poco - proof of chosen ones (preliminary abstract)

Nico Verrijdt
nicoverrijdt@gmail.com

May 16, 2021

Abstract

There are issues with consensus algorithms like bitcoin's proof-of-work and cardano's proof-of-stake which were meant to be superseded in a rather young research and development field like blockchain. Those known issues, a major issue that is the huge energy waste in the case of bitcoin and a rather minor issue in the case of cardano where rewards are given to the most important stakeholders (read: rich user gets richer). The latter issue might be an idealistic point of view but fairness among users in a system should be a design that lasts longer without needs to do major improvements/adaptations.

And so the poco consensus algorithm - proof of chosen ones - was invented and which goal it is to address above issues. Swiftly introduced poco divides all the users in 100 buckets, dynamically established, and each bucket also consists of multiple layers who grow hundredfold going deeper. The top layer are the hundred 'chosen ones' and they are headed by a coordinator.

Mining blocks is somehow a game of probabilities in the network of users and the most probable block will become the final block. Explained shortly, every iteration (fxed delay) in the mining process involves calculating multiple final block candidates. The faster a certain block is calculated and verified by the chosen ones, the greater the chance of becoming a final block. As there are multiple candidates in multiple layers/iterations and each block is based (chained) on their previous block, a filtering process is going on through the iterations until a candidate remains as the sole candidate in its layer, which means a new block is minted.

Energy consumption for poco is limited to computing the blocks, but the total amount of blocks that need to be calculated are also limited because later calculations won't have an improved probability of becoming the final block. It is indeed survival of the fittest and not a mass event. Ddos prevention also determines the total amount of calculated blocks.

The chosen ones are selected quasi ad random (introducing fairness), the seed for deciding the chosen ones is the hash of the subjected block, and these chosen ones included in a minted block are the only users who get rewarded . These rewards are the only means of growing the total amount of coins and there is no limit on the total amount of coins.

Keywords: blockchain; poco; proof of chosen ones;