Letter to the Editor | Open Access

DMMS: A Decentralized Blockchain Ledger for the Management of Medication Histories

Patrick Li[1], Scott D. Nelson[2], Bradley A. Malin[3], You Chen[4]

[1]Computer Science, Saratoga High School, Saratoga, CA, USA; [2]Department of Biomedical Informatics, Vanderbilt University Medical Center, Nashville, TN, USA; [3]Department of Biomedical Informatics, Vanderbilt University Medical Center, Nashville, TN, USA; [4]Department of Biomedical Informatics, Vanderbilt University Medical Center, Nashville, TN, USA

Blockchain in Healthcare Today, January 4, 2019. © The Author(s). 2019

The original article was published in *Blockchain in Healthcare Today*. DOI: https://doi.org/10.30953/bhty.v2.38

Section: Use Cases/Pilots/Methodologies

Keywords: Blockchain Ledger, Decentralized, Hyperledger Fabric Framework, Medication. Histories

Sirs,

Regarding the letter writer's first point, we do not agree with the opinion the authors proposed. As we stated in our paper, medication management and exchange across health institutions can bring great benefits for patients, payers and healthcare organizations. We admin that there are barriers to achieve the goals of secure and trustworthy medication exchanges. That is also the reason why we need to conduct research to remove these barriers. As we discussed in our paper, we can make connections between nodes in DMMS network and EHR systems to avoid duplicative works.

We think the authors' proposed comprehensive and modular EHR still cannot solve the secure and trust problem raised by centralized system. If authors want to implement a decentralized EHR system, then they will face many big challenges such as a variety of healthcare processes and complex workflows. That is also the reason why we only considered secure and trustworthy medication management as a pilot study.

On page 4, we acknowledged that we did not use a precise term here. Instead of using the term "definition," we can state the differences between public and private blockchain as: "There are several distinctions between public and private blockchains, which often display properties of permissionless and permissioned blockchains respectively"

Additionally, according to the Hyperledger website "Hyperledger Fabric is an open source enterprise-grade permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts, that delivers some key differentiating capabilities over other popular distributed ledger or blockchain platforms." It is highly customizable but mostly within the scope of private business-centered applications. I believe our definition of it is correct in the paper.[1]

We agree and apologize on page 5 that we did not conduct an intensive investigation on Etherium network during the study of the work. Thank you for this critique, we can specify this further in our paper.

On page 6 of our article, the reason we call patients assets is because that is the naming convention for hyperledger composer data structure. In the hyperledger fabric framework, there are three main categories as explained: Assets, Participants, and Transactions. In this business network, patients display properties most related to those of assets described in the hyperledger composer structure, which is why we categorize patients as assets. Of course, patients will not be treated in the traditional term of assets as that would be highly unethical. [2]

Thank you for this critique on page 7, we can change "breach" to "intrusion"

Regarding the statement on page 9, as we stated in our paper, DMMS is independent on the EHR systems. All the data generated and transferred within the DMMS network are secure and trustworthy. To avoid providers prescribing medication

The way private keys, as noted on page 10 of our article, are stored is very similar with the way the online cryptocurrency wallets managed by cryptocurrency exchange platforms. The private keys in our study are managed and maintained by nodes in the DMMS network, and only permissioned nodes can join the network, thus the private keys in the DMMS are more secure than the private keys of the online cryptocurrency wallets.

On orders in both DMMS network and EHR systems, we discussed a potential solution to connect the two systems.

To the best of our knowledge, third-party EHR vendors do not actually store any EHR data generated by private healthcare organizations. If they plan to store or maintain data coming from private healthcare organizations, the data should be in an encrypted manner to avoid private information leaking.

Sincerely,

You Chen, PhD

References

1. Introduction. Hyperledger Fabric. 2019. Available at URL: https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html
2. Introduction. Welcome to Hyperledger Composer. Accessed 2019: https://hyperledger.github.io/composer/v0.19/introduction/introduction