Enhancing Alternative Proof of Work for Cryptocurrencies Using Machine Learning*

Faculty Poster Abstract

Sajedul Talukder[1] *and Abdur R. Shahid*[2]
[1]*Southern Illinois University*
Carbondale, IL 62901
sajedul.talukder@siu.edu
[2]*Robert Morris University*
Moon Township, PA 15108
shahid@rmu.edu

Abstract

Blockchain consensus refers to the process of validating the network's status by guaranteeing that all blocks include the same information and have the correct values across all nodes. A cryptocurrency, often known as "crypto," is digital money that uses the Proof of Work (PoW) method to establish consensus. PoW is used by popular cryptocurrencies like Bitcoin to establish consensus, which is a time-consuming and resource-intensive procedure. Miners expend a lot of energy to perform a brute-force search for the desired hash value using a nonce that isn't helpful otherwise, in order to add a block of transactions to the blockchain. A nonce is a one-time-use value that, when appended to a block and hashed, ensures that the output of the block hash begins with the correct number of zeros. In this paper, we present machine learning-based methods that give a quicker means of establishing consensus and create a template for Proof of Work protocols that ensure similar security guarantees as Bitcoin. To forecast the nonce value from block headers properties, we utilize a mix of multi-layer perceptrons (MLP) and recurrent neural networks (RNN). Our approach minimizes the protocol's time and energy usage by quickly determining the correct nonce value while maintaining security and decentralization.