Distributed Immunisation Information System

Kaine Bent

April 12, 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 aid 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, utilising Decentralised Ledger Technology (DLT) which has been highly discussed since the wide adoption of blockchain technology introduced by [1] - As discussed in [2]. 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.

2.2 Legislation

The General Data Protection Regulation (GDPR) is a privacy and security law, passed by the European Union (EU), imposes obligations onto organizations that target or collect data related to EU citizens and residents.[3]

The GDPR sets out several key principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

These stated principles are essential to our approach to processing personal data. Compliance with the principles established in the GDPR is fundamental to ensuring good practice in data protection. In Article 35(1) of the GDPR it states that a Data Protection Impact Assessment (DPIA) is required “Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.”. This asserts that if the system being designed and developed in this project is implemented in the real world performing a DPIA is mandatory. Though, a DPIA will not be necessary for this undertaking. As the GDPR is mainly concerned with the European Economic Area (EEA), producing this system in the UK brings concerns. The UK is currently in a transition period until the 31st of December 2020. At the end of this transition period the UK will become a third country. Presently, the UK is seeking adequacy decisions from the European Commission. “The effect of an adequacy decision is that personal data can be sent from an EEA state to a third country without any further safeguard being necessary” because “The European Commission has the power to determine whether a third country has an adequate level of data protection.” [3]. If the adequacy decision is not secured, by the end of the transition period, the provisions set out in [4] will take effect.

Chapter 3

Essential Considerations

3.1 Ethical Implications

”Issues of concern are falsified or counterfeit vaccine certificates” are described in [4], 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.

3.2 Data Privacy

3.3 Healthcare Stuff

use these:
[5] $<--$ ’Comparison of Smart Contract Blockchains for Healthcare Applications’
[6] $<--$
’A-Privacy-Preserving-Healthcare-Framework-Using-Hyperledger-Fabric’

3.3.1 FHIR

FHIR - standards for sharing healthcare information.

3.4 Security

a reference = [7] $<--$ ’On the Security and Privacy of Hyperledger Fabric - Challenges and Open Issues’

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. [8]

3.5 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 4

Chaincode

Selected Go, as there are apparent benifits outlined in [9]

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

System Analysis & Design

zero-knowledge asset transfer vs zero-knowledge proof?

7.1 Hyperledger Fabric

WRITE ABOUT THIS!

7.1.1 Architecture Overview

Hyperledger projects follow a design philosophy, which includes a modular, extinsible approach; enabling interoperability. Design puts an emphasis on secure solutions, crucial to systems using sensitive data. Hyperledger's token-agnostic approach simplifies bringing blockchain to business infrastructure.

7.1.2 Inspiration

Use $-->$ [10].

7.1.3 Consensus

Distributed systems & consensus, use [11].

The consensus problem occurs when attempting to achieve reliability in a distributed system, in the presence of faulty processes. A system requires processes to reach an $a$greement on a value after one or more processes propose what the value should be. In a system such that: each process p_i communicates with other processes via message passing (we assume communication is reliable), up to some number f of the N processes are faulty, the remainder of processes are correct.
Reaching consensus is achieved as follows. Every process p_i starts in an *undecided* state and *proposes* a single value v_i. The processes communicate

with eachother and exchange values. Each process then sets the value of a *decision variable*, d_i. In doing so the process enters the *decided* state and can no longer change d_i.[12]

1. Termination: Eventually each correct process sets a decision variable.
2. Agreement: The decision of all correct processes is the same.
3. Integrity: If the correct processes al proposed the same value, then any correct process in the *decided* state has chosen that value.[12]

In Hyperledger business blockchain frameworks consensus is reached by performig two seperate activities:

1. Ordering of transactions
2. Validating transactions

In the first step, the transactions are received from the client. An ordering service is used to order the transactions. To enable confidentiality, the ordering service may be agnostic to the transaction; that is, the transaction content can be hashed or encrypted.[13] This is extremely benificial to this system, as maintaining confidentiality is essential to abiding by the GDPR [3].

Chapter 8

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 9

Blockchian-as-a-Service

Using Blockchain for Electronic Health Records shahnaz_using_2019 **shortcomings are discussed here: brotsis_security_2020 ** . The computing power and security provided by BaaS can make up for the shortcomings aforementioned.**song"˙research"˙2021**.
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 [14].

[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] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Nov. 20, 2019, Publication Title: Manubot. [Online]. Available: `https://git.dhimmel.com/bitcoin-whitepaper/` (visited on 11/18/2020).

[2] A. Sunyaev, "Distributed ledger technology," in *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Cham: Springer International Publishing, 2020, pp. 265–299, ISBN: 978-3-030-34957-8. DOI: `10.1007/978-3-030-34957-8_9`. [Online]. Available: `https://doi.org/10.1007/978-3-030-34957-8_9`.

[3] (). General data protection regulation (GDPR) – official legal text, General Data Protection Regulation (GDPR), [Online]. Available: `https://gdpr-info.eu/` (visited on 04/04/2021).

[4] P. Schlagenhauf, D. Patel, A. J. Rodriguez-Morales, P. Gautret, M. P. Grobusch, and K. Leder, "Variants, vaccines and vaccination passports: Challenges and chances for travel medicine in 2021," *Travel Medicine and Infectious Disease*, vol. 40, p. 101 996, 2021, ISSN: 1477-8939. DOI: `10.1016/j.tmaid.2021.101996`. [Online]. Available: `https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7899929/` (visited on 04/03/2021).

[5] H. Yu, H. Sun, D. Wu, and T.-T. Kuo, "Comparison of smart contract blockchains for healthcare applications," *AMIA Annual Symposium Proceedings*, vol. 2019, pp. 1266–1275, Mar. 4, 2020, ISSN: 1942-597X. [Online]. Available: `https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7153130/` (visited on 04/03/2021).

[6] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, and W. J. Buchanan, "A privacy-preserving healthcare framework using hyperledger fabric," *Sensors*, vol. 20, no. 22, p. 6587, Jan. 2020, Number: 22 Publisher: Multidisciplinary Digital Publishing Institute. DOI: `10.3390/s20226587`. [Online]. Available: `https://www.mdpi.com/1424-8220/20/22/6587` (visited on 04/10/2021).

[7] S. Brotsis, N. Kolokotronis, K. Limniotis, G. Bendiab, and S. Shiaeles, "On the security and privacy of hyperledger fabric: Challenges and open issues," in *2020 IEEE World Congress on Services (SERVICES)*, ISSN: 2642-939X, Oct. 2020, pp. 197–204. DOI: `10.1109/SERVICES48979.2020.00049`.

[8] G. Shaw, “Penetration testing technical report,” p. 20, Aug. 8, 2019.

[9] 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`.

[10] P. Yuan, X. Xiong, L. Lei, and K. Zheng, “Design and implementation on hyperledger-based emission trading system,” *IEEE Access*, vol. PP, pp. 1–1, Dec. 20, 2018. DOI: `10.1109/ACCESS.2018.2888929`.

[11] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, Jul. 1, 1982, ISSN: 0164-0925. DOI: `10.1145/357172.357176`. [Online]. Available: `https://doi.org/10.1145/357172.357176` (visited on 04/10/2021).

[12] G. Coulouris, J. Dollimore, T. Kindberg, and G. Blair, *Distributed Systems: Concepts and Design*. Pearson Education, Nov. 21, 2011, 1066 pp., Google-Books-ID: 3ZouAAAAQBAJ, ISBN: 978-0-13-300137-2.

[13] “Hyperledger architecture, volume 1,” Aug. 2017. [Online]. Available: `https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf` (visited on 04/11/2021).

[14] 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`.