INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

A Truly Decentralized Consensus Protocol that Eliminates Tendency towards Centralization

A Dissertation by

Mr. Kumudu Kesara Wimal

Supervised by

Mr. Geethapriya Liyanage

Submitted in partial fulfillment of the requirements for the MSc in Advanced Software Engineering degree at the University of Westminster.

May 2023

Abstract

The consensus protocol is a crucial element of blockchain technology that guarantees all participants agree on the same data values and follow the same direction, even in the presence of defective components. This research project has identified a problem that affects both users of blockchain technologies and investors in cryptocurrencies. The question of whether current blockchain platforms are truly decentralized has been raised by the blockchain community over the years. The most popular blockchains use Proof of Work (PoW), Proof of Stake (PoS), or a combination of both, but both systems have limitations in terms of decentralization. Several alternative consensus protocols have emerged recently, but none have achieved total decentralization or welcomed any level user to be the next miner or forger.

Therefore, true decentralization of a blockchain system is more challenging as most of the popular consensus protocols were invented to accommodate decentralization but eventually, driven by the centralization of power. This research study proposes a truly decentralized consensus protocol that is capable to avoid the centralization of power even in the future regardless of the number of network participants. The protocol also makes sure it avoids the use of specialized hardware resources, decreases the level of energy consumption, and encourages network activities. Additionally, the new consensus protocol offers a more democratic and fair approach to blockchain consensus.

Furthermore, the implemented solution underwent comprehensive testing to ascertain its level of decentralization. Considering the lack of a suitable metric for evaluating the practical extent of decentralization achieved by a blockchain system, this study adopted a set of requirements delineated in a prior investigation. Based on this assessment, it was determined that the solution has successfully attained genuine decentralization. Moreover, the test results demonstrate that the solution has achieved enhancement in terms of security and performance, thereby ensuring its effectiveness in circumventing the need for specialized hardware and reducing energy consumption.

Keywords: Blockchain, Consensus protocol, Distributed ledger technology, Decentralized network, Incentive, Security