Consensus algorithms in blockchain must be cared for achieving the robust system

yoshiyasu takefuji[1]

[1]Affiliation not available

November 11, 2020

Abstract

Tushar W. et al. wrote a review paper on negawatt trading using blockchain technology. In their paper, four consensus algorithms in blockchain are introduced. They should address known security issues of the existing consensus algorithms in blockchain for robust system. In order to use the blockchain technology, detection and protection mechanisms must be embedded in blockchain applications for protecting vulnerabilities of known consensus algorithms.

RATIONALES

Tushar W. et al. wrote a review paper on negawatt trading using blockchain technology[1]. In their paper, they introduced consensus management used in the blockchain technology. In the consensus management[1,2], four consensus algorithms are introduced: proof of work, proof of stake, voting based, authority based, in addition to practical byzantine fault tolerance[1,3]. Although the security problems lie in the existing consensus algorithms within the blockchain, such significant security issues must be addressed in their review paper.

As far as we know, the decentralized consensus algorithms are all vulnerable against known attacks including a 51% attack, long range attack, DDoS attack, P+Epsilon attack, Sybil attack, balance attack, and BGP hijacking respectively[4,5]. In other words, blockchain developers and users must understand the vulnerabilities of the existing consensus algorithms in blockchain. Vulnerability issues in the blockchain consensus algorithms were detailed[6].

Tushar W. et al. should address known security issues of consensus algorithms in blockchain. In order to use the blockchain technology, detection and protection mechanisms must be embedded in blockchain applications for protecting vulnerabilities of known consensus algorithms.

References:

1. Tushar W. et al., Challenges and prospects for negawatt trading in light of recent technological developments. Nat Energy (2020).

https://doi.org/10.1038/s41560-020-0671-0

2. N. Ul Hassan, C. Yuen and D. Niyato, "Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges, and Solutions," IEEE Industrial Electronics Magazine, vol. 13, no. 4, pp. 106-118, Dec. 2019, doi: 10.1109/MIE.2019.2940335.

3. M. F. Zia et al., "Microgrid Transactive Energy: Review, Architectures, Distributed Ledger Technologies, and Market Analysis," IEEE Access, vol. 8, pp. 19410-19432, 2020, doi: 10.1109/ACCESS.2020.2968402.

4. Sayeed, S.; Marco-Gisbert, H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. Appl. Sci.2019,9,1788.

5. Yang, F.; Zhou, W.; Wu, Q.; Long, R.; Xiong, N. N.; Zhou, M. Delegated Proof of Stake with Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism.IEEEAccess2019,7, 118541-118555.

6. Yoshiyasu Takefuji, Security Protection Mechanisms Must Be Embedded in Blockchain Applications, *Journal of Chemical Education***2020** *97* (7), 1819-1820

DOI: 10.1021/acs.jchemed.0c00040