European Journal of Human Genetics
https://doi.org/10.1038/s41431-020-0597-9

CORRESPONDENCE

Detection and protection mechanisms against vulnerabilities are needed in blockchain applications

Yoshiyasu Takefuji[1]

Received: 9 January 2020 / Accepted: 19 February 2020

To the Editor:

The paper mentioned about a POW (Proof Of Work) consensus algorithm in the blockchain system. I thought that Dwarna uses the POW algorithm so that they need the strong protection against known seven attacks. POW and other consensus algorithms are known to be vulnerable to the known attacks. Dwarna uses X.509 protocol instead of the existing consensus algorithms. However, detection and protection mechanisms against X.509 vulnerabilities are needed in blockchain applications.

Mamo et al. wrote an article entitled "Dwarna: a blockchain solution for dynamic consent in biobanking" [1]. The authors did not show any mechanisms of detection and protection against blockchain consensus attacks in the paper. As long as blockchain consensus algorithms are used in applications, we must provide detection/protection mechanisms against malicious attacks. There are unknown attacks and known attacks against blockchain consensus algorithms [2]. The existing consensus algorithms are POW, POS (Proof Of Stake), DPOS (Delegated Proof of Stake), RPCA (Ripple Protocol Consensus Algorithm), and SCP (Stellar Consensus Protocol). As far as we know, there is no perfect protection against POW and other consensus algorithms. Known attacks are 51% attack, Long Range attack, DDoS attack, P+Epsilon attack, Sybil attack, Balance attack, and BGP Hijacking respectively. However, the authors informed me that Dwarna uses X.509 protocol instead of the existing consensus algorithms which was not mentioned in the paper. X.509 protocol is de facto standard for public key infrastructure. They need to embed the necessary protection against X.509 vulnerabilities because they are listed in top 5 open source vulnerability (https://securityboulevard.com/2019/12/top-5-new-open-source-security-vulnerabilities-in-november-2019/).

Compliance with ethical standards

Conflict of interest The author declares that he has no conflict of interest.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References

1. Mamo N, Martin GM, Desira M, Ellul B, Ebejer J-P. Dwarna: a blockchain solution for dynamic consent in biobanking. Eur J Hum Genet. 2019. https://doi.org/10.1038/s41431-019-0560-9.
2. Takefuji Y. AI's role in cryptocurrencies and blockchain applications, keynote in ITT (information technology trends). 2019. UAE. http://itt.hct.ac.ae/technical-program/keynote-speakers/.

✉ Yoshiyasu Takefuji
takefuji@keio.jp

[1] Environment and Information Studies, Keio University, Fujisawa, Kanagawa 2520882, Japan

Published online: 02 March 2020