

Preserving Decentralized EHR-s Integrity

Marten KASK^{a,1}, Toomas KLEMENTI^a, Gunnar PIHO^b and Peeter ROSS^a

^aTalTech, Dept. of Health Technologies, Akadeemia Str 15A, Tallinn, 12618, Estonia

^bTalTech, Dept. of Software Science, Akadeemia Str 15A, Tallinn, 12618, Estonia

ORCID ID: Marten Kask <https://orcid.org/0000-0001-5437-783X>,

Toomas Klementi <https://orcid.org/0000-0002-8260-526X>,

Gunnar Piho <https://orcid.org/0000-0003-4488-3389>,

Peeter Ross <https://orcid.org/0000-0003-1072-7249>

Abstract. A blockchain and decentralized storage technology-based architecture is proposed to support the integrity of Electronic Health Records (EHRs).

Keywords. blockchain, Hyperledger Fabric, Electronic Health Record, integrity

1. The Proposed Architecture

Several studies have researched the issues related to data integrity and concluded that blockchain-based technology could significantly increase data integrity in the health data domain [1]. We propose a solution (Figure 1) that uses Hyperledger Fabric technology [2] and decentralized storage [3] to preserve the integrity of EHRs where at least two different organizations (e.g., hospitals) exchange EHRs.

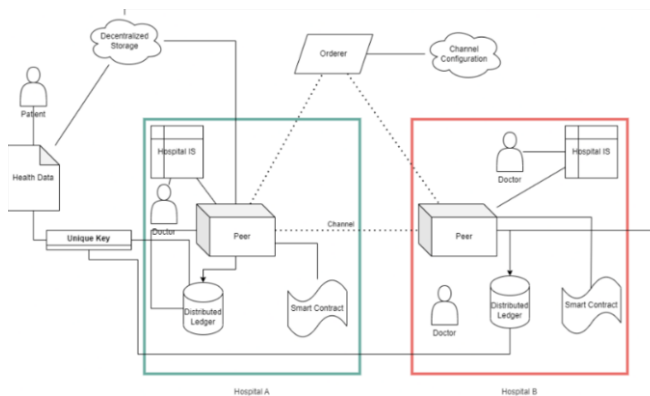


Figure 1. Example deployment of proposed architecture to support the EHRs integrity [4]

Figure 2 illustrates a simplified EHR entry process. A Doctor enters the health data of the patient. A unique hash of the EHR is generated, encrypted and submitted to be stored in Hyperledger Fabric blockchain. If the Hospital A IS receives the confirmation that the ledger has been updated, the constructed EHR is sent to the decentralized storage.

¹ Corresponding Author: Marten Kask, E-mail: marten.kask@taltech.ee.

The process of retrieving an EHR is similar. Instead of invoking a smart contract to enter new data, identification data provided by the Patient is processed to retrieve a unique hash that can be used to access EHR from decentralized storage. Future work should evaluate whether the proposed architecture resolves data integrity concerns, analyze scalability and future-proofing as computational power evolves, and explore the potential integration of the European Digital Identity.

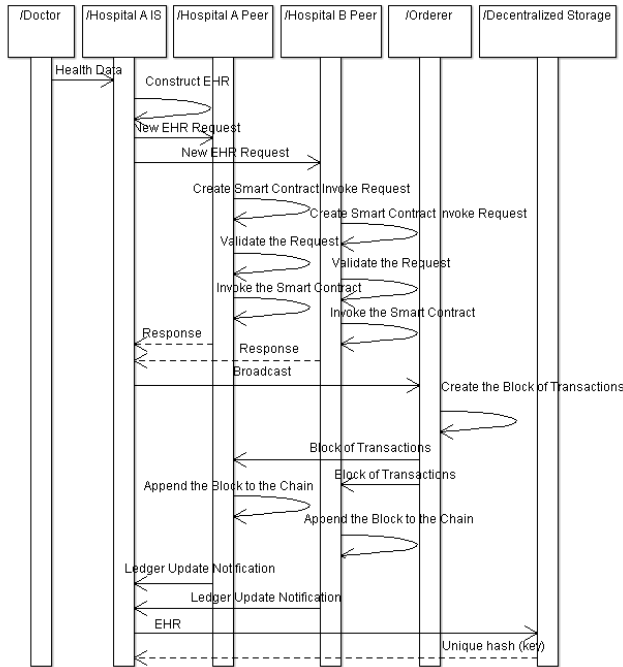


Figure 2. Sequence Diagram of the Proposed Process of Entering a New EHR [4]

This work in the project ‘ICT programme’ was supported by the European Union through the European Social Fund.

References

- [1] Kask M, Piho G, Ross P. Systematic Literature Review of Methods for Maintaining Data Integrity. In: Advances in Model and Data Engineering in the Digitalization Era: MEDI 2021 International Workshops: DETECT, SIAS, CSMML, BIOG, HEDA, Tallinn, Estonia, June 21–23, 2021, Proceedings 10. Springer; 2021. p. 259-68. doi: 10.1007/978-3-030-87657-9_20
- [2] Introduction - hyperledger-fabricdocs main documentation;. Accessed: 2023-05-20. Available from: https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger_fabric_whitepaper.pdf.
- [3] Klementi T, Kankainen K.J.I., Piho G, Ross P. Prospective research topics towards preserving electronic health records in decentralised content-addressable storage networks. HEDA-2022: The International Health Data Workshop, June 19-24, 2022, Bergen, Norway. CEUR-WS.org. Available from: https://ceur-ws.org/Vol-3264/HEDA22_paper_7.pdf.
- [4] Kask M, Klementi T, Piho G, Ross P. Maintaining Data Integrity in Electronic Health Records with Hyperledger Fabric. HEDA 2023: the 3rd International Workshop on Health Data. Co-located with STAF 2023, 18–21 July, Leicester, United Kingdom. CEUR-WS.org. Available from: <https://ceur-ws.org/Vol-3440/paper7.pdf>.