AN EVALUATION OF BLOCKCHAIN CONSENSUS ALGORITHMS

Dr. Shambhu Bhardwaj*

*Associate Professor,
Department of Computer Science, Faculty of Engineering,
Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, INDIA
Email id: shambhu.bhardwaj@gmail.com

ABSTRACT

Cryptocurrencies have exploded in popularity, and underlying them is an innovative technology known as blockchain: a distributed digital ledger in which bitcoin transactions are recorded once they have been validated. Many clients or "validators" inside the cryptocurrency's peer-to-peer network verify transactions within a ledger using one of many different consensus methods for addressing the issue of dependability in a network containing multiple faulty nodes. The Proof of Work (PoW) and Proof of Stake (PoS) algorithms are the most commonly used consensus algorithms; however, there are additional consensus algorithms that employ alternate PoW and PoS implementations, as well as hybrid implementations and even entirely new consensus methods. We compare and contrast traditional consensus algorithms with some of its contemporaries that are presently in use in contemporary blockchains in this article. Our investigation focuses on the algorithmic steps performed by each consensus algorithm, as well as the algorithm's scalability, the manner by which validators are compensated for their time spent confirming blocks, and the system's security concerns. Finally, we discuss our findings as well as some potential future trends in blockchain consensus algorithms.

KEYWORDS: *Blockchain, Consensus Algorithms, Consensus, Cryptocurrency, Network.*

REFERENCES

1. P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," 2017, doi: 10.1109/COMPTELIX.2017.8003959.

2. P. Waelbroeck, "An Economic Analysis of Blockchains," CESifo Work. Pap. Ser., 2018.

3. G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," J. Inf. Process. Syst., 2018, doi: 10.3745/JIPS.01.0024.

4. J. Wang, "A simple Byzantine Generals protocol," J. Comb. Optim., 2014, doi: 10.1007/s10878-012-9534-3.

5. T. Distler, C. Cachin, and R. Kapitza, "Resource-Efficient Byzantine Fault Tolerance," IEEE Trans. Comput., 2016, doi: 10.1109/TC.2015.2495213.

6. Y. Hu, Y. Xiong, W. Huang, and X. Bao, "KeyChain: Blockchain-based key distribution," 2018, doi: 10.1109/BIGCOM.2018.00027.

7. N. Houy, "'It will cost you nothing to 'kill' a proof-of-stake crypto-currency," Econ. Bull., 2014, doi: 10.2139/ssrn.2393940.

8. D. Mazieres, "The Stellar consensus protocol: A federated model for Internet-level consensus. url:https://www.stellar.org/papers/stellar-consensusprotocol.pdf," Stellar Dev. Found., 2016.

9. X. Fan and Q. Chai, "Roll-DPos: A randomized delegated proof of stake scheme for scalable blockchain-based Internet of Things systems," 2018, doi: 10.1145/3286978.3287023.

10. L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 2018, doi: 10.23919/MIPRO.2018.8400278.

11. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017, doi: 10.1109/BigDataCongress.2017.85.