Cluster Computing
https://doi.org/10.1007/s10586-022-03746-5

Cooperative hybrid consensus with function optimization for blockchain

Mohammadreza Ipchi Sheshgelani[1] · Saeid Pashazadeh[1] · Pedram Salehpoor[1]

Received: 15 February 2022 / Revised: 2 July 2022 / Accepted: 10 August 2022

Abstract
Blockchain-based consensus methods such as PoW (Proof of Work) and PoS (Proof of Stake) are widely used and favored these days, but each has disadvantages. One of the significant issues PoW encountered with it is wasting a large amount of energy. PoW faces environmental protection problems and has serious opponents. To address this problem and others, we propose a cooperative hybrid consensus method that uses PoW initially, followed by PoS to choose a leader for adding the block to the blockchain. We change the primary hash calculation in PoW with function optimization. Our protocol provides a cooperation mechanism to collaborate with decentralized nodes. Every node that works fine gets a reward for its cooperation. To evaluate the performance of the proposed method, we simulated it using different benchmark functions. Simulated experiments demonstrate that our proposed protocol successfully performs optimization with the iteration-best measurement. Also, we proposed the security analysis of our protocol. The security analysis and experimental results represent that our proposed protocol is appropriate in practice.

Keywords Consensus · Metaheuristic function optimization · Distributed computing · Blockchain

1 Introduction

The invention of blockchain is one of the most inspiring technologies of the last decade. Bitcoin is the first and most important application of the blockchain. Bitcoin was introduced to securely transmit currency between two endpoints with no trusted third party. In addition to the cryptocurrency field, the other achievement of Bitcoin is to solve the Byzantine generals' Problem using consensus. The consensus method used in Bitcoin is named Proof of Work. In PoW participants, we call them miners, race each other to solve a puzzle. The advantage of miners is proportional to their hardware power, which we call hash rate. Which miner solves the mathematical puzzle can add the block to the blockchain and earn the reward. PoW consensus [1] method works fine and is practically proven to be correct, but it has problems:

- Powerful hardwares are working an uninterrupted way to solve the puzzle, but this working is useful for the consensus protocol only.
- The electricity power consumption of the network is an environmental problem. According to [2, 3], in July 2021, the Bitcoin energy consumption amount is 148.10 TWh which is comparable to the electricity consumption of Malaysia.
- The basic idea of Nakamoto [4] is one-CPU-one-Vote, which is now impractical due to intense competition, and only powerful ASICs can have a chance of winning rewards. This problem caused to direct the mining to an industrial process.

Mentioned problems cause researchers to try to find alternative consensus methods rather than PoW. One of the most noteworthy alternatives is PoS [5]. In PoS mining, selecting probability is proportional to stake amount. Both PoW and PoS have advantages and disadvantages, so hybrid methods were introduced to cover each other.

✉ Saeid Pashazadeh
pashazadeh@tabrizu.ac.ir

Mohammadreza Ipchi Sheshgelani
m.ipchi@tabrizu.ac.ir

Pedram Salehpoor
psalehpoor@tabrizu.ac.ir

[1] Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Published online: 22 September 2022