Distributed Immunisation Information System

Kaine Bent

April 4, 2021

Abstract

..

Chapter 1

Introduction

Inspired by the ideas of using blockchain to benefit society through decentralised applications in [5], this project seeks to design and develop a distributed solution to our current immunisation information systems. As mentioned in [6], current implementations of IISs, especially that in developing countries, are lacking in terms of technological proficiency. As stated in [7], IISs are centralised repositories of personally identifiable vaccination information for individual members of a served population. This project aims to produce a decentralised version of an IIS, using the recent conception of Decentralised Ledger Technology (DLT) which stems from the blockchain technology introduced by [8]. From research such as [9] and [10], we know that blockchain provides the required security and privacy necessary for implementing these types of systems. [10] states that blockchain technology can reform the interoperability of healthcare databases. The system this project proposes uses a permissioned blockchain, in which the health authorities of different nations are trusted nodes in the network. Each health authority will provide immunisation records of their population to the ledger – such data will only be accessible by the health authority that provided it as well as the individual the record belongs to. This shall be enforced by using asymmetrical cryptography. A private key will be required to access these records, the key being held by the individual and their relevant health authority. This enables the individual's control over their immunisation records along with the ability to provide their private key and verify their immunisations. This, as discussed in [7], will simplify the processes of vaccination verification that may be required in pandemic scenarios, registering for school, starting with a new employer, or crossing international borders. This system would benefit bodies striving to verify individuals' immunisations internationally. This report explores the required components of such a system, the professional considerations that are necessary for building this system such as legislation and ethical concerns, along with the requirements of an IIS and that of one implemented using blockchain.

Chapter 2

Professional considerations

The system proposed in this project will process personal data, in the form of immunisation records, so necessitates consideration of ethical and legal requirements.

2.1 BCS Code of Conduct

This project has been aligned with the BCS Code of Conduct; relevant sections are as follows:

1. Public Interest You shall:
    a have a due regard for public health, privacy, security and wellbeing of others and the environment. Encryption methods will be used where necessary to ensure the confidentiality of information in the system.
    b have due regard for the legitimate rights of Third Parties. This system will make use of asymmetric-key encryption as well as hash functions to protect data, including that of third parties.
    c promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise. This project proposes the system detailed be adopted by nations to provide a means of access to personal immunisation records, enabling ease of access for the population.
2. Professional Competence and Integrity You shall:
    a only undertake to do work or provide a service that is within your professional competence.
    b NOT claim any level of competence that you do not possess. This project has been thoroughly considered and the conclusion has been reached that it is within my professional competence.

c develop your professional knowledge, skills and competence on a continuing basis. Maintaining awareness of technological developments, procedures, and standards that are relevant to your field. This project explores the current solutions for immunisation information systems, evolving my professional knowledge. This project displays an awareness of technological standards and procedures necessary for a distributed IIS.

d ensure that you have the knowledge and understanding of Legislation and that you comply with such Legislation, in carrying out your professional responsibilities. This project includes a section exploring the legislation concerning this system. Specifically, the geographic area in which this system is being produced and how legislation governs the operations of such a system.

e respect and value alternative viewpoints and, seek, accept and offer honest criticisms of work. This project shall regularly be shared with my project supervisor to gain alternative viewpoints and criticisms, which will be implemented.

f avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction. The design section of this project will detail the necessary security methods to maintain confidentiality, integrity and authenticity in the system.

Chapter 3

Ethical implications

"Issues of concern are falsified or counterfeit vaccine certificates" are described in **schlagenhauf˙variants˙2021**, when considering digital vaccination passports. Blockchain enables an immutable store of data, rendering any attempt at providing a spoofed record would be nullified due to the data the individual provides not being in the ledger. Hyperledger Fabric, the framework of choice to aid in production of the network, allows access to verify that private data is in fact in a ledger without revealing it.

Chapter 4

Chaincode

Selected Go, as there are apparent benifits outlined in [1]

Chapter 5

Framework selection

An important decision, which dictates the system requirements. Hyperledger fabric is ... Using their MSPs is different to things like this TrustID: A New Approach to Fabric User Identity Management how? Why are we not customising and instead going with fabric's defaut implementation, maybe because it fits our use case better? It makes sense as the orginisations using the system are governed already by their heath body, for UK it's MAYBE Department of Health & Social Care - look this up! See if there's a general term for lead health body or whatever
Fabric has all the identity functionality built in, Indy + Aries would be more flexible but does that matter with an permissioned network? Fabric MSPs etc vs DIDs? Or does it use DIDs? w3 DIDs

5.1 Hyperledger Fabric

Transaction flow "The SDK serves as a shim to package the transaction proposal into the properly architected format (protocol buffer over gRPC) and takes the user's cryptographic credentials to produce a unique signature for this transaction proposal." - .

Chapter 6

benefits

[Covid-19: Vaccines and vaccine passports being sold on darknet] - this system would negate these spoofed vaccination records as all data will be on the system and if not it's illegitimate.

Chapter 7

Essential Considerations

7.1 Ethical Implications

7.2 Data Privacy

7.3 FHIR

FHIR - standards for sharing healthcare information.

7.4 Security

Whilst penetration testing Hyperledger Fabric, there was found a high severity issue, which describes the potential to guess the content of a Private Data Collection. This is achieved using SHA256 as an oracle. To ensure this vulnerability is not available in the system, it is necessary to ensure any private data is salted before being hashed. **shaẇpenetrationẇ2019**

7.5 Default application SDK

Go is best for chaincode but what would be the most suitable for the access applications? Java, because it's already highly used in enteprise already? **find reference for this ** Java also enables cross-platform usage, most convenient for these systems that are already up and running. - Node satisfies these conditions also, Node has Performance Traffic Engine in fabric-test toolset. Fabric Network Operator tool, from Hyperledger, also utillises the Node SDK, looking like we might just wanna use Node? Benefits to web app vs desktop? Java is probs more secure ** find ref ** but web app with Node would likely be more flexible, as it can be used for the access application as any device runs Node but internet is required. Java is statically typed, but this

is also achieved when using TypeScript with Node - this brings both SDKs to an equal playing field, in terms of maintainability. Orgs will be able to develop their own applications, enabled by OSS. However, considerations are in place for the best default SDK to use, as the correct choice could simplify adoption. Does Node possess an advantage in terms of ease of adoption? Can more mobile devices use Node than Java? Does it even matter which SDK?

Chapter 8

Designing a Distributed Immunisation Information System

zero-knowledge asset transfer vs zero-knowledge proof?

Chapter 9

Immunisation verification

smarthealth.cards by Vaccination Credential Initiative (VCI) - smart card framework.

Use an SDK to invoke chaincode that compares the provided data (hash of the transaction? - in which your immunisation record is stored) with the hash (SHA-250 probs) of the data in the ledger. If there's no match there's no verification, details?

Chapter 10

Blockchian-as-a-Service

Using Blockchain for Electronic Health Records shahnaz$_{u}sing_{2}$019
**shortcomings are discussed here: brotsis$_{s}ecurity_{2}$020 ∗
∗.$Thecomputingpowerandsecurityprovidedby BaaScanmakeupfortheshortcomingsaforementioned.$**song˙res**
Comparing Blockchain-as-a-Service platforms, to identify which tool is most suitable for delpoying the proposed Distributed Immunisation Information System built with Hyperledger Fabric.

Beginning, I was aware of two options: Azure and IBM.

Reading [2].

[Performance Analytical Comparison of Blockchain-as-a-Service (BaaS) Platforms] says "Blockchain highly suffers from scalability problem due to its capped transaction latency as well as consensus approach"

Azure have FHIR API, is it the only one? looks like maybe Amazon also
Azure FHIR API

Bibliography

[1] L. Foschini, A. Gavagna, G. Martuscelli, and R. Montanari, "Hyperledger fabric blockchain: Chaincode performance analysis," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, ISSN: 1938-1883, Jun. 2020, pp. 1–6. DOI: 10.1109/ICC40277.2020.9149080.

[2] M. M. H. Onik and M. H. Miraz, "Performance analytical comparison of blockchain-as-a-service (BaaS) platforms," in *Emerging Technologies in Computing*, M. H. Miraz, P. S. Excell, A. Ware, S. Soomro, and M. Ali, Eds., ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Cham: Springer International Publishing, 2019, pp. 3–18, ISBN: 978-3-030-23943-5. DOI: 10.1007/978-3-030-23943-5_1.