

# Distributed Immunisation Information System

Kaine Bent

April 24, 2021

## Abstract

..



# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Problem Space, blockchain intro . . . . .	4
1.1.1	Blockchain architecture cryptography?? . . . . .	4
<b>2</b>	<b>Essential Considerations</b>	<b>5</b>
2.1	Professional considerations . . . . .	5
2.1.1	BCS Code of Conduct . . . . .	5
2.1.2	Legislation . . . . .	6
2.1.3	Ethical Implications . . . . .	7
2.1.4	Data Privacy . . . . .	7
2.1.5	Healthcare Stuff . . . . .	8
2.1.6	Security . . . . .	8
2.2	benefits . . . . .	8
<b>3</b>	<b>System Design</b>	<b>9</b>
3.1	Default application SDK . . . . .	9
3.2	Framework selection . . . . .	9
3.2.1	Hyperledger Fabric . . . . .	10
3.3	System Architecture . . . . .	12
3.4	Chaincode . . . . .	12
<b>4</b>	<b>Immunisation verification</b>	<b>13</b>
<b>5</b>	<b>Blockchian-as-a-Service</b>	<b>14</b>
5.1	IBM Blockchain Platform . . . . .	14

# List of Figures

# Chapter 1

## Introduction

(a) Motivation of the project (b) Aims of the project, ideal place first paragraph (c) Structure of the report

### 1.1 old intro

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. Forgery and personal data security are dominant concerns of similar projects, but such problems are routinely solved for financial and other sensitive transactions. **dye'covid-19'2021** This project attempts to utilise the techniques that achieve this, in other industries, to the vaccination passport problem.

As divulged in [2], DLT designs can be instantiated as a *public* or *private* distributed ledger [3], [4]. In public DLT designs, the underlying network allows arbitrary nodes to join and participate in the distributed ledger's maintenance. No registration or verification of the nodes' identities is required. Public DLT designs are often maintained by a large number of nodes, like with Bitcoin and Ethereum. The designs enable consistent high levels of availability. To allow for a high number of (arbitrary) nodes to find consensus, the designs for public DLT should be well scalable to not deter performance as more nodes join the network. [2]

In contrast, private DLT designs engage a defined set of nodes, with each node identifiable and known to the other network nodes. This means that private DLT designs require node verification when joining the distributed ledger, for example, by using Public Key Infrastructure (PKI). PKI comprises hardware, software, policies, procedures and roles that are used for the secure electronic transfer of data by means of an insecure network. A PKI manages the creation, distribution and revocation of digital certificates, which the use of public key cryptography requires. [2]

Blockchains can execute programmable transaction logic in the form of *smart contracts* as demonstrated by Ethereum [5]. The predecessor of smart contracts were the scripts in Bitcoin, introduced in [1]. Smart contracts function as *trusted distributed applications* and gains its security from the blockchain and the underlying consensus among peers. This is similar to the approach of building resilient applications with state-machine replication (SMR) [6]. Though, blockchains are different from traditional SMR with Byzantine

## 1.2 Problem Space, blockchain intro

### 1.2.1 Blockchain architecture cryptography??

Randomized hashing offers the signer additional protection by reducing the likelihood that a preparer can generate two or more messages that ultimately yield the same hash value during the digital signature generation process – even if it is practical to find collisions for the hash function.

hash functions are formally defined in [7] as *a function*  $h : D \rightarrow \dots$

$R$  where the domain  $D = 0, 1^*$ , and the range  $R = 0, 1^n$  for  $\text{smoen} \geq 1$  using one way hash functions, as defined by Merkle in [8], are hash functions store only hashes, this way data is kept anonymous and GDPR isn't a worry. Also, keeps the private data away from any verifiers etc because all they check against is a hash.

digital signatures < -- NEW!! NIST Publishes Special Publication 800-106 (Draft) "Randomized Hashing Digital Signatures". that documents our basic randomization technique for use with digital signatures. <http://csrc.nist.gov/publications/drafts/Draft-SP-800-106/Draft-SP800-106.pdf>



## Chapter 2

# Statement of originality

This report is submitted as part requirement for the degree of ... at the University of Sussex. It is the product of my own labour except where indicated in the text. The report may be freely copied and distributed provided the source is acknowledged.

## Chapter 3

# Essential Considerations

### 3.1 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.

Blockchains are not viable for data-storage, so ipfs (versinoed peer-to-peer file sharing system ) or off-chain storage ?

<https://www.ibm.com/downloads/cas/RXOVXAPM> < -- talks about GDPR necessitating off-chain storage, because of Art. 17 GDPR Right to erasure ('right to be forgotten') <https://gdpr-info.eu/art-17-gdpr/> any research here? definitely necessitates incorporation of FHIR, or anything similar which is useful, to interoperability in terms of exististing Immunisation Information Systems infrastructure.

#### 3.1.1 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.

### 3.1.2 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.[9]

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.

Medical records are pieces of personal, sensitive data which are stored, processed, processed and transmitted in healthcare systems.

Recital 26 Not Applicable to Anonymous Data\* so basically don't worry about GDPR <https://gdpr-info.eu/recitals/no-26/>

### **3.1.3 How did you address ethical issues?**

### **3.1.4 How did you address BCS Code of Conduct?**

### **3.1.5 Ethical Implications**

”Issues of concern are falsified or counterfeit vaccine certificates” are described in [10], 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.

### 3.1.6 Data Privacy

other than GDPR, considerations include: what?

### 3.1.7 Healthcare Stuff

use these:

[11] < -- Implementation Considerations for Blockchain in Healthcare Institutions

[12] < -- 'Comparison of Smart Contract Blockchains for Healthcare Applications'

[13] < --

'A-Privacy-Preserving-Healthcare-Framework-Using-Hyperledger-Fabric'

### FHIR

FHIR - standards for sharing healthcare information.

### 3.1.8 Security

a reference = [14] < -- '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. [15]

## 3.2 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 4

# System Design

Developing and testing chaincode was initially performed using the Fabric test network, provided in the official documentation for Hyperledger Fabric **noauthor'using'nodate**. It is based on a limited configuration:

1. It includes two peer organizations and an ordering organization.
2. For simplicity, a single node Raft ordering service is configured.
3. To reduce complexity, a TLS Certificate Authority (CA) is not deployed. All certificates are issued by the root CAs.
4. The sample network deploys a Fabric network with Docker Compose. Because the nodes are isolated within a Docker Compose network, the test network is not configured to connect to other running Fabric nodes. **noauthor'using'nodate**

Currently, medical data has the HL7 standard as a data exchange format but the exchange of medical records between countries is not widespread. **kung'personal'2020**

### 4.1 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 enterprise 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 utilises the Node SDK, looking like the project 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?

## 4.2 Hyperledger Fabric

An important decision, which dictates the system requirements. Hyperledger fabric is ... Using their MSPs is different to things like this

'<https://www.hyperledger.org/blog/2020/04/21/trustid-a-new-approach-to-fabric-user-identity-management>' TrustID:

A New Approach to Fabric User Identity Management how? Why are we not customising and instead going with fabric's default implementation, maybe because it fits our use case better? It makes sense as the organisations using the system are governed already by their health 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? '<https://www.w3.org/TR/did-core/>' w3 DIDs

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." - "<https://hyperledger-fabric.readthedocs.io/en/latest/txflow.html>".

For this project we will be using v2.2.2, as it delivers important new features and changes for users and operators alike, including support for new application and privacy patterns, enhanced governance around smart contracts, and new options for operating nodes. [16]

'<https://wiki.hyperledger.org/display/fabric/Design+Documents>'  
WRITE ABOUT THIS!

As discussed in [17], blockchain systems usually, both permissioned and permissionless, follow the order-execute architecture. This execution style involves ordering transactions first, using a consensus protocol, then executes them in the same order on all peers sequentially.<sup>1</sup>

Whilst the order-execute architecture is conceptually simple and therefore widely used, there are drawbacks which occur when using it for a

---

<sup>1</sup>This report follows the convention set in the Hyperledger Fabric whitepaper of calling the transaction execution (named "transaction validation" in blockchains such as Bitcoin) *transaction execution* to bring the terminology together.

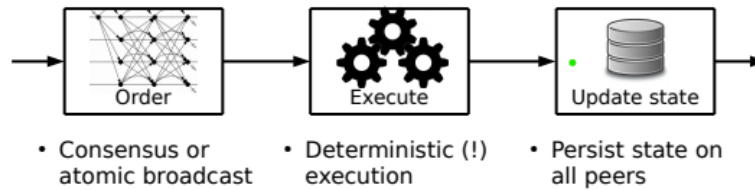


Figure 4.1: Order-execute architecture in replicated services

Source: [17]

general-purpose permissioned blockchain.[17] The most significant disadvantages are as follows: *Sequential execution*. Executing transactions sequentially on all peers limits the effective throughput that can be achieved on the blockchain.[17] One solution to this problem, used by Ethereum [18], utilises the concept of *gas* consumed by a transaction execution, which is converted at a *gas price* to a cost in the cryptocurrency and billed to the transaction submitter. This solution is excellent for use in permissionless blockchains, though does not suffice when designing a general-purpose, permissioned, token-agnostic, blockchain like Hyperledger Fabric. [17] Hyperledger Fabric distributed applications consist of two parts: A smart contract, called *chaincode*, which is program code that implements the application logic and runs during the *execution phase*. As well as an *endorsement policy* that is evaluated in the *validation phase*.

### 4.2.1 Architecture Overview

Hyperledger projects follow a design philosophy, which includes a modular, extensible 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. [19]

Hyperledger projects embrace security by design and follow the best practices specified by the Linux Foundation's Core Infrastructure initiative.

<https://www.coreinfrastructure.org/>

### 4.2.2 Privacy by Design

<https://www.hyperledger.org/blog/2018/10/23/private-data-collections-a-high-level-overview>

private-data-collections-a-high-level-overview < -- private data collections, is privacy by design - enables GDPR compliancy etc

[https://www.researchgate.net/publication/330748854\\_The\\_privacy\\_protection\\_mechanism\\_of\\_Hyperledger\\_Fabric\\_and\\_its\\_application\\_in\\_supply\\_chain\\_finance](https://www.researchgate.net/publication/330748854_The_privacy_protection_mechanism_of_Hyperledger_Fabric_and_its_application_in_supply_chain_finance) < -- The privacy protection mechanism of



Hyperledger Fabric and its application in supply chain finance <https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/Research-and-Innovation/Privacy-by-Design-Helps-blockchains-comply-With-GDPR.pdf> < -- Privacy by Design Helps Blockchains Comply With GDPR

### 4.2.3 Inspiration

Use -- > [20]. j- says there is a "LACK OF UNIVERSALLY DEFINED STANDARDS" is this true still? should this report be proposing standards for blockchain healthcare systems, are there thusfar?

### 4.2.4 Consensus

Distributed systems & consensus, use [21].

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 *agreement* 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 (assuming 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 each other 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  $d_i$ . [22]

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 all proposed the same value, then any correct process in the *decided* state has chosen that value. [22]

In Hyperledger business blockchain frameworks consensus is reached by performing two separate 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. [19] This is extremely beneficial to this system, as maintaining confidentiality is essential to abiding by the GDPR [9]. Consensus in Hyperledger Fabric is broken into 3 phases: *Endorsement*, *Ordering* and *Validation*.

1. Endorsement is driven by policy (eg. m of n signatures) upon which participants endorse a transaction.
2. Ordering phase accepts the endorsed transactions and agrees to the order to be committed to the ledger.
3. Validation takes a block of ordered transactions and validates the correctness of the results, including checking endorsement policy and double-spending.

zero-knowledge asset transfer vs zero-knowledge proof?

Using Go chaincode, generating UML diagrams from this, classes such as: Record, with states: immunised or not?

### 4.3 System Architecture Overview

going to call the "admissions staff" (people who want to check immunisation information)

### 4.4 Chaincode

**alexaki'blockchain-based'2018** suggests that medical records should contain metadata of a patient-provider encounter (visit date/time, location, etc.), the data stored off-chain and should be entered when the record is produced. As immunisations expire, the ledger must store metadata on immunisations to ensure the record in the ledger can be invalidated when the date is reached.

Chaincode is Hyperledger Fabric's version of smart contracts. Chaincode is a program, which can be written in general-programming languages Go, JavaScript (for Nodejs runtime) or Java, that implements a prescribed interface.

Selected Go, as there are apparent benefits outlined in [23]

The duration of protection conferred by vaccines should be tied to passport expiry dates **dye'covid-19'2021**. This is implemented via the expiration of our immunisation record contract.

## Chapter 5

# 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-256 probs) of the data in the ledger. If there's no match there's no verification, details?

## Chapter 6

# Blockchain-as-a-Service

Using Blockchain for Electronic Health Records '<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8863359>' [24]

\*\*shortcomings are discussed here:

'<https://ieeexplore.ieee.org/document/9284197>' [14] \*\*. The computing power and security provided by BaaS can make up for the shortcomings aforementioned.[25].

Comparing Blockchain-as-a-Service platforms, to identify which tool is most suitable for deploying the proposed Distributed Immunisation Information System built with Hyperledger Fabric.

Reading [26].

[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 '[https://azure.microsoft.com/en-gb/services/azure-api-for-fhir/?ocid=AID754288&wt.mc\\_id=azfr-c9-scottha%2CCFID0475](https://azure.microsoft.com/en-gb/services/azure-api-for-fhir/?ocid=AID754288&wt.mc_id=azfr-c9-scottha%2CCFID0475)' Azure FHIR API

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

## 6.1 IBM Blockchain Platform

IBM Blockchain Platform for IBM Cloud is built with Hyperledger Fabric v1.4.11 and v2.2.2. The system proposed in this report uses v2.2.2, as it delivers important new features and changes for users and operators alike, including support for new application and privacy patterns, enhanced governance around smart contracts, and new options for operating nodes. [16]

May have to use IBM just because of their whole hybrid cloud infrastructure, could be too easy to give up [27]

Requested demo of IBM Health Pass, will look more into this physically when the change occurs. For now, review the literature provided publicly - not much lmao '<https://www.ibm.com/watson/health/resources/digital-health-pass-blockchain-explained/>' '<https://mytechdecisions.com/compliance/ibm-salesforce-work-covid-19/>'

## Chapter 7

# Conclusion

This should be an assessment of the finished product.

Have you met your objectives? If not, why not?

Suggestions for future extensions

Alternatives methodologies might lead to a better system

Appendix A

Appendix Title

# 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](https://doi.org/10.1007/978-3-030-34957-8_9).
- [3] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, “Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues,” *IEEE Access*, vol. 6, pp. 1513–1524, 2018, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2779263.
- [4] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, “A taxonomy of blockchain-based systems for architecture design,” in *2017 IEEE International Conference on Software Architecture (ICSA)*, Apr. 2017, pp. 243–252. DOI: 10.1109/ICSA.2017.33.
- [5] (). Ethereum whitepaper, [ethereum.org](https://ethereum.org), [Online]. Available: <https://ethereum.org> (visited on 04/22/2021).
- [6] F. B. Schneider, “Implementing fault-tolerant services using the state machine approach: A tutorial,” *ACM Computing Surveys*, vol. 22, no. 4, pp. 299–319, Dec. 1, 1990, ISSN: 0360-0300. DOI: 10.1145/98163.98167. [Online]. Available: <https://doi.org/10.1145/98163.98167> (visited on 04/22/2021).
- [7] B. V. Rompay and K. U. L. Esat, “Analysis and Design of Cryptographic Hash Functions, MAC Algorithms and Block Ciphers,” p. 259,
- [8] R. C. Merkle, “Secrecy, authentication, and public key systems.,” AAI8001972, PhD thesis, Stanford University, Stanford, CA, USA, 1979, 187 pp.



- [9] (). General data protection regulation (GDPR) – official legal text, General Data Protection Regulation (GDPR), [Online]. Available: <https://gdpr-info.eu/> (visited on 04/04/2021).
- [10] P. Schlagenhaut, 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. 101996, 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).
- [11] K. Paranjape, M. Parker, D. Houlding, and J. Car, “Implementation considerations for blockchain in healthcare institutions,” *Blockchain in Healthcare Today*, Jul. 9, 2019, ISSN: 2573-8240. DOI: 10.30953/bhty.v2.114. [Online]. Available: <https://blockchainhealthcareday.com/index.php/journal/article/view/114> (visited on 04/18/2021).
- [12] 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).
- [13] 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).
- [14] 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.
- [15] G. Shaw, “Penetration testing technical report,” p. 20, Aug. 8, 2019.
- [16] (). What’s new in hyperledger fabric v2.x — hyperledger-fabricdocs master documentation, [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatsnew.html> (visited on 04/22/2021).
- [17] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and

- J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," *Proceedings of the Thirteenth EuroSys Conference*, pp. 1–15, Apr. 23, 2018. DOI: 10.1145/3190508.3190538. arXiv: 1801.10228. [Online]. Available: <http://arxiv.org/abs/1801.10228> (visited on 11/19/2020).
- [18] D. G. Wood, "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER," p. 39,
- [19] "Hyperledger architecture, volume 1," Aug. 2017. [Online]. Available: [https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger\\_Arch\\_WG\\_Paper\\_1\\_Consensus.pdf](https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf) (visited on 04/11/2021).
- [20] 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.
- [21] 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).
- [22] 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.
- [23] 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.
- [24] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147 782–147 795, 2019, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2946373.
- [25] J. Song, P. Zhang, M. Alkubati, Y. Bao, and G. Yu, "Research advances on blockchain-as-a-service: Architectures, applications and challenges," *Digital Communications and Networks*, Feb. 20, 2021, ISSN: 2352-8648. DOI: 10.1016/j.dcan.2021.02.001. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2352864821000092> (visited on 04/04/2021).
- [26] 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.

- [27] “IBM blockchain platform technical overview,” May 2020. [Online]. Available: <https://www.ibm.com/downloads/cas/Q9DGBLV7> (visited on 04/12/2021).