A consensus mechanism must be cared for protecting blockchain against attacks

yoshiyasu takefuji[1]

[1]Affiliation not available

October 23, 2020

Abstract

Telenti A. et al. wrote a perspective on treating medical data as a durable asset using blockchain and AI technology[1]. In order to use the blockchain technology, detection and protection mechanisms against attacks must be embedded in blockchain applications for protecting vulnerabilities of known consensus algorithms.

RATIONALES

Telenti A. et al. wrote a perspective on treating medical data as a durable asset using blockchain and AI technology[1]. It is not so easy to use the blockchain technology for securely storing medical data as they mentioned. McAfee disseminated "blockchain threat report."[2] Charles McFarland wrote an article entitled "Threat Report: Don't Join Blockchain Revolution Without Ensuring Security."[3] Blockchain news, scams, vulnerabilities, malware, and research are reported respectively[4]. 10 blockchain and new age security attacks are introduced.[5] Yves Longchamp et al. questioned on the blockchain security.[6]

The main security problem lies in a consensus mechanism used in blockchain. According to Investopedia[7], "a consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record-keeping, among other things."

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.[8,9] In order to use the blockchain technology, detection and protection mechanisms must be embedded in blockchains for protecting known vulnerabilities of consensus algorithms against attacks.

CONCLUSION

In order to securely store medical data using the blockchain technology, protection mechanisms are needed for protecting known vulnerabilities of the existing consensus algorithms.

References:

1. Telenti, A., Jiang, X. Treating medical data as a durable asset. Nat Genet 52, 1005–1010 (2020). https://doi.org/10.1038/s41588-020-0698-y

2.https://www.mcafee.com/enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf

3.Charles McFarland, Threat Report: Don't Join Blockchain Revolution Without Ensuring Security,*https://www.mcafee.com/blogs/other-blogs/mcafee-labs/threat-report-dont-join-blockchain-revolution-without-ensuring-security/*

4.*https://blockthreat.substack.com/*

5.Aruba Marketing,10 Blockchain and New Age Security Attacks You Should Know https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/

6.Yves Longchamp et al., Are blockchains that safe? How to attack them and how to prevent these attacks, Sept. 2020,*https://www.seba.swiss/research/are-blockchains-safe-how-to-attack-them-and-prevent-attacks*

7.*https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp*

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

9. 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.