Pre-Project Report on

Vaccine Supply Chain Management using Blockchain

Submitted in partial fulfillment of the requirements

for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

Akhil Suden - 2017BITE023

Muneeb Ul Islam - 2017BITE030

Ashish Kumar - 2017BITE043

Under the supervision of

Ms. Iqra Altaf Gillani

Department of Information Technology

National Institute of Technology Srinagar,

J&K

January 2021

Contents

List of Figures

Chapter 1

Introduction

Immunization is an indispensable mechanism for preventing infectious diseases in modern society, and vaccine safety is closely related to public health and national security. However, issues such as vaccine expiration and vaccine record fraud are still widespread in vaccine supply chains. Therefore, an effective management system for the supervision of vaccine supply chains is urgently required. As the next generation of core technology after the Internet, blockchain is designed to build trust mechanisms that can change current information management methods [1].

With every vaccine monitored over the blockchain, each link along the chain could keep track of the entire process, and health departments could monitor the chain as a whole and intervene, if required, to ensure proper functioning [6]:

- Manufacturers could track whether shipments are delivered on time to their destinations
- Distributors would provide a more efficient delivery tracking platform, including storage requirements verifications, and would be the first to know and notify if things go wrong
- Hospitals and clinics could better manage their stocks, mitigating supply and demand constraints. Furthermore, they would get guarantees concerning vaccine authenticity and proper storage conditions
- Individuals would have an identical guarantee for the specific vaccine they receive

1.1 Motivation

Covid-19 Disease has lead to worldwide demand for vaccine development in every part of the world. While India is well on its way to develop a coronavirus vaccine, making sure that the vaccine reaches everyone in a timely manner is a humongous challenge. No one has the experience in managing such a large-scale operation. However, the biggest vaccine supply challenge can be solved by the right technology intervention combined with human ingenuity. The foremost challenge that India will face in accelerating the administration of a viable vaccine is ensuring that these vaccines are transported in compliance with all regulations and without breaking the cold chain from multiple production locations to all corners of the country. Christopher Holmes, MD, IDC Insights Asia Pacific says, "Getting the vaccine from the manufacturing sites to the global population will be the next challenge. Whilst the current emphasis is on vaccine development, governments need to put the processes and infrastructure in place to adequately and effectively manage the vaccine development ecosystem"[3].
So Blockchain proves to be the required technology which could help us to safely distribute vaccine to different parts of country.

1.2 Problem Statement

The main objective of this study is to develop a "vaccine blockchain" system based on blockchain. This vaccine blockchain system is designed to support vaccine traceability and smart contract functions, and can be used to address the problems of vaccine expiration and vaccine record fraud.

1.3 Organisation

The rest of the report is organised as follows. In Chapter 2 we will discuss underlying concepts Technologies to be used for our project. In Chapter 3, we survey the relevant literature. After that, we discuss our proposed approach in Chapter 4 along with software requirements and further work to be done for our project.

Chapter 2

Underlying Concepts & Technologies

2.1 What is Blockchain:

BLOCKCHAIN at its core is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers[4].

The blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto remains unknown to date. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server.

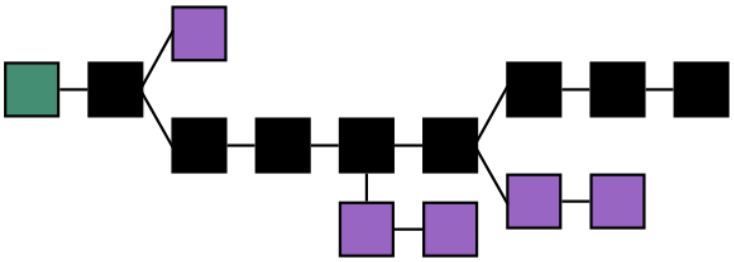

Figure 2.1: Blockchain formation. The main chain (black) consists of the longest series of blocks from the genesis block (green) to the current block. Orphan blocks (purple) exist outside of the main chain.

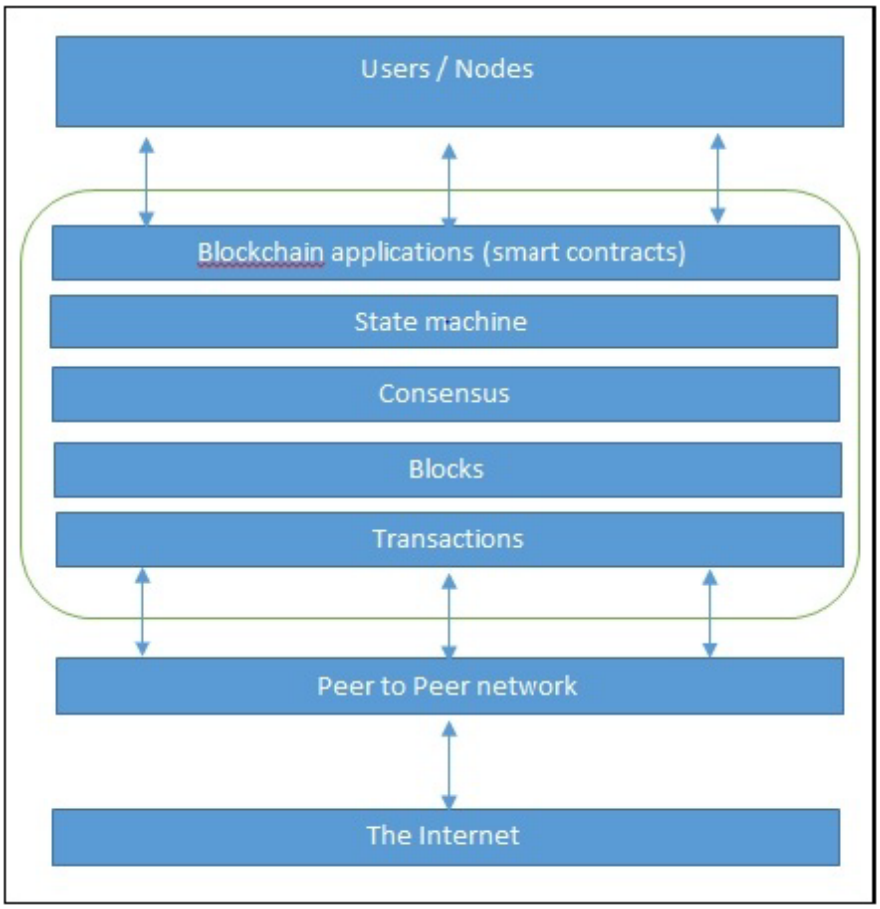

Figure 2.2: Network View of Blockchain

Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the internet, as can be seen in the following diagram. It is analogous to SMTP, HTTP, or FTP running on top of TCP/IP. At the bottom layer in the preceding diagram, there is the internet, which provides a basic communication layer for any network. In this case, a peer-to-peer network runs on top of the internet, which hosts another layer of blockchain. That layer contains transactions, blocks, consensus mechanisms, state machines, and blockchain smart contracts. All of these components are shown as a single logical entity in a box, representing blockchain above the peer-to-peer network. Finally, at the top, there are users or nodes that connect to the blockchain and perform various operations such as consensus, transaction verification, and processing.

2.2 FEATURES OF A BLOCKCHAIN:

1. **DISTRIBUTED CONSENSUS :** This enables a blockchain to present a single version of truth that is agreed upon by all parties without the requirement of a central authority.

2. **TRANSACTION VERIFICATION :** Any transactions posted from nodes on the blockchain are verified based on a predetermined set of rules and only valid transactions are selected for inclusion in a block.

3. **PLATFORMS FOR SMART CONTRACTS :** A blockchain is a platform where programs can run that execute business logic on behalf of the users.

4. **TRANSFERRING VALUE BETWEEN PEERS :** Blockchain enables the transfer of value between its users via tokens.

5. **SMART PROPERTY :** For the first time it is possible to link a digital or physical asset to the blockchain in an irrevocable manner, such that it cannot be claimed by anyone else; you are in full control of your asset and it cannot be double spent or double owned.

6. **IMMUTABILITY :** This is another key feature of blockchain: records once added onto the blockchain are immutable. There is the possibility of rolling back the changes but this is considered almost impossible to do as it will require an unaffordable amount of computing resources.

7. **SMART CONTRACTS :** These programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met.

2.3 CONSENSUS MECHANISMS:

A consensus mechanism is a set of steps that are taken by all, or most, nodes in order to agree on a proposed state or value. There are various requirements that must be met to provide the desired results in a consensus mechanism.

The following describes these requirements:

- **Agreement**: All honest nodes decide on the same value.
- **Termination**: All honest nodes terminate execution of the consensus process and eventually reach a decision
- **Validity**: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node
- **Fault tolerant**: The consensus algorithm should be able to run in the presence of faulty or malicious nodes(Byzantine nodes)
- **Integrity**: This is a requirement that no node can make the decision more than once in a single consensus cycle.

Below are some consensus algorithms:

1. **PROOF OF WORK :** This type of consensus mechanism relies on proof that enough computational resources have been spent before proposing a value for acceptance by the network. This is used in bitcoin and other cryptocurrencies.
2. **PROOF OF STAKE :** This algorithm works on the idea that a node or user has enough stake in the system; for example the user has invested enough in the system so that any malicious attempt would outweigh the benefits of performing an attack on the system. Another important concept in Proof of Stake (PoS) is coin age, which is derived from the amount of time and the number of coins that have not been spent. In this model, the chances of proposing and signing the next block increase with the coin age.

3. **DELEGATED PROOF OF STAKE :** Delegated Proof of Stake (DPOS) is an innovation over standard PoS whereby each node that has stake in the system can delegate the validation of a transaction to other nodes by voting. This is used in the bitshares blockchain.

4. **PROOF OF ELAPSED TIME :** Introduced by Intel, it uses Trusted Execution Environment (TEE) to provide randomness and safety in the leader election process via a guaranteed wait time. It requires the Intel SGX (Software Guard Extensions) processor in order to provide the security guarantee and for it to be secure.

5. **DEPOSIT-BASED CONSENSUS :** Nodes that wish to participate on the network have to put in a security deposit before they can propose a block.

6. **PROOF OF IMPORTANCE :** This idea is important and different from Proof of Stake. Proof of importance not only relies on how much stake a user has in the system but it also monitors the usage and movement of tokens by the user to establish a level of trust and importance. This is used in Nemcoin.

7. **FEDERATED CONSENSUS OR FEDERATED BYZANTINE CONSENSUS :** Used in the stellar consensus protocol, nodes in this protocol keep a group of publicly trusted peers and propagate only those transactions that have been validated by the majority of trusted nodes.

2.4 What are Smart Contracts?

Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met. At the most basic level, they are programs that run as they've been set up to run by the people who developed them.

What smart contracts on blockchain can do is streamline this complex process that involves several intermediaries because of a lack of trust among participants in the transaction.

Smart contracts work by following simple "if/when…then…" statements that are written into code on a blockchain. A network of computers executes the actions (releasing funds to the appropriate parties; registering a vehicle; sending notifications; issuing a ticket) when predetermined

conditions have been met and verified. The blockchain is then updated when the transaction is completed.

Let's see how this plays out in a supply chain example. Buyer B wants to buy something from Seller A, so she puts money in an escrow account. Seller A will use Shipper C to deliver the product to Buyer B. When Buyer B receives the item, the money in escrow will be released to Seller A and Shipper C. If Buyer B doesn't receive the shipment by Date Z, the money in escrow will be returned. When this transaction is executed, Manufacturer G is notified to create another of the items that was sold to increase supply. All this is done automatically.

2.5 Using Blockchain

In a blockchain transaction, two cryptographic primitives are used to prevent malicious users breaking the system. A **digital signature** is used to make sure that the information is signed by the claimed person as well as to test whether the information is modified by some malicious people. The signature process contains signature generation and signature verification. Given a message, the signatory generates a signature by using his private key, and the verifier can use signatory's public key to verify the messages authenticity. Instead of signing on the message directly, a cryptographic hash function is applied to the original message to produce a message digest for performance reason.

Merkle tree is an important element in blockchain security. It is a binary tree of hashes as proposed by Ralph Merkle that is used to verify data integrity efficiently and securely. One of the strengths of Merkle tree is that there is no need to recompute the hash of all data if one data block changes.

Chapter 3

Literature Survey

In this chapter, we have surveyed the literature related to this project. Each of the relevant papers will be discussed in detail.

Requirements elicitation for a blockchain vaccine supply chain management web/mobile application[7] This paper presents the processes carried out to be able to develop/gather the complete and right requirements to developing a secure and effective blockchain system for the vaccine supply chain. The paper hence presents the requirements elicitation activity of the Blockchain web/mobile application for vaccine supply chain.

The methods employed were; document review, survey, focus group workshops, interviews, observation brainstorming .

The paper present results of each of the methods used in requirements elicitation for eight themes, namely: temperature monitoring; quality, suitability and capacity of transport facilities; information systems and supportive management functions; storage quality, suitability and capacity; maintenance of cold-chain equipment; vaccine distribution; vaccine management policies and stock management.

The results presented gave understanding of the operation of the existing vaccine supply chain and the requirements for the blockchain web/mobile application for vaccine supply chain.

A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital[6] This paper emphasizes the need of using blockchain technology in the healthcare systems. It presents the problems the current healthcare systems are facing and a proposal to solve all these problems using blockchain.This paper highlights the fact that it is difficult to detect counterfeits because these drugs pass through different complex distributed networks, thus forming opportunities for counterfeits to enter the authentic supply chain. This paper proposes a novel drug supply chain management using Hyperledger Fabric based on blockchain technology to handle secure drug supply chain records. The proposed system solves this problem by conducting drug record transactions on a blockchain to create a smart healthcare ecosystem with a drug supply chain. A smart contract is launched to give time-limited access to electronic drug records and also patient electronic health records. The paper highlights the key capabilities of blockchain in combating the problem of counterfiet drugs.

Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare [8] This paper provide an overview of the opportunities and challenges associated with blockchain adoption and deployment for the health supply chain, with a focus on the pharmaceutical supply, medical device and supplies, Internet of Healthy Things (IoHT), and public health sectors. This paper highlights critical challenges in protecting the integrity of the health supply chain appear well suited for adoption of blockchain technology. The paper also takes into account challenges associated with the growth of the Internet of Healthy Things (IoHT) and how its development and adoption has far outpaced security requirements. In response to challenges as with the cybersecurity vulnerability identified in the pacemakers, government agencies and regulators are taking steps to increase awareness of the risks to the general public and healthcare ecosystem in the IoHT. The paper concludes by emphasizing the fact that Blockchain technology has the unrealized promise to help improve the health supply chain, but further study, evaluation an alignment with policy mechanisms is needed.

Chapter 4

Our Proposed Approach & Implementation

4.1 Proposed Framework

In our Blockchain, history of transactions in the system are stored along with queries for the data that are generated by system application programming interfaces (APIs).The blockchain stores information about the drugs, any updation on the drugs, their origin, their temperature record taken at specific intervals.

In the supply chain, the vaccine goes through various stakeholders:

- Manufacturer produces the products and adds it to Blockchain.
- Distributer distributes the product to wholesalers and retailers.
- Retailer sells it to the administration.

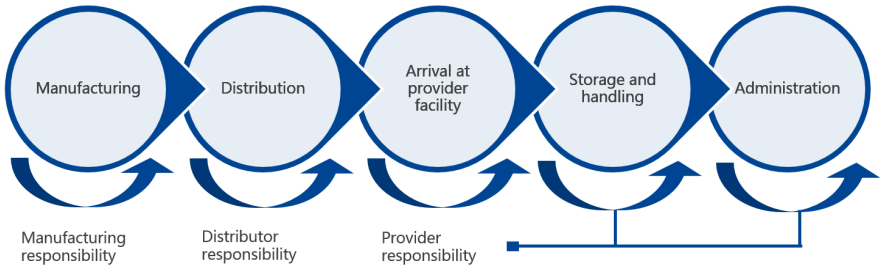

Figure 4.1: Fig: Vaccine flow through various stakeholders in the supply chain.

Flow of Data

- **Manufacturer** produces the drugs and adds the QR code to it, containing essential information like timestamp, item name, location, temperature, manufacturing and expiry date. The information added by the manufacturer gets stored on the blockchain, making it possible for other stakeholders to to trace the drugs' supply chain transparently. Once the information is added to the blockchain, a hash ID is produced that can be used for tracking back and verify the transactions.

- The logistics service providers deliver the drugs to **distributors** where they can verify the origin of medicines with the help of hash ID stored on the blockchain.They can trace back the information added by manufacturers such as the date of manufacturing, where it was manufactured and if it passed quality checks or not. Distributors validate the received medicines and sign the transaction digitally which is then added to the blockchain.
  During transit of the vaccine, some specific temperature levels need to be maintained and are continuously monitored by devices.

- **Retailer** get the drugs which can be traced back to know its origin previous temperature record using the hash ID saved on the blockchain.If any illegal distributor tries to sell counterfeit drugs with fake drug ID to Retailer or patients, it is easily detected by our Blockchain, so fraud is prevented. Also he can check whether vaccine is wastage or not by checking temperature record of the vaccine, stored in blockchain.

- **Administration** can be ensured if the medicine they are buying is safe to take or not. By scanning the QR code attached to the drug's packaging , they can get to know about its source and other effectiveness features by seeing transaction history of the blockchain . The hash ID linked to the QR code verifies that data fetched from blockchain is authentic.

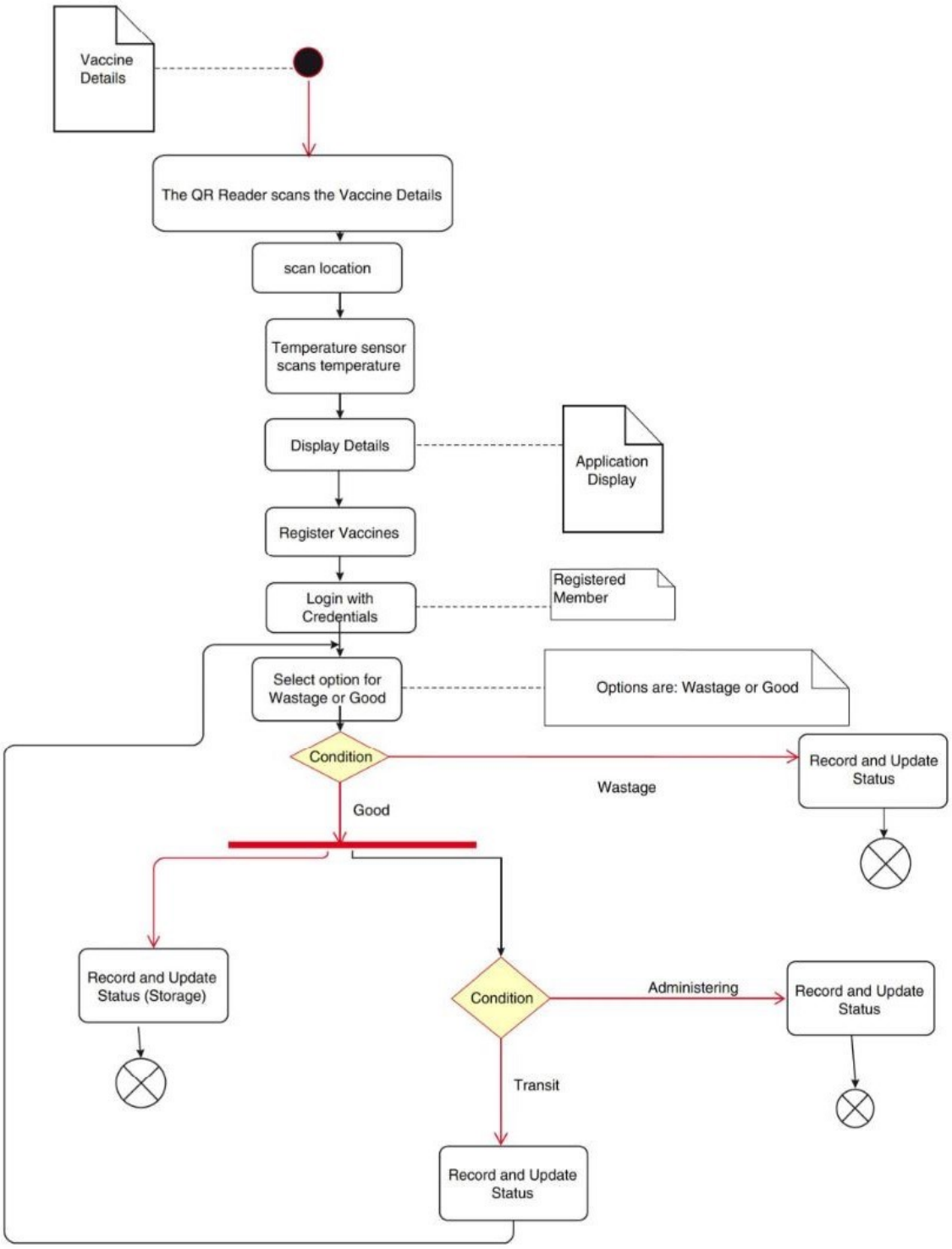

Figure 4.2: Data flow diagram at authorised stakeholder

4.2 Underlying Tools

The Tools to be used in this project are -

1. **dApp** :A decentralized application (dApp) is an application built on a decentralized network that combines a smart contract and a frontend user interface.

2. **MetaMask:** MetaMask is a tool able to run an Ethereum dApp in a browser. When using the dApp, a user can use MetaMask to sign the transactions he creates for storing the metadata about his data on the blockchain. By doing so, anyone accessing that data is confident that it was the authentic user who recorded the information.

3. **Ganache:** Ganache allows you to create a private Ethereum blockchain for us to run tests, execute commands, and inspect state while controlling how the chain operates. It gives us the ability to perform all actions you would on the main chain without the cost. Many developers use this to test their smart contracts during development. It provides convenient tools such as advanced mining controls and a built-in block explorer.

The process we'll go through:

- Open solidity online compiler.
- Compile the Smart Contract.
- Hash is generated.
- Get user's Metamask Ethereum address or use ganache.
- User confirms transaction to Ethereum via Metamask.
- IPFS hash is written on Ethereum.

Technical Stack Involved

- **Web3.js** : Front-End Library
- **Solidity** : The language used to build smart contracts that runs on Ethereum

- **Infura** : API access to Ethereum network and IPFS
- **Truffle** : Truffle Suite is a development environment based on Ethereum Blockchain, used to develop DApps.

Further work to be done

- Programming of smart contract.
- Creation of Metamask account.
- Connecting Metamask to blockchain.
- Developing a Front end using Web3js.
- Compiling the smart Contract and using the hash so generated to connect Frontend and Backend.

Bibliography

[1] Binbin Yong, Jun Shen, Xin Liu, Fucun Li, Huaming Chen, Qingguo Zhou
An intelligent blockchain-based system for safe vaccine supply and supervision, International Journal of Information Management, ISSN 0268-4012, https://doi.org/10.1016/j.ijinfomgt.2019.10.009.

[2] https://www.weforum.org/agenda/2020/11/using-blockchain-to-monitor-covid-19-vaccine-supply-chain/ [Accessed 01 January 2021]

[3] https://www.financialexpress.com/lifestyle/health/immunisation-supply-chain-getting-ready-for-the-shot/2158592/ [Accessed 01 January 2021]

[4] Mastering Blockchain Second Edition Distributed ledger technology, decentralization, and smart contracts explained by Imran Bashir ISBN 978-1-78883-904-4

[5] https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things [Accessed 01 January 2021]

[6] Faisal Jamil, Lei Hang, KyuHyung Kim, DoHyeun Kim (2019), A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital, Electronics; DOI:10.3390/electronics/8050505

[7] Mindila, A. N., Wafula, J. M., Ratemo, H. A., Tabu, C., Charo, J., Silali, C. (2019). Requirements elicitation for a blockchain vaccine supply chain management web/mobile application. Gates Open Research, 3(1420), 1420.

[8] Kevin A. Clauson, Elizabeth A. Breeden, Cameron Davidson, Timothy K. Mackey (2018), Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An

Exploration of Challenges and Opportunities in the Health Supply Chain, Blockchain in Healthcare TodayTM ISSN 2573-8240