European Journal of Human Genetics (2020) 28:696
https://doi.org/10.1038/s41431-020-0598-8

CORRESPONDENCE

Reply to Y. Takefuji

Nicholas Mamo[1] · Gillian M. Martin[1,2,3] · Maria Desira[1] · Bridget Ellul[4] · Jean-Paul Ebejer[1]

Received: 7 February 2020 / Accepted: 19 February 2020 / Published online: 2 March 2020

We would like to thank Prof. Takefuji for his interest in our publication. We agree in principle with the issues raised in the correspondence: security is important to guard against malicious attacks and to protect research partner data.

However, Dwarna does not use the Proof-of-Work (PoW) consensus mechanism. This is made amply clear when we discuss Hyperledger Composer in the Related Work Section. Later, in the Implementation section, we explain how we are using Hyperledger Composer.

Hyperledger Composer is based on the Hyperledger Fabric blockchain: a permissioned blockchain that requires network peers to be authenticated before effecting any transactions. Thus, instead of the PoW consensus mechanism, Hyperledger Fabric adopts a less intensive workflow using X.509 certificates [1–4].

This avoids the security threats associated with PoW that are listed in Prof. Takefuji's correspondence. As noted, the X.509 protocol is used ubiquitously (e.g., in protocols TLS/SSL, HTTPS, S/MIME, EAP-TLS, used for WI-FI connectivity, email, ecommerce, secure web browsing, etc.), placing it under rigorous scrutiny. It should be noted that ref. [5], mentioned in Prof. Takefuji's correspondence, flags an issue not with X.509 itself, but with certificate parsing in certain versions of the Python programming language. This vulnerability has no relevance to the Dwarna system we described.

As explained more thoroughly in the article, we take additional measures to ensure data privacy and security. Hyperledger Fabric network peers are only created in the backend. As explained in our article, Hyperledger Composer identities for research partners can only be issued through the REST API, itself only accessible from the WordPress plugin.

Furthermore, we discuss other security and privacy challenges (STRIDE and LINDDUN models) and how Dwarna tackles them in the manuscript's Supplementary information.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

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

References

1. Hyperledger. Transaction Flow. 2020. Available at: https://hyperledger-fabric.readthedocs.io/en/latest/txflow.html. Accessed 28 Jan 2020.
2. Hyperledger. What is Hyperledger Fabric? 2020. Available at: https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html#what-is-hyperledger-fabric. Accessed 28 Jan 2020.
3. Hyperledger. Why Hyperledger Fabric? 2020. Available at: https://fabrictestdocs.readthedocs.io/en/latest/whyfabric.html. Accessed 28 Jan 2020.
4. Hyperledger. Identity. 2020. Available at: https://hyperledger-fabric.readthedocs.io/en/latest/identity/identity.html. Accessed 4 Feb 2020.
5. Johnson P. Top 5 New Open Source Security Vulnerabilities in November 2019. 2019. Available at: https://securityboulevard.com/2019/12/top-5-new-open-source-security-vulnerabilities-in-november-2019/. Accessed 27 Feb 2020.

✉ Jean-Paul Ebejer
jean.p.ebejer@um.edu.mt

[1] Centre for Molecular Medicine and Biobanking, Biomedical Sciences Building, University of Malta, Msida MSD 2080, Malta

[2] Department of Sociology, Faculty of Arts, University of Malta, Msida MSD 2080, Malta

[3] BBMRI-ERIC, Neue Stiftingtalstraße 2/B/6, 8010 Graz, Austria

[4] Department of Pathology, Faculty of Medicine and Surgery, University of Malta, Msida MSD 2080, Malta