Mohammod Arafat Mollik

USING BLOCKCHAIN TO FIGHT AGAINST COUNTERFEIT MEDICINES

School of Technology

2021

ACKNOWLEDGMENTS

First and foremost, I would like to thank the creator of the first widely accepted cryptocurrency Bitcoin, who goes by the pseudonym Satoshi Nakamoto. His idea brought blockchain technology acceptance to our society.

I am very grateful to my supervising teacher Dr. Smail Menani for supporting me along the process. I have also received great assistance from Oskari Heikel. He is the founder and COO of the company Truemed ltd. As they are working to find a solution to a similar problem that my thesis was about, we had good collaboration on a short period of time from both parties.

Furthermore, I would also like to thank my beloved girlfriend, Nafisa Haque, who was mentally a great support to me. I express my warmest and heartiest thanks to my family and friends who kept believing in me during my hard times and supporting me throughout my failures.

Mohammod Arafat Mollik

25.05.2021

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Author	Mohammod Arafat Mollik
Title	Using Blockchain to Fight Against Counterfeit Medicines
Year	2021
Language	English
Pages	40
Name of Supervisor	Smail Menani

Counterfeit drugs have become a global threat that recently have drawn significant attention. Estimated by WHO, more than a million people die because of using fake drugs. If we dig through the reasons behind counterfeit drugs existing in our lives, one of the main reasons is imperfect supply chain. In our current way of drug supply chain management, there are lot of loopholes that allows these fake drugs to be manifested. The present scenario states that there are presumably not enough data being shared among the parties in the supply chain, thus creating an opportunity for these counterfeiting. This results in not only loss of precious life but also billions of dollars are being lost in the process.

This thesis went through an in-depth concept of how we can fight against counterfeit drugs specifically using the power of blockchain technology. Also, this thesis consists of how blockchain technology can create a more secure platform for data serialization in the supply chain of medicines and a demo application explaining how it can be implemented in the real world. This thesis will explain how promising this new technology can be and how this can prevent not only counterfeit drugs but also any other kind of products that needs strong authenticity in the supply chain.

Keywords Blockchain, smart contracts, drug supply chain, security, and fake drugs

CONTENTS

LIST OF ABBREVIATIONS

IOT	Internet of things
DAPPs	Decentralized applications
SAAS	Software-as-a-Service
P2P	Peer to Peer
POW	Proof of Work
EVM	Ethereum Virtual Machine
RPC	Remote Procedure Call
ABI	Application Binary Interface

LIST OF FIGURES

LIST OF CODE SNIPPETS

1 INTRODUCTION

1.1 Background

Consider a scenario in which a person dies because of fake medication. It is not a far-fetched possibility. For most developing countries and even some developed countries, it has become a reality. The shape, height, color, and even packaging of fake medicine is similar to the original. These fake goods can contain small quantities of active ingredients or none at all or something much worse as lethal ingredients. Fake drugs are without a doubt, a great danger to customers and the pharmaceutical industry. Real-time visibility of drug manufacturing and management is needed to solve this. With that being said, counterfeiting is a problem that blockchain can overcome. As the data held in a blockchain can be viewed publicly, this can increase the transparency in the supply chain, thus creating opportunity to eradicate this counterfeiting problem.

The concept of blockchain technology was originated from the cryptocurrency Bitcoin. Bitcoin's main feature was that a transaction of currency could be done without a third party involved. It can be compared to the traditional way of transferring currency which is through banks. This way of transferring currency is done in a centralized way, meaning there is someone that has the power to regulate this transaction.

In a blockchain, a transaction can be done in a very secure way without anyone to intervene, meaning one can send currency to another person without relying on other entity. This is called decentralization. Even though, at first it was all about transferring currency to one another through a decentralized way, soon the concept became much more complicated than that. Apparently transferring currency through blockchain also meant transferring data from one place to another. In other words, Bitcoin was just some crypted piece of data that was transferred from one place to another in a very secured way.

After some people releasing this potential of cryptocurrency, they decided to create something new that interacts with these encrypted data to essentially create

something called smart contracts. Smart contract simply means that a network of computers executes some actions when the predetermined conditions have been met. There are multiple entities involved in these smart contracts but there is not centralized authority to control the transaction. Once the code has been executed then there is no need for a middleman. People realizing this feature started to create applications using the power of smart contracts. These applications are called DAPPs or decentralized applications. DAPPs can look like a normal application in the phone, but in the backend all the data is processed through blockchain. DAPPs can be used in nearly everything. For instance, trading currency in a decentralized way, to lend money or borrow money in a decentralized way, making social media where nobody governs the platform, controlling IOT devices etc. So many possibilities open when smart contracts can be implemented to complete various tasks.

1.2 Objectives

If we think about the health care sector, we are using so many advanced technologies that make our lives easier. We are using technologies, such as VR, AI, Robotics, or IoT devices. All these new kinds of technologies had their share of revolutionizing the health care industry. As we adapt to new technologies every now and then, blockchain deserves a chance. The objective of this thesis is to explain the ways blockchain technology can be implemented in the supply chain management of medicines and help to counter fake drug supply.

Particularly, this thesis goes through an academic concept of blockchain, some studies about the use cases in the health care industry, their advantages, and limitations, use of smart contracts and DAPPs. Eventually the thesis proposes some methods on how to apply this technology to improve the medical supply chain.

2 THE CONSEQUENCES OF COUNTERFEIT MEDICINE

2.1 History Behind Counterfeit Medicine

Many types of disruption occurred in the supply chain even before the term supply chain management (SCM) entered into our language. These supply chain disturbances have become more sophisticated due to ecosystem changes, business model changes and other new adaptations that have developed over decades. At present, emerging technologies have become quite vulnerable to cyberattacks.

From different kinds of risk involved in supply chain distribution, cyberattacks have become very common. Some group of people conducted multiple cyber-attacks throughout the years that manipulated the database of these supply chain distributors. They inject fraud information on the database, thus resulting in counterfeit products to be entered in the supply chain.

A statistic shows that until February 25, 2021,cyberattacks on healthcare have more than doubled in 2020, compared to previous years. Among the attacks, ransomware was responsible for 28 percent of all attacks. Because of this reason, many important medical supplies, such as personal protective equipment, vaccines and many other supply chains were compromised by these targeted campaigns, according to the latest IBM X-Force report!/1,2/ Some vulnerability caused cyberattacks on healthcare, manufacturing companies, and energy sector more than doubled from the previous year. Manufacturing and energy were, in particular, the most targeted sectors in 2020, coming in second only to finance and insurance. Attackers took advantage of a nearly 50 percent increase in vulnerabilities in industrial control systems (ICS), which are critical to both manufacturing and energy production. /2/

These cyber-attackers are accumulating lists of open, vulnerable databases linked to healthcare organizations, with the aim of monetizing the data by offering it to other hackers. On-premises servers connected specialty equipment, SaaS systems, and other cloud-based technology all have these flaws. These vulnerabilities are

most often accompanied by access misconfigurations or weak access controls, making the database and even the network vulnerable to attacks /3/ .

2.2 The Scale of Counterfeit Drugs Problem

Pharmaceutical industry is very vulnerable to be faked. It has become a challenge to tackle this exploit. Highly intense and strong demand for fast shipping leaves out a big vulnerability for these pharmaceuticals to be pirated. This can be confirmed by Figure 1 below. This figure shows the data between 2014-2016. In this data, based on the customs seizures, from 97 product categories, pharmaceutical products are 10th most pirated product.

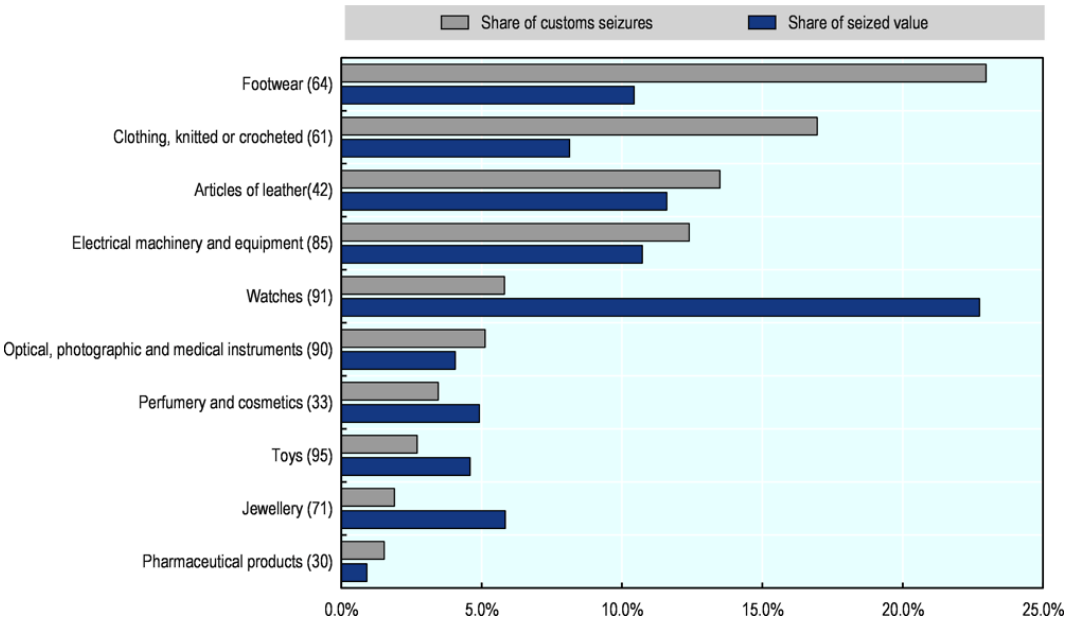


Figure 1. Top product categories counterfeit or pirated, 2014-2016 /4/

The importance of global trade in counterfeit pharmaceuticals, according to the OECD/EUIPO (2019) report in 2016, reached USD 4.4 billion. This accounts for 0.84 percent of all pharmaceutical imports worldwide.

Other compliance data collected in the PSI dataset show the large extent of counterfeiting in the pharmaceutical industry. Over the last five years, this dataset includes information on counterfeiting, illicit diversion, and major theft events

(2014 to 2018). The annual totals of pharmaceutical crime events over that time span are shown in Figure 1. The graph shows that overall reports rose by 102 percent from 2014 to 2018. Two factors continue to be significant in these increases: Over the past five years, government agencies have improved their reporting and a greater number of PSI member organizations have increased their reporting. In terms of member reporting, the institute received around 33% more cases for analysis and evaluation in the year of 2018 than in the year of 2014. Counterfeiting is achieved on a wide scale as well as on a smaller, least complex scale in all continents. Packaging and drugs are often assembled and printed in various countries before being transported to a final destination for assembly and distribution. As an example, fake medicines from Asia may be wrapped in forged African packaging, or vice versa. Medicines are often hidden or smuggled, and they are branded as something else. /4/

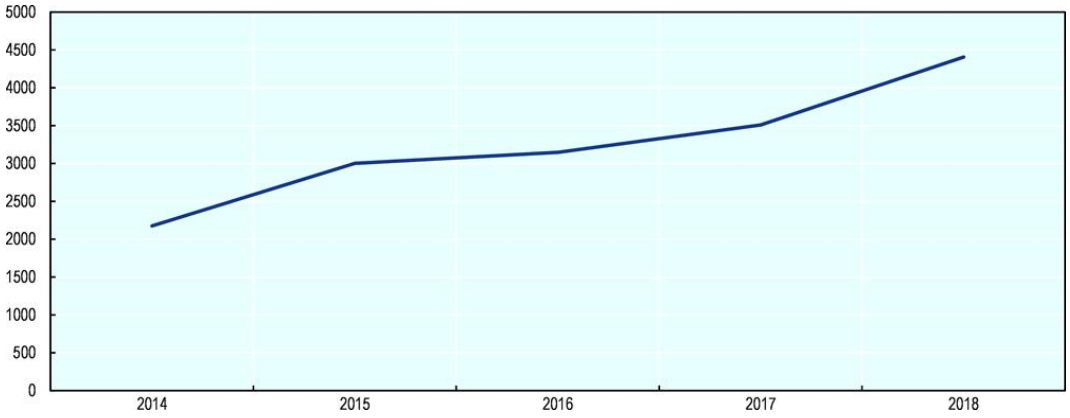


Figure 2. Number of total incidents, 2014-2018 /4/

3 HOW FAKE DRUGS CAN ENTER IN THE SUPPLY CHAIN

3.1 Supply Chain Management in Healthcare

The resources necessary to provide goods or services to a customer are referred to as the supply chain. Supply chain management in healthcare is often a very complex and fragmented method.

Obtaining capital, material handling, and supplying products to providers and patients are all aspects of medical supply chain management. Biometric traits and facts about medical products and services are normally transferred through a variety of different parties, such as retailers, insurance agencies, hospitals, vendors, group buying organizations, and relevant regulatory agencies, to complete the process.

On the other hand, healthcare facilities and clinical practice may generate significant cost-cutting opportunities by fostering productivity in the healthcare supply chain.

Executives in pharmaceutical chain management are in charge of providing entities with the goods that clients require as well as stock control. Simply put, supply chain is the process of onshore and offshore connections with providers and buyers in order supply high quality products and services while declining supply chain costs.

The pharmaceutical process usually begins with the procurement of healthcare supplies and transfer to a production facility. Based on the goods, physicians may procure supplies directly from the factory or dealer, via a group of financial institution, which agrees to pay an agreement with the retailer on the hospital's behalf.

Governing bodies, such as that of the Controlled Substance Enforcement, and pharmaceutical providers, such as Single payer or Medicare firms, also are engaged in pharmaceutical chain management. Governing bodies and wage earners dictate whether or not a clinical tool is eligible for patient access and if the physicians would be reimbursed for using it on clinical practice.

3.2 Different ways fake pharmaceuticals enter the supply chain

As it has been shown that supply chain in healthcare is quite complicated, there are many ways fraud copies of medicine can enter the supply chain. Some of the following was a fake drug can enter the supply chain:

1. Hacking the database: Different parties in a supply chain management may use different database or servers. The data can be vulnerable to the hackers. The hackers may inject their own set of data to the database. This data may contain information of fake drugs that can then be disguised as the real ones into the supply chain.
2. Manufacturer: The manufacturer is the first link in the medication supply chain. Since there are many possible ways for products to be counterfeited, this is the most likely place for a generic substance or ingredient to enter distribution. In certain cases, the incorrect prescription is placed in bottles and compromised remedies are marketed instead of real medications.
3. Counterfeiting from the suppliers: As there are many suppliers involved in the system, someone from the inside may be involved in fraudulent activity and they can just edit the database and disguise the fake drugs into the supply management.
4. Fake drugs in Retail sites: Even if the drugs are legitimately supplied to the retail sites. The drugs can also be just replaced inside the retail sites. Fake drugs can then be used as real ones and the real drugs can be resold in higher price or any other way.

These are just some ways a fake drug can enter in the supply chain. For a counterfeiter's point of view, they will always look for a loophole in the supply chain management where they can inject their fake drugs into the system.

There are many ongoing projects who are trying to fight this major problem. Most of them are using traditional way to secure the database from fraudulent activity. Implementing blockchain technology to fight this problem can be the most cost efficient and secure way. The implementation of blockchain technology can ensure that the drugs offered are authentic by checking with suppliers, dealers, repositories, and pharmacies.

4 IMPLEMENTING BLOCKCHIAN AS A SOLUTION

4.1 What is Blockchain?

Blockchain technology has been around for more than a decade now. Even though blockchain started being widely known through the popularity of Bitcoin, the history of blockchain goes way beyond. The concept of blockchain technology was described in 1991 by researcher W. Scott Stornetta and Stuart Haber. Their main objective was to introduce a solution for time-stamping digital documents that cannot be tampered of changed. They developed a system that was able to cryptographically secure the data of those document in blocks. /5/

Later on, in 2004, Hal Finney who was a computer scientist and cryptographic activist had proposed a system known as Reusable Proof of Work (RPOW). This proof of work algorithm solved the double spending problem as it was able to keep the ownership of the tokens or assets by a trusted server. However, the server is not like the traditional server. The server was designed as such that the users throughout the world were able to verify the accuracy and credibility in real time. RPOW was presumably a significant step towards the history of cryptocurrencies and blockchain technology. /6/

After the RPOW became conceptualized, in 2008, a person by the pseudonym "Satoshi Nakamoto" came up with a theory known as distributed blockchain. He improved Hal Finney's RPOW system and created a way of how new blocks can be added to the initial chain. The new system utilizes a peer-to-peer network for the timestamping. It was able to verify a transaction or an exchange of data without a central authority. Nowadays this technique has been used in the cryptocurrency space as it serves as a public ledger for all the transaction being help on the blockchain. /6/

To understand the concept of public ledger, we can go through a very simple example. Imagine a person named Bob is an owner of a house. Bob decides to sell the house to Alice. Alice receives the house ownership by exchanging a demanded money. Now if this were done in a public ledger, it would mean that the transaction that happened between Alice and Bob is written in a publicly accessible database. This publicly shared database has to be secured, managed, transparent, and

indestructible. In real life there will be a need of a centralized authority or middleman to manage this database. But with Satoshi Nakamoto's model, the shared database will be managed through blockchain thus there will be no need for a central authority.

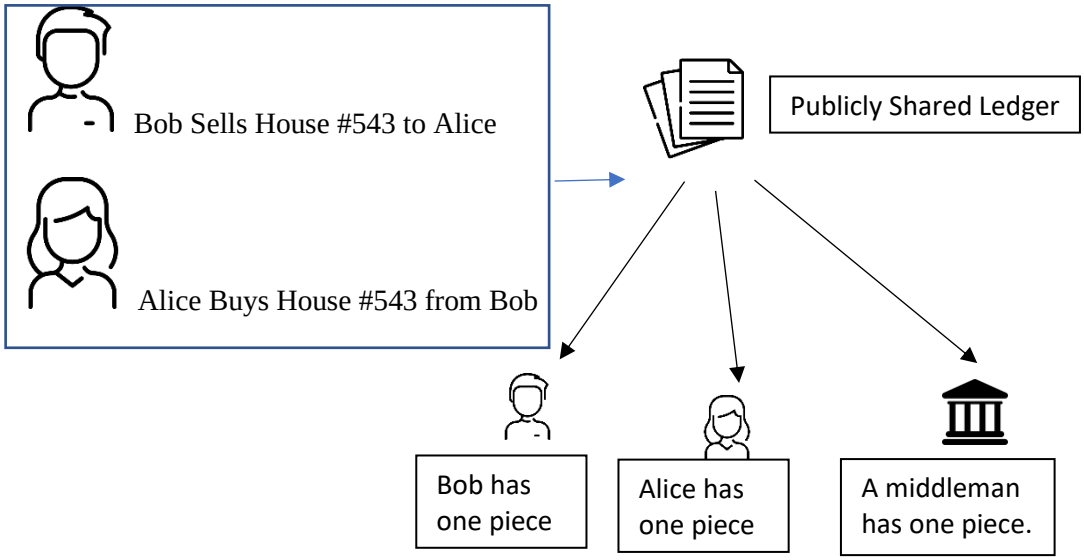


Figure 3. Example of a shared ledger

Instead of keeping this ledger in a central server, Satoshi Nakamoto decided to eliminate the use of centralization for good. Instead of storing several copies in a central registry, multiple copies are equally dispersed and stored in several machines around the network, with no one having a master copy. Since there is no such thing as a "master copy" in blockchain, all user's rights are equivalent, making it as decentralized and distributed.

A blockchain transaction, like a conventional transaction, contains information, such as who the transaction is sent from and to, what is exchanged (could be digital money or some kind of data), when it was sent, and other technological properties. This is done in such a way that it is transmitted to the whole network first and then checked by the participants of the network. If all is in order, the requested operation will be carried out and recorded in a block; otherwise, any invalid actions will be detected automatically by any of the network members, and the transaction will be reverted. As the data written in the blockchain is not editable and transparent, it can be possible to create a trust-less solution. To ensure that the blockchain technology is capable these features mentioned, any blockchain network must be built from

three factors: secure cryptography, an autonomous peer-to-peer network and consensus algorithm.

4.2 What is peer-to-peer network?

The peer-to-peer network model is not the same as the traditional client-server model. In fact, it is the opposite of this client-server model. In a widely used client-server model, one or a group of data servers are carried out by a single entity or organization. To perform some kind of operation, all the requests and responses will be handled by the single server and eventually, all the data will be stored in the centralized data storage. In this case if a hacker successfully attacks the server, he can have access to all the information that is being saved in the server. Thus, all the data will be in danger. The peer-to-peer model proposes that there will be no need for a central server, but there can be multiple servers with shared data all over the network. Here, each server is commonly known as a peer or a node. A node can be a regular computer with some disk storage. This disk storage will be the part of this shared database in the P2P network. Because all the data is shared between the nodes, even if the hacker has access to one of the peers, the endangered data can still be restored by the help of all the other database in the network. All data transfers are directly transferred between nodes in a peer-to-peer (P2P) network, with no third-party access. To achieve decentralization, blockchain technology makes use of a peer-to-peer network.

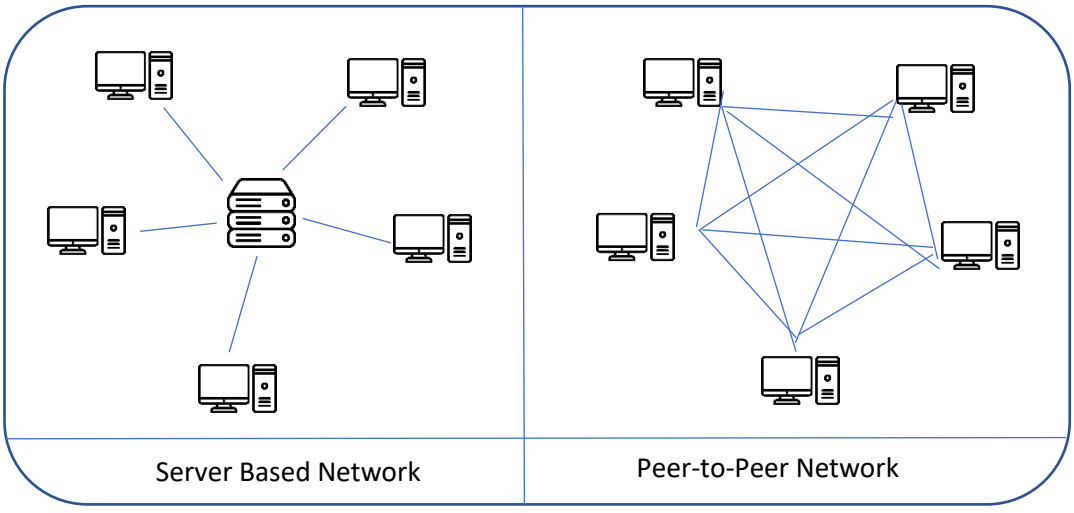
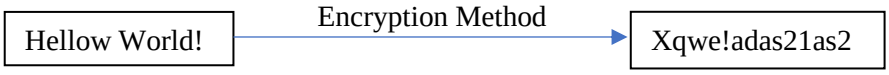


Figure 4. Server Based Network Vs Peer-To-Peer Network

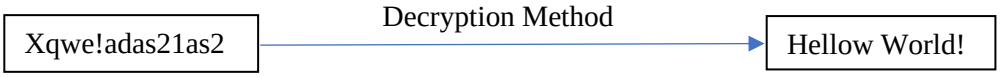
4.3 What is cryptography?

The method of designing protocols that prohibit third parties from accessing private data is known as cryptography. Below are some important terms related to cryptography:

1. **Encryption**: Encryption means to turn a text into unreadable format, but only authorized parties can understand the information. In other words, the process of creating an incomprehensible text from a plain text is called cryptography. The figure below makes it easier to understand:



2. **Decryption**: Opposite to encryption, decryption means to convert the unreadable message into its original readable format. Below is an example of decryption:



3. **Cipher**: Cipher is an algorithm that performs the encryption or decryption. To perform this algorithm there are some well-defined steps needed to be completed in-order to encrypt a data in a way that an authorized person is able to decrypt the data again.

Blockchain technology uses this cryptography in so many different ways. For instance, creating wallets, performing transactions, or preserving protocols for privacy e. To understand how cryptography works in a blockchain, we need to understand some topics such as hashing, Public-key, Private-key and Merkle Trees. We will discuss these important topics below.

4.3.1 Public-key and Private-key

Public-key and Private keys are very important when it comes to cryptography in blockchain technology. To understand what it is a fundamental element in blockchain technology let us take Alice and Bob as an example. Imagine, Alice wants to send some data through the blockchain to Bob. Alice and Bob both have the public and private keys. When sending the data to Bob, Alice can view Bob's public key, but she cannot view Bob's private key. The same thing happens vice versa, meaning that when Bob receives some data, Bob can view only the public key where the data was sent from. The data that was sent to Bob from Alice will essentially travel through the peer-to-peer network in the blockchain system. All the peers or nodes will validate the transaction so that the transaction only goes through to a single entity which is Bob. Bob will receive the encrypted data from Alice in a very secured way. After that Bob will need the private key which is associated with the public key. By using both the public and private key Bob will be able to decrypt the encrypted data which was sent from Alice. Any other person with unauthorized public or private key cannot view the encrypted data that was sent from Alice to Bob. Figure 5 below explains the transaction in an easy way.

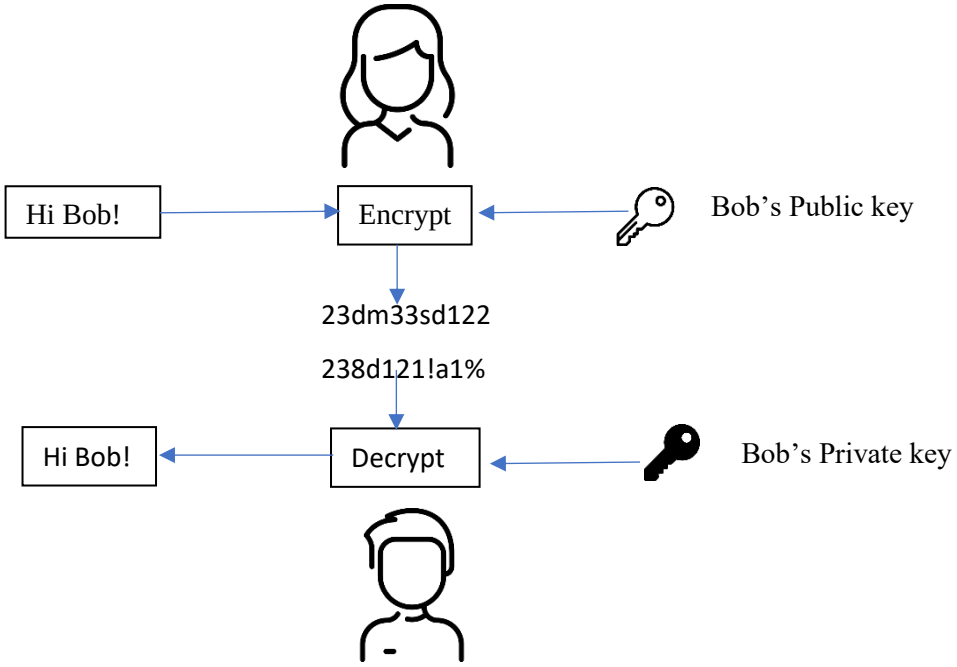


Figure 5. Use of Public-key and Private keys.

4.3.2 Cryptographic Hashing

In the terms of computer science hashing means taking an input of string which can be of any length and converting it to a fixed length output. Cryptographic hashing can make blockchain technology immutable as each new block of data produces a hash output of the previous block's data.

Let us assume that, a blockchain just added its 100th block of data. The data that exists in the previous 99 blocks will be added to the new block as a hash output. The same thing happened to block number 99, meaning when the 99th block was being added, previous 98 blocks of data were stored in the block as hash output. This source results in the first block which is known as the genesis block. However, this way of creating a chain is what makes a blockchain so immutable. If someone tried to alter even 1 bit of data in any blocks of the blockchain that means he would alter the hash output of that data. The nodes or peers of the network will immediately notice the change that does not match their own hashes and they will reject the change, ultimately creating a consensus mechanism that does not allow unauthorized altered data to be entered into the blockchain. Figure 6 shows how the hashing works in the blockchain.

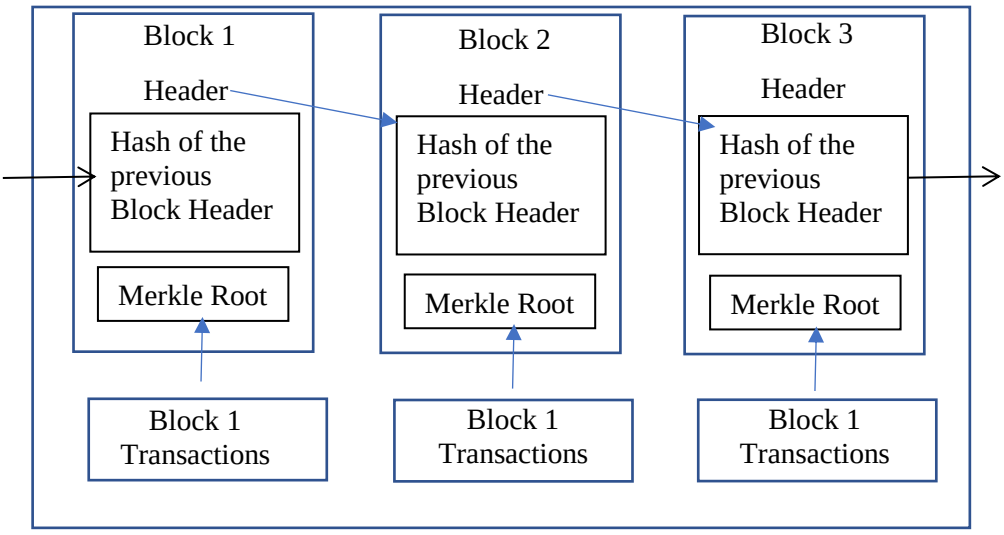


Figure 6. Simplified version of a Blockchain

4.3.3 Merkle Tree and Root

Imagine how much processing power and storage space will be required to fulfil a blockchain infrastructure that handles hundreds of thousands of transactions per day. To satisfy such system, an immense computing power would be required. Here is where the Merkle tree comes into play. A Merkle tree is a data structure that helps computers to safely and easily validate individual documents in a system without having to go through the entire material of a vast database.

There is a root node, and it has many nodes that is linked with it. Those nodes are called child nodes. Again, the child nodes also have their own child nodes and so on. Groups of nodes in this Merkle tree are known as sub-trees and a node that has no children is called a leaf-node. A Merkle tree (or hash tree) is a tree that stores hash outputs rather than raw data in each node using cryptographic hash functions. Every parent node is a hash of its child node hashes, and each leaf node is a cryptographic hash of its original data. Figure 7 shows how it works. /7/

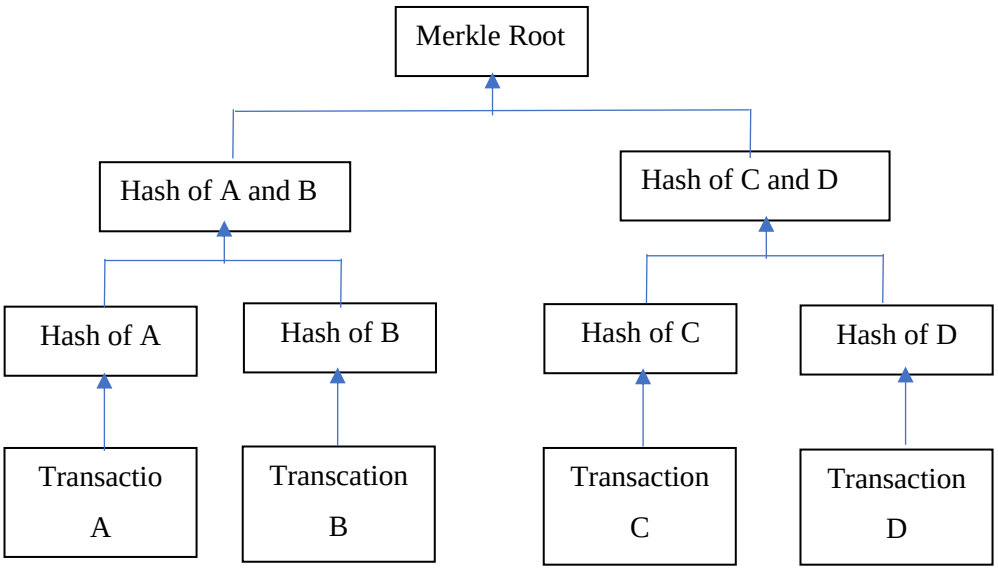


Figure 7. Merkle Tree

Now that we discussed how cryptography works in a blockchain, we can further discuss what mining does in a blockchain and what the benefits are.

4.4 How Mining Works in Blockchain Technology

Mining is actually a very important process to secure the blockchain network as well as creating new cryptocurrency. There are many different types of blockchain today but let us take bitcoin as an example to understand how mining works. While many people think of cryptocurrency mining as merely creating new coins, it is really a solution to the potential issue of a digital asset being double spent on a distributed network. The idea of digital currencies was confronted with a problem: digital networks can be tampered with. Bitcoin's public ledger, for example, enables validated miners to update transactions on the database to avoid fraud. The job of these miners is to protect the network from double spending. New coins are created as a reward for the miner's efforts in protecting the network through this mining operation. Since a centralized authority is not required in distributed ledgers to control the network, the mining process validates transactions independently. Therefore, Miners can protect the network from fraudulent activity by participating in these transaction validating process. A proof-of-work (PoW) consensus protocol is used to ensure that only validated cryptocurrency miners can mine and verify transactions (in the case of Bitcoin). This consensus protocol helps to protect the network form external attacks.

Proof of Work: Simply put, miners are just some random people using their computers processing power to solve some mathematical problem in order to create a new block in the blockchain and they get some cryptocurrency as reward. Using their computer processor power to achieve a consensus in a decentralized manner is called Proof-of-work.

4.5 What is Smart Contracts and DAPPs

As we have previously discussed what blockchain is, how it is so secured now let us discuss some other implementation of blockchain. As we know blockchain is not only used for making a secure transaction of some cryptocurrency, but it can also be used for doing so many things as a blockchain is a distributed ledger or database. Not only cryptocurrencies can be transferred securely through this technology but also data can be transferred in a secured way. Which means it is possible to build some kind of self-executing smart contracts with the help of blockchain. In addition,

if smart contracts can be safely made executable, it would also be possible to make decentralised application with the help of smart contracts as well.

The history of smart contract goes back to 1996 when an American programmer Nick Szabo first described the principles of smart contracts. Smart contracts, in Szabo's opinion, are automated protocols for information transmission that use mathematical algorithms to automatically perform a transaction until the established conditions are met while maintaining complete control over the process. /8/

Any kind of data including money, commodities or other digital assets can be exchanged using smart contracts. The contract is held and replicated in a decentralized database that cannot be tampered with or removed.

Using the potential of smart contracts, the concept of DAPPs was born. DAPPs means Decentralised Applications. Anyone can use a DAPP to execute a smart contract that serves a purpose. DAPPS with proper graphical interface can look very much similar to the regular applications running of centralised servers. But, in the backend of DAPPs all the data are stored in shared/distributed database which makes it more secure and immutable. DAPPs can run autonomously once launched, which means low cost on server maintenance and low cost for security measurements. These make DAPPs in some cases much more efficient than normal applications. To put it simply, DAPPs are essentially “blockchain-enabled” platforms, and smart contracts allow them to connect to the blockchain.

Now that we have discussed the meaning of smart contracts and the correlation with DAPPs we can now understand what real-life implementation can be possible. We will discuss with a demo DAPP that how we can create a solution to prevent fake supplies to enter into the supply chain of medicines.

5 DEMO WEB APPLICATION USING WEB3

5.1 The Use Case

In present days we see how mobile applications or web applications are being used in solving so many problems. From creating a way to attend school from our own home during a pandemic to use applications to maintain our health and well-being, applications have become a part of our life. But most applications that require a database that runs on centralised server. This is why there is lack of transparency in the data that is being transferred. If there can be a way how an application would have such transparency that everyone in the world can check and track information as well as verifying if the data is authorized or not, then that would be a great solution to the counterfeiting problem in supply chain, especially in medical supply chain. In this thesis I would propose a way how an end-consumer can check what the source of this product he/she is consuming and if it authorized or not. We will go through a demo application that actually runs on the decentralised database and it has enough transparency that the end-user can be confident with the authenticity in what he/she is buying. The web application will be demonstrated next, which once executed, can be run in a decentralised way and people can check if the source of the product is authentic or not.

The demo application has two simple functions. One, an authorised user with authorized wallet address can scan a product's barcode/QR code and upload to the blockchain. The wallet address of this user will be called admin.

The second function is that all other users that have the product in their hands can scan the product's code and can see the transparent information in the blockchain. The user does not have the authority to upload any information into the blockchain related to that specific smart contract.

This application is very transparent, meaning the transactions that happen here will be public. The reason why transparency is very important for this specific use case is because the end user can gain more confidence on the product they are purchasing. If the end user uses the application and scans the barcode on the product, the user can see all the information that were previously uploaded on the

blockchain. The user can see important information, such as the date when it was manufactured, the expiry date, and the product name . By viewing this important information, the user can be sure that the product he/she is purchasing is manufactured from the verified company itself. This is how the application can help to prevent fake drugs being supplied to the end user.

We have previously discussed how we can use the potential of smart contracts to build applications. For this use case, the Ethereum blockchain is used. The DApp is written using WEB3 and the Solidity programming language. The Ethereum Mainnet is not used, the Ropsten Test Network is used instead. We will use the Metamask application for the wallet. Every user of a DApp needs a wallet, otherwise he/she will not have an identity in the blockchain thus cannot perform any kind of transactions. To view the information on the blockchain we will use Etherscan. There are other ways to view a transaction details on a blockchain but Etherscan has a good graphical overview, and it is very easy to use which is why we will use Etherscan to analyse the originality of a product.

Below are the descriptions of some terms that were used in this paragraph:

- **WEB3**: Web3 is known as JavaScript framework that has a collection of libraries that makes it possible to interact with a remote or local Ethereum node. /9/
- **Solidity**: Solidity is a programming language, and it is mainly designed to build smart contracts on the Ethereum blockchain.
- **Ropsten Network**: Developers mainly use the Ropsten Test network to build DApps for free of charge. The Ropsten network works almost like the real Ethereum network but it is not considered as secured and reliable as the Ethereum Mainnet. It is only used for testing DApps and nothing else.
- **Metamask**: Metamask is a wallet that gives the user a public key and a private key which is needed to interact with the blockchain.
- **Etherscan**: Etherscan is a leading block explorer on the Ethereum blockchain. Etherscan is a website which provides with information of a specific transaction fluently.

5.2 Use of Web3?

Web3 is a collection of libraries that allows the user to interact with the blockchain. Its much like the traditional web development where developers use jQuery to make Ajax calls to a web server. But instead of using jQuery to read or write some data into or from a data server, developers can use Web3 to do to read and write to the blockchain. /10/

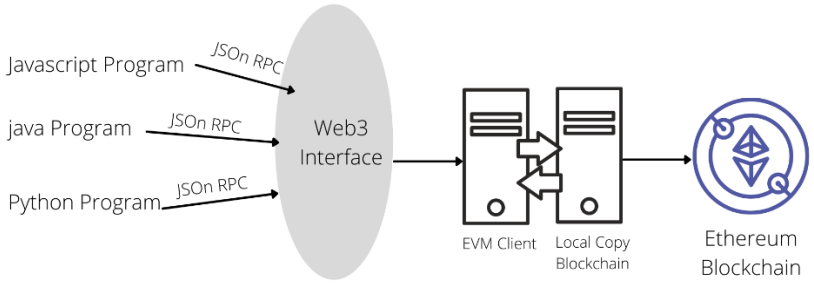


Figure 8. How web3 interacts with Eth Blockchain

From Figure 8, we can see that using the Json RPC different programming language are compiled through Web3 interface and use EVM client to execute the smart contract and then interact with the blockchain. For our demo application, our EVM client is Metamask and the local blockchain is the Ropsten Network.

5.2 Design

Figure 9 shows how the smart contract will actually work. In the application two entities will primarily be used, one is the admin user, and another is the regular user. The admin user account can represent an account of a manufacturer company such as a medicine company. To simplify the use case, let's assume the admin account is held by a medicine company who makes drugs. All the drugs they make, they will scan the product's barcode/QR code. The code will contain some important information. For example, expiry date of that medicine, the product name and branch id etc. This information will then be stored in the blockchain via a verified account only. The verified account will be determined by the smart contract itself.

Meaning, only the specific account the smart contract recognised as the admin account will be able to perform certain functions. In the example that certain function is able to scan a barcode and upload it to the blockchain. Any account other than the admin account itself is viewed as regular user account. A regular user account cannot upload any information in the blockchain. The user can only scan a product and if the information is in the blockchain, then can view the information related to that specific product barcode/QR code.

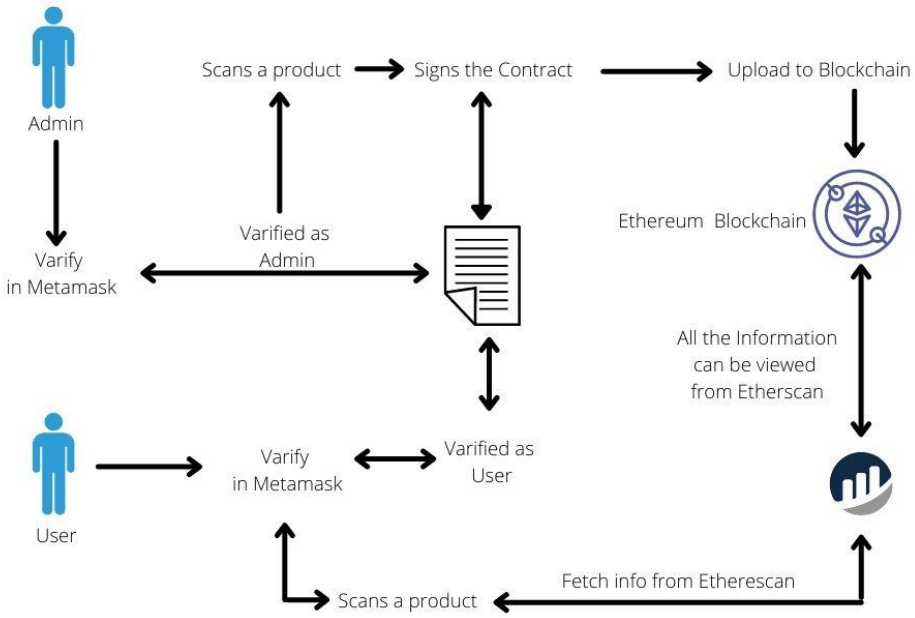


Figure 9. How the smart contract will work with 2 entities (Regular user and Admin)

5.3 Application Description

When the user opens the demo application, he/she is required to login via a Metamask wallet. After confirming the identity via Metamask wallet, the user can proceed. If the wallet address matches with the admin address, which was hardcoded in the code itself, the user can access some functions only limited to the admin account.

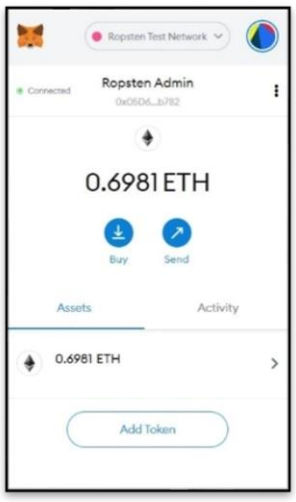


Figure 10. Login Via metamask to confirm admin account

If the user is verified as the admin, then he/she is able to open the camera of the device he is using and can scan a product barcode/QR code. For our demo, we will be using QR code for scanning because it is much more efficient in containing more information than barcode. The admin can now scan a QR code which is embedded into the packaging of the product. The QR code contains some general information like product name, ID, expiry date etc.

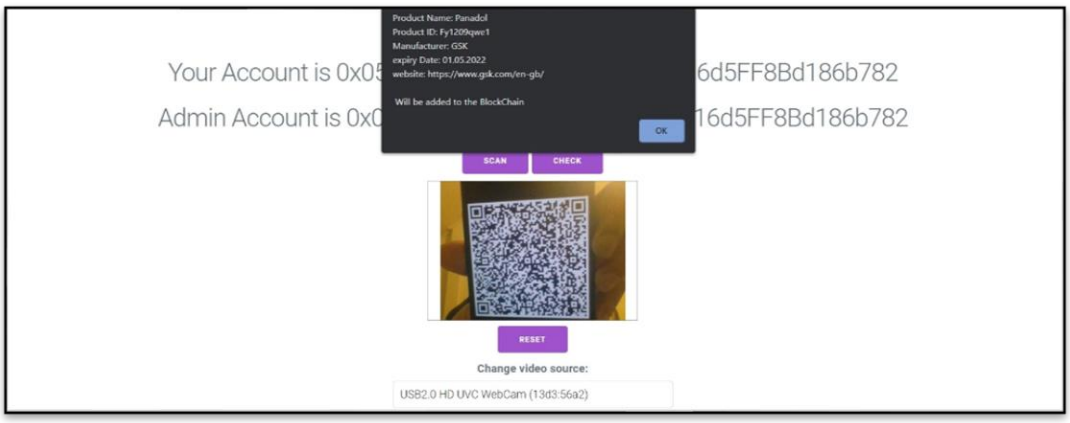


Figure 11. Scanning and Uploading to The Ehereum Blockchian

This information will be then uploaded to the blockchain. The admin will confirm the transaction via Metamask and pay a small network fee for the Ethereum blockchain. Now the information is uploaded into the blockchain via a verified wallet address. In Etherscan it is possible to see the details of the transaction.

In Figure 12, we can see some information which is very important when it comes to verifying the legitimacy of a product. They are described in-details below:

- **Transaction Hash**: A transaction hash is unique for every transaction that happens on the blockchain. If we have a transaction hash, we can find out all the information related to that specific transaction.
- **Timestamp**: The timestamp is the time when the transaction was confirmed. This timestamp cannot be changed or edited. This gives a huge advantage as an end user can use this feature to verify the date of production and much more.
- **From and to**: This means from which account a transaction was initiated and to which account the transaction was sent. We can see that the transaction was sent from the admin account and to the smart contract of the DApp.
- **Input data**: Here we can see what data were being transferred as a mean of transaction to the smart contract. Here we can see the exact same data that was being read from the QR code.

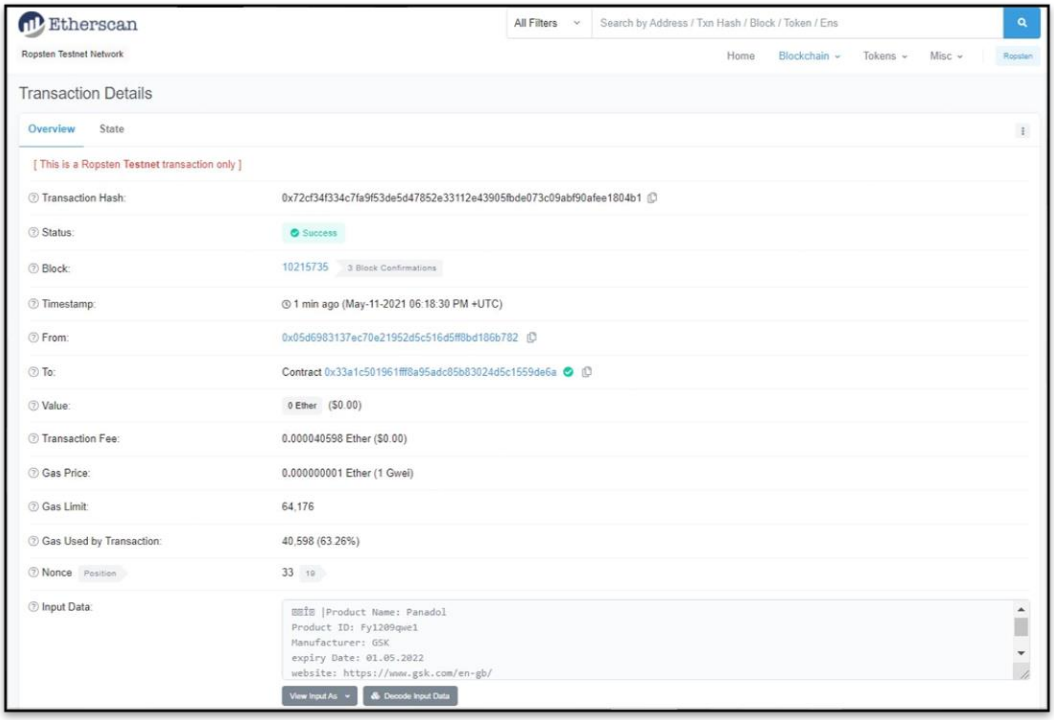


Figure 12. Details of the transaction via Etherscan

Now, let us use another Metamask wallet to use the application. This time the wallet address does not match with the address from the admin account which means some functions are not available for the user for instance uploading any information to the blockchain. The user can only scan a QR code and check if there is any relevant information into the blockchain.

We can see in figure 13, after scanning the same QR code that was scanned and uploaded to the blockchain by the admin account, in the result section, the same information was printed. In addition to that, who uploaded the information was also shown. Finally, an Etherscan link was also printed so that the user can check by themselves that if the transaction is valid or not.

Even though this is just a demo with some small functionalities, this demo shows that there is endless potential of this technology. If it is to be integrated into the software industry, then useful applications can be built to solve complex problems today such as injection of fake drugs in the supply chain.

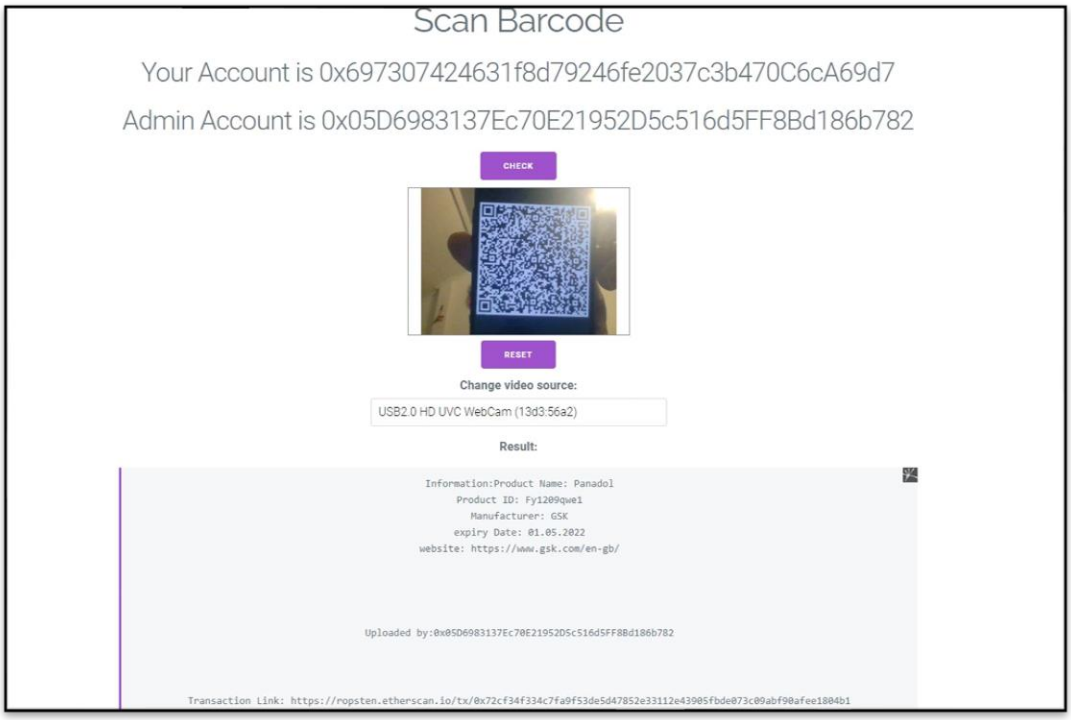


Figure 13. User checking a barcode and retrieving information from blockchain.

5.4 Code Description

In this section building of DApp is explained together with different functionalities.

5.4.1 Installing necessary components

The first step is to install node.js. After downloading and installing it from the Node official website, the following command can check that the updated version is installed.

- node -v; This will show the installed version of node.js in the computer.
- npm -v; This will show the installed version of npm in your computer.

The next step is to install express and web3 using the following command line:

npm install web3

npm install express

Finally, a Metamask browser extension is installed and an account is created. After creating an account, Metamask should be in the Ethereum mainnet. It has to be

changed into the Ropsten test network. This is because using Ethereum's main network will be time consuming and also expensive. The Ropsten network is faster to deploy and it is free. For any transaction that is performed in the blockchain, there is a fee to be paid. The fee is paid in Ether. Some Ether needs to be sent to Metamask wallet and it can be done using the Ropsten website:. This is a free way to send Ether to our wallet. Now that there is Ether in the Metamask wallet that will cover transaction fees the setup is ready.

5.4.2 Bulding the DApp

First, other applications and setup node-dependencies were tested locally. The following code was put in the package.json file.

```
{
  "name": "Treumed-Dapp",
  "version": "1.0.0",
  "description": "This is a demo app for Thesis",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1",
    "start": "node index.js"
  },
  "author": "Arafat Mollik",
  "license": "ISC",
  "dependencies": {
    "express": "^4.17.1"
  }
```

Code-Snippet 1: The package.json file

Some basic information, such as name and description were specified. Some debugging methods were written in "scripts". The main file is index.js which is specified in "main". In the dependencies we can see that I am using express framework for node.js is used. Now index.js was created.

```
var express = require('express');
var app = express();

app.use(express.static(__dirname + '/'));
console.log('App is running on 3500');
app.listen(process.env.PORT || 3500);
```

Code-Snippet 2: Index.Js file

This code means that if index.js is complied, then the express node will run at localhost and the port number would be 3500.

After that a smart contract was written. The smart contract was written in the solidity programming language. Two main functions are needed to complete the smart contract. One is to specify and authorize the user who can scan and “set” the product QR code on to the contract. The function is to allow all users to be able to scan the product and “get” the value of that QR code. Specify the admin account is shown below.

```
     function setProductDetail(string memory _productID)public {
          require(msg.sender==admin,"Only Admin 0x05d6983137ec70e21952d5c516d5ff
        8bd186b782");
         ProductDetail storage product=productDetails[_productID];
         product.productQR=_productID;
         product.owner=msg.sender;
    }
    function settransactionHash(string memory _productID,string memory _transact
ionHash)public {
         require(msg.sender==admin,"Only Admin 0x05d6983137ec70e21952d5c516d5ff8b
d186b782");
         ProductDetail storage product=productDetails[_productID];
         product.transactionHash=_transactionHash;
    }

    // to get product details stored using the QR

    function getProductDetails(string memory _productID) view public returns(str
ing memory,address,string memory) {
         ProductDetail storage product=productDetails[_productID];
         return(product.productQR,product.owner,product.transactionHash);
    }
```

Code-Snippet 3: Setting and Getting Product Detail

Now that the smart contract is written let us move on to the front-end. The following code loads or enables web3 and ask for the Metamask connection. If there is not Metamask, then the functionalities will not work.

```
async function loadWeb3() {

    console.log('loaded 1');
    if (window.ethereum) {
        window.web3 = new Web3(window.ethereum);
        window.ethereum.enable();
    } else {
        alert('Please install Metamask');
    }
}
```

Code-Snippet 4: Reading info from Metamask

Contract instances and variables could be created next. *web3.eth.Contract* object was used to convert the json format to low level ABI calls over RPC. This will allow us to interact with smart contracts as if they were javaScript objects. /11/ An example is shown below:

```
await new window.web3.eth.Contract(
        [
            {
                inputs: [
                    {
                        internalType: 'string',
                        name: '_productID',
                        type: 'string',
                    },
                ],
                name: 'setProductDetail',
                outputs: [],
                stateMutability: 'nonpayable',
                type: 'function',
            }
```

Code-Snippet 5: Creating instances

After creating the instances and variables the following code was written to verify if the user is an admin or a regular user. This function gets the account that is registered with Metamask and verifies if it matches with the admin account.

```
        async function getCurrentAccount() {
            const accounts = await window.web3.eth.getAccounts();
            return accounts[0];
        }

        async function getadminAccount() {
            const account = await getCurrentAccount();
            const message = await window.contract.methods.admin().call({ from: a
        ccount });
            return message;
        }
```

Code-Snippet 6: Get The account from Metamask

The following code loads all the functions and UI. The admin account is loaded and if it matches then we show the specific UI element that was meant to be shown only to the admin account which is scanning and uploading option.

```
async function load() {
    await loadWeb3();
    window.contract = await loadContract();
    const account = await getCurrentAccount();
    console.log(account);
    var admin = await getadminAccount();
    console.log(admin);
    if (account == admin) {
        document.getElementById('startButton').style.display = 'inline-block';
    } else {
        document.getElementById('startButton').style.display = 'none';
    }
    document.getElementById('account').innerHTML = account;
    document.getElementById('admin').innerHTML = admin;
}
```

Code-Snippet 7: Load all functions and UI

Below are the functions to add the barcode information to the Ropsten network and to check the information from the network. The getCurrentaccout function was used to make sure only the admin account can access this functionality.

```
async function addCode(code) {
    const account = await getCurrentAccount();
    const message = await window.contract.methods.setProductDetail(code).send({
from: account });
    alert('Transaction Confirmed');
    alert('https://ropsten.etherscan.io/tx/' + message.transactionHash);
    document.getElementById('result').textContent =
```

```
        'https://ropsten.etherscan.io/tx/' + message.transactionHash;
    const thash = await window.contract.methods
        .settransactionHash(code, message.transactionHash)
        .send({ from: account });
    alert('Transaction Hash Saved ');
}
async function checkCode(code) {
    const account = await getCurrentAccount();
    const message = await window.contract.methods.getProductDetails(code).call({
 from: account });
    if (message[0] != '') {
        document.getElementById('result').textContent = 'BarCode is:' + message[
0];
        document.getElementById('thash').textContent =
            'Transaction Hash is: https://ropsten.etherscan.io/tx/' + message[1]
;
    } else {
        alert('Barcode is not Found');
    }
}
```

Code-Snippet 8: Add and check the QRcode/Barcode

Now to access the camera and scan the barcode/QR code some code was taken from the Github website and added below functionalities.

```
codeReader.decodeFromVideoDevice(selectedDeviceId, 'video', (result, err) => {
                if (result) {
                    console.log(result);
                    alert(result.text + ' Will be added to the BlockChain');
                    addCode(result.text);
                    document.getElementById('result').textContent =
                        result.text + ' BarCode have been added To BlockChain ';
                }
                if (err && !(err instanceof ZXing.NotFoundException)) {
                    console.error(err);
                    document.getElementById('result').textContent = err;
                }
```

Code-Snippet 9: Open camera and read the info from Qrcode

The function above takes the text that is found from scanning the QR code and then sends it to the addCode function, which then sends the information to the Ropsten network. The following function checks if the contents of the barcode are in the blockchain or not.

```
document.getElementById('checkButton').addEventListener('click', () => {
            codeReader.decodeFromVideoDevice(selectedDeviceId, 'video', (result,
 err) => {
                if (result) {
                    console.log(result);
                    checkCode(result.text);
                }
                if (err && !(err instanceof ZXing.NotFoundException)) {
                    console.error(err);
                    document.getElementById('result').textContent = err;
                }
            });
```

Code-Snippet 10: Scan and retrieve info from blockchain

After this the code is finished. To compile this code, the command "node index.js" needs to be written After that in the http://localhost:3500/ the DApp should appear.

5.5 Upgrading the Application for real life implementation

In the Demo DApp demonstration, only two entities work were shown. One is the admin who represents the Manufacturer company and the other is the user who represents the customer of the product. In real life supply chain management, there is not only two but multiple entities that needs to be considered. There is a carrier, shipment company, retail company, local shop and many more. Even though the demo DApp demonstrates the concept of how the nature of transparency can be used to make our supply chain better, there is more work to be done if it were to be a real-life application. The possible implementation can be proposed as follows:

The manufacturer company will scan their product codes and upload it to the blockchain through smart contract. The product will leave the company and go through a shipment process. The carrier will execute the smart contract by confirming that he has received the delivery and processing to send it to the desired address. During this action the carrier cannot change or counterfeit the barcode/QRcode. He only has the functionality to scan and confirm that he has received the package and then adding additional information for instance where the package will be sent next. Then the package will be sent to the next carrier and that carrier will do the same process. Here, there is no way that the carrier can simply swap a fake medicine into the supply chain because the barcode would not match.

In addition, because the application does not use a centralised server, a hacker cannot change the barcode information and inject fake barcode information so that it would be easier to replace real drugs to fake ones. After the carrier has sent the package to the destination retail shop, the retailer will again scan the QR code and confirm that the package is received; he cannot change the product code nor can he change the information in the blockchain. After the retailer shop, the product may end up in a local store and thus to an end-user. The end-user will just scan the code and can see where and when the barcode was scanned and if the source of this supply chain is actually the manufacturer company or not. This is how the consumer can check the authenticity of the medicine or product using the power of blockchain technology.

6 CONCLUSIONS

To summarize, the DAPP demonstrated in this thesis can be a real-life solution to the counterfeiting problem in the supply chain system of not only medicine industry but also all other kind of industry as well, even though there are lot of challenges to this as well. For instance, to make this application work, all the parties or entities in the supply chain system must come to an agreement to be have a transparent database through blockchain. This might not be acceptable to everyone. Furthermore, there is an extreme demand of blockchain developers and scalable blockchain solution to make this model work. Probably within five years or so there will be enough developers and there will be more scalable blockchain technology other than Ethereum that can levitate the implementation of this application. The power of blockchain can also be used in many other applications in the medical industry, such as keeping medical records safe and secure, creating a secure delivery system of authentic medicines, paying doctors for online appointment. So many things can be achieved by leveraging the characteristics of blockchain technology. If we think about the past decade, we could not think that after 10 years, we can use technologies the way like some technologies we use today. So, maybe it is difficult to imagine how blockchain technology can conquer the cyber space but it is happening right in front of our eyes, until someday we are suddenly using decentralised applications on a daily basis.

REFERENCES

1. *Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware.* Davis, Jessica. s.l. : https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware, 2021.

2. *IBM Security Report: Attacks on Industries Supporting COVID-19 Response Efforts Doubl.* PRESS, RELEASE. s.l. : https://markets.businessinsider.com/news/stocks/ibm-security-report-attacks-on-industries-supporting-covid-19-response-efforts-double-1030115823.

3. *Dark Web Analysis: Healthcare Risks Tied to Database Leaks, Credentials-2021.* Jessica, Davis. s.l. : https://healthitsecurity.com/news/dark-web-analysis-healthcare-risks-tied-to-database-leaks-credentials, 2021.

4. *Mapping the scale of the fake pharmaceutical challenge.* s.l. : https://www.oecd-ilibrary.org/sites/fe58fe07-en/index.html?itemId=/content/component/fe58fe07-en#biblio-d1e3074.

5. Haber, Stuart and Stornetta, W. Scott. *How to time-stamp a digital document.* 1991.

6. *History of Blockchain.* BINANCE. s.l. : https://academy.binance.com/en/articles/history-of-blockchain.

7. *INTRODUCTION TO CRYPTOGRAPHY IN BLOCKCHAIN TECHNOLOGY.* Website, CrushCrypto. s.l. : https://crushcrypto.com/cryptography-in-blockchain/.

8. *What Are Smart Contracts?* s.l. : https://www.cryptoninjas.net/what-are-smart-contracts/.

9. Documentation, WEB3. *web3.js - Ethereum JavaScript API.* s.l. : https://web3js.readthedocs.io/en/v1.3.4/#.

10. *Intro to Web3.js · Ethereum Blockchain Developer Crash Course.* dappuniversity.com. s.l. : Gregory McCubbin.

11. *web3.eth.contract.* Docs, WEB3 Read the. s.l. : https://web3js.readthedocs.io/en/v1.2.11/web3-eth-contract.html.