd block as opposed to the previous even block. This will not impact actions in any earlier rounds, though. Since this addition to the strategy will not meaningfully impact the expected utility, it has been omitted from the coalition strategy implementation for the sake of simplicity.

Robustness

The strategy outlined with slight alterations may give a symmetric subgame perfect equilibrium, but it seems tedious to prove it rigorously. The important fact is that as long as $> 50\%$ of the miners are true coalition, the coalition strategy still functions as intended.

Assume there are some number of blocks in the longest chain past where coalition miners spent all of their currency. This will occur for instance when there are longest miners in the network. That chain cannot remain the longest indefinitely. The coalition miners will never build on that chain and instead add to a chain beginning directly before where they all spent their currency. This means the coalition miners will play catch up using a chain on which they have not spent any currency.

Additionally, it is important to note that the block chosen to mine on will be the same among all coalition members. The miners all spend on the same rounds, and since bribes are not considered, the stake before spending must always be strictly larger than the stake after spending. The block selected will always be the longest chain originating on previous block to the most recent block the miners spent on that does not use any blocks the miners spent on. Removing the most recent bribe is required, since in the case where a bribe plus mining reward gives a coalition miner as least as much stake than they spent, that miner will incorrectly determine when to spend their currency.

Written by Liam Johansson with input from Anthony Hein and Ken Oku