## Czech University of Life Sciences Prague

## Faculty of Economics and Management

## Department of Information Engineering

## Bachelor Thesis

# Injecting the Element of Trust in Traditional Business Models Using Blockchains

**Dharmang Chokshi**

## CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

# BACHELOR THESIS ASSIGNMENT

Dharmang Pankajkumar Chokshi

Systems Engineering and Informatics
Informatics

Thesis title

**Injecting Element of Trust in Traditional Business Models Using Blockchains**

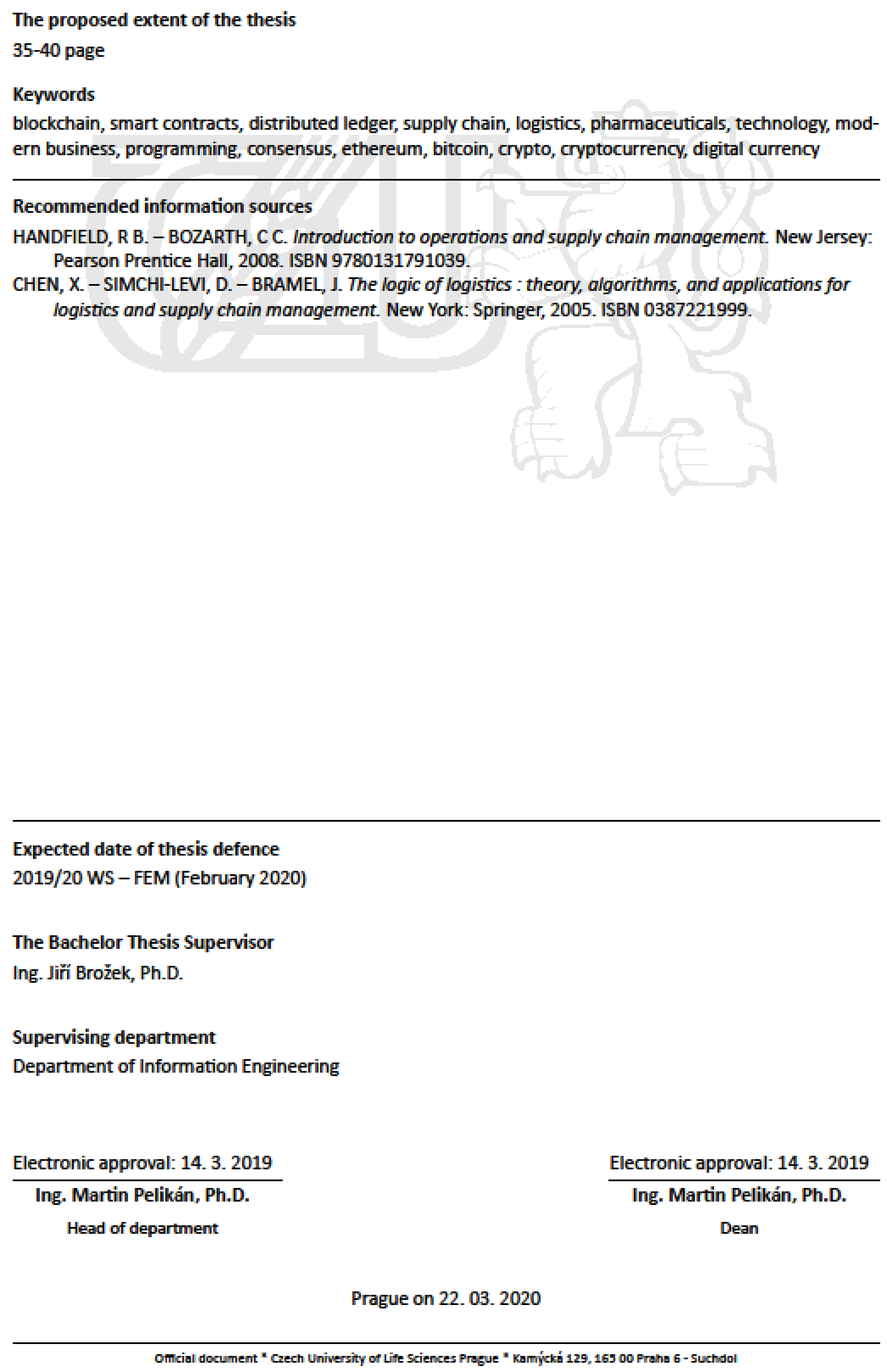
**Objectives of thesis**

The primary objective of the thesis is to identify the importance of blockchain technology and its applications which can be fused in traditional business models, to have a better transparency and clarity for the businesses in dealing with anything that includes any kind of transactions or interactions with external or third-party entities. So eventually, to induce the element of trust and robustness of any kind of agreement or promise as previously agreed upon by the two parties, between whom the interaction is happening.

**Methodology**

We will be exploring the core of the blockchain technology and by using its power and workings, we will foray into the applications which are built upon the functioning of the backbone of the blockchain technology, and that is smart-contracts. We will see the use cases of multiple industries including logistics and pharmaceuticals. We will also be comparing the effectiveness of having the smart-contracts in the mix vs. not having them.

The examples of smart-contracts will also be helpful in demonstrating that how ground-breaking technology like blockchain can be used to disrupt the processes of any business or a company, which can be streamlined for better output in all the dimensions of how a traditional business is done, to how modern day companies can take advantage of technology at our disposal.



**The proposed extent of the thesis**

35-40 page

**Keywords**

blockchain, smart contracts, distributed ledger, supply chain, logistics, pharmaceuticals, technology, modern business, programming, consensus, ethereum, bitcoin, crypto, cryptocurrency, digital currency

**Recommended information sources**

HANDFIELD, R B. – BOZARTH, C C. *Introduction to operations and supply chain management.* New Jersey: Pearson Prentice Hall, 2008. ISBN 9780131791039.

CHEN, X. – SIMCHI-LEVI, D. – BRAMEL, J. *The logic of logistics : theory, algorithms, and applications for logistics and supply chain management.* New York: Springer, 2005. ISBN 0387221999.

**Expected date of thesis defence**

2019/20 WS – FEM (February 2020)

**The Bachelor Thesis Supervisor**

Ing. Jiří Brožek, Ph.D.

**Supervising department**

Department of Information Engineering

| | |
|---|---|
| Electronic approval: 14. 3. 2019 | Electronic approval: 14. 3. 2019 |
| **Ing. Martin Pelikán, Ph.D.** | **Ing. Martin Pelikán, Ph.D.** |
| Head of department | Dean |

Prague on 22. 03. 2020

Official document * Czech University of Life Sciences Prague * Kamýcká 129, 165 00 Praha 6 - Suchdol

## Declaration

I declare that I have worked on my bachelor thesis titled "**Injecting Element of Trust in Traditional Business Models Using Blockchains**" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 18/03/2020 ___________________________

## Acknowledgement

I would like to thank Ing. Jiří Brožek, Ph.D. for his guaidance and feedback all along the way. Mr. Rajan Kumar Upadhyay for his time and insights that are reflected in the interview. And all others who adviced me and helped me throughout this thesis.

Especially, Lucie Flanderova, for her constant support and motivation, without her I would not have been able to manage my time properly and would have stayed hungry!

# Injecting Element of Trust in Traditional Business Models Using Blockchains

## Abstract

If we could eliminate the need and dependency of having middlemen and intermediaries in the world full of deals, if transactions were to be verified, recorded and executed autonomously without any third parties, it would just completely disrupt and eliminate an entire layer of trust and complexity from our ways of doing business and run enterprises much more efficiently. That is the power of blockchain.

Be it any industry ranging from finance to energy or manufacturing to retail, with its in-depth study and well-planned and well-executed implementation, blockchain has full potential of reaching its peak and providing greater efficiency and new business models with faster and leaner trading at a global level and not to mention the advantages of superior transparency and traceability and increased automation of commercial processes all around us.

**Keywords:** blockchain, distributed ledger, decentralised apps, smart contracts, supply chain, logistics, pharmaceuticals, technology, modern business, programming, consensus, ethereum, bitcoin, crypto, cryptocurrency, digital currency

# Obohacení Tradičních Obchodních Modelů o Element Důvěry Pomocí Blockchain

## Abstrakt

Kdybychom mohli eliminovat potřebu a závislost zprostředkovatelů a prostředníků v obchodním světě, kdyby transakce měly být ověřovány, zaznamenávány a prováděny autonomně bez jakýchkoli třetích stran, pouze by to zcela narušilo a odstranilo celou vrstvu důvěry a složitosti z našich způsobů podnikání a přispělo k mnohem efektivnějšímu řízení podniků. To je síla blockchainu.

Ať už jde o jakékoli odvětví, od financí přes energii nebo výrobu až po maloobchod, díky své hloubkové studii a dobře naplánované a dobře provedené implementaci má blockchain plný potenciál dosáhnout svého vrcholu a zajistit vyšší efektivitu a nové obchodní modely s rychlejším a štíhlejším obchodováním na globální úrovni, nemluvě o výhodách v podobě vynikající transparentnosti a sledovatelnosti a zvýšené automatizaci komerčních procesů všude kolem nás.

**Klíčová slova:** blockchain, distribuovaná kniha, decentralizované aplikace, inteligentní smlouvy, dodavatelský řetězec, logistika, farmaceutika, technologie, moderní obchod, programování, konsenzus, ethereum, bitcoin, krypto, kryptoměna, digitální měna

# Table of content

## List of pictures

# 1 Introduction

Since ages, businesses and Industries in all the sectors have been built and running on the basic principle of trust. Whether it is between multiple parties or between individual parties. However, this business of trust is about to be disrupted and transformed with the use of blockchain technology and its applications like smart contracts and distributed ledgers. Because, by harnessing the power of the smart contracts or distributed ledgers, we can actually eliminate our dependence and reliance on the factor of trust when it comes to dealing with external or internal entities. If we want to discuss the applications like distributed ledgers and smart contracts, we need to understand the concept of technology lying underneath of them, powering them, and that is blockchain technology.

I think it's important to understand the ecosystem in which the smart contract lives. The ecosystem is Blockchain. Blockchain is one of those buzz-word that we hear everywhere. On social media, consultancy magazines, in technology magazines as well. And it's also one of the most overhyped technologies that we can hear about, where many people believe that this will be one the most transformative technologies that they have encountered in a long time. So certainly, what we can deduce from that is that there is a lot of promise or expectations from the blockchain as a technology. However, there is a sober reality. The technology must work, and it also has to deliver certain business benefit. We also have to find use cases where blockchain actually makes tangible sense. We often have a very good business case, but we will find that solving that with a blockchain is maybe not necessary, that the traditional web 2.0 is more than enough for this case or especially in the real supply chain environment. The blockchain has a lot of promise and can deliver and the technology can solve the problem, but they may not be suitable business case, which means that the technology can be very expensive to implement or simply there is no demand for business partners (Crosby *et al.* 2016).

One of the "textbook use cases" that we read about in terms of logistics is end-to-end supply chain and especially in pharmaceutical industry this seems to be very interesting use case. If we want to track every single box of pills that we can buy in a pharmacy by scanning a code, you can actually prove the origin of its source. Theoretically this makes sense, but many of these use cases were implemented into production or found out that the people actually don't care that much and they have high trust in a retailer that produces or distributes the pharmaceuticals and they don't feel the need to verify that. They simply trust the vendor and they would expect the government will do the certain audits to make sure that they will provide a quality service. And that is something what we have to believe in terms of blockchain that the technology, as promising as it can be, it can only survive if there is a tangible business case as well (Pilkington, 2016). Having said that, it doesn't necessarily mean that the technology is wrong, that it will not live up to the promises. But there is certain curve that we have to go through, in order to validate how much of this promise can actually be delivered in a real life.

A distributed ledger is just another general ledger which is constantly updated with the entries that cannot be changed after recording them once, after they have been written. A distributed general ledger is spread all over the network and all participants or parties has a copy of the whole book of records. Records or entries in the blockchain network of the ledger can be of different types like contents (payloads) depending on the intended purpose, for example, transactions (bitcoins) or contract texts and instructions (smart contracts) or identity confirmations and asset transitions (asset management).

Blockchain can also be defined as a distributed ledger technology that can record transactions between parties in a secure and permanent way. By 'sharing' databases between multiple parties, blockchain essentially removes the need for intermediaries who were previously required to act as trusted third parties to verify, record and coordinate transactions. By facilitating the move from a centralized to a decentralized and distributed system, blockchain effectively liberates data that was previously kept in safeguard (Zheng *et al.* 2017).

What kind of impact could this have on everyday life?

Imagine in healthcare, sensitive data from all stakeholders ranging from patients to medical companies, could be shared using the highest levels of encryption and data protection to greatly improve service efficiency and quality. Or in finance, companies and customers could potentially adopt a common digital currency as an alternative to traditional money, reducing the cost of transfers and enabling micro transactions. And in logistics, data sharing across the supply chain could enable higher levels of transparency, empowering consumers to make better choices about the products they buy. These are just some of the many opportunities that blockchain presents (Mettler, 2016).

# 2 Objectives and Methodology

## 2.1 Objectives

The primary objective of the thesis is to identify the importance of blockchain technology and its applications which can be fused in traditional business models, to have a better transparency and clarity for the businesses in dealing with anything that includes any kind of transactions or interactions with external or third-party entities. So eventually, to induce the element of trust and robustness of any kind of agreement or promise as previously agreed upon by the two parties, between whom the interaction is happening.

The secondary objective is to explore the realms of smart contracts and distributed Ledger technology in such a way that they can be implemented and executed in parallel with the current functioning of any businesses. We will also be looking into the use cases of already established industry leaders in the sector of pharmaceuticals and logistics as well as supply chain businesses. We will also try to establish the fact that how and why using the blockchain technology can be beneficial for these businesses. We also need to take into consideration, where and how there can be obstacles faced for injecting the blockchain technology network, where it can be much more beneficial if we don't use it.

## 2.2 Methodology

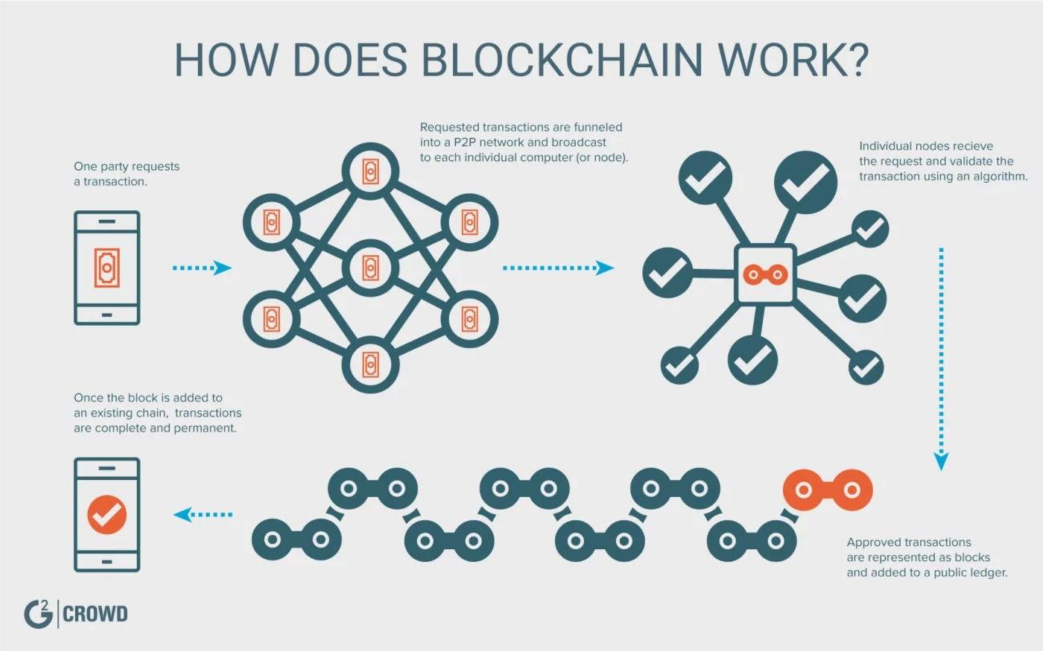
We will be exploring the core of the blockchain technology and by using its power and workings, we will foray into the applications which are built upon the functioning of the backbone of the blockchain technology, and that is smart-contracts. We will see the use cases of multiple industries including logistics and pharmaceuticals. We will also be comparing the effectiveness of having the smart-contracts in the mix vs. not having those (Sikorski *et al.* 2017).

The examples of smart-contracts will also be helpful in demonstrating that how ground-breaking technology like blockchain can be used to disrupt the processes of any business or a company, which can be streamlined for better output in all the dimensions of how a traditional business is done, to how modern day companies can take advantage of technology at our disposal.

# 3 Literature Review

## 3.1 Understanding Blockchain

Blockchain is a theoretically **incorruptible** digital **ledger** of economic **transactions** that can be **programmed** to record not just financial transactions but virtually everything of value.



HOW DOES BLOCKCHAIN WORK?
One party requests a transaction.
Requested transactions are funneled into a P2P network and broadcast to each individual computer (or node).
Individual nodes recieve the request and validate the transaction using an algorithm.
Approved transactions are represented as blocks and added to a public ledger.
Once the block is added to an existing chain, transactions are complete and permanent.
G2 CROWD

Figure 1: Blockchain Work Flow Fundamentals (Source: Brynne Ramella. G2 Learning Hub. https://learn.g2.com/what-is-blockchain)

The first word to be focused here is "**incorruptible**", what that means is that when something is deployed off blockchain, it is theoretically impossible to change it, to manipulate its data, to hack it. The reason why it is "**theoretically**" is because hackers have proven to be very innovative in a way they can solve the problems that were considered unsolveable, however if the blockchain is distributed at scale and there are a serious number of nodes, then there seems to be almost no computational power that can actually do that. Now, in a blockchain, of the size of bitcoin or ethereum, a lot of data points are distributed and the data scattered (Ahram *et al.* 2017).

The second is “**ledger**”. The ledger is actually record of transactions. The example of bitcoin – bitcoin is cryptocurrency and people use it to buy certain things of value or to invest the money. We are purchasing bitcoin and all these transactions leave a digital footprint. So there are records all over the ledger. And because these records are actually distributed in a ledger which means that ledger is replicated among multiple nodes all around the planet, that is what makes it theoretically incorruptible (Bürer, *et al.,* 2019). Because if we would have to hack the ledger and give ourself more money than we are entitled to, for example, then what we would have to do is you would actually have to hack all these different nodes that have this copy of the ledger. This makes it very safe but it is also something that is making it very slow. Because obviously if you are making a new transaction it has to be populated through all these distributed networks and update the entries in each and every node on the network (Biswas and Muthukkumarasamy, 2016).

The next word I want to mention is “**programmed**”. So that means that you can actually program a blockchain according to your preferences and make it function in a certain way to your liking, just like any other software that you can program in a programming language. But it is not necessarily true about all the blockchains, for example bitcoin, doesn‘t really allow you to write smart contracts but there are blockchains that are not only limited to the transaction recording and are not only about the ledger. Ledger can contain information and some of the information can be pieces of code. And that code is what we call “**smart contract**”.

The “**consensus**” means that if we want to validate a new transaction, the distributed ledgers have to agree with us, as this is indeed a valid transaction. If user on the network wants to record a transaction or input an entry to the distributed ledger, the validity of that transaction has to be confirmed by a defined set of users or other parties which are already on the blockchain network so that no one else besides them can manipulate or edit or change the content in an unauthorised fashion. To successfully achieve these all, the users or parties have to be interlinked via a common network and receive each transaction together at the same time parallally (Lemieux, 2016).

A set of predefined rules gives us the assurance of the integrity of the distributed ledgers. These rules have to be followed by all the parties without trusting each other or a central institution in between them. As a result of this algorithm, no central institution has the power to operate or manage the distributed ledger, thus, a shared distributed database managed jointly by all the users and parties involved.

So the 4 pillars of Blockchain are:

1. Distributed Ledger
2. Privacy
3. Smart Contracts
4. Consensus

### 3.1.1 Blockchain Fundamentals

When you are trying to purchase something authentic, you need to make sure that you are actually buying the real thing and not some cheap look-alike. How will you be able to guarantee that the product is indeed the original? You need to have the information on the subject, and you need to be able to verify that information in order to make a successful transaction. You need to have reliable sources of information which can be trusted and true sources that cannot be tampered with. However, in a present cyber world where everything is happening on the internet it is a lot harder to maintain this authentic source of trusted information which can be verified (Crosby, et al., 2016). The internet has had multiple cyber attacks happening by hackers and cyber criminals which include internet fraud, malware, banking hacks, credit card fraud, etc. It has become virtually impossible to maintain this authentic source of information. The solution to this problem can be solved by the technology called Blockchain. Blockchain can be used as a trusted source of information that can be verified and cannot be tampered or changed in any way (Underwood, 2016).

Trying to understand the definition of Blockchain: It is an ever-growing ledger that keeps a permanent record of all transactions that took place on the network in a secure and chronological order and cannot be changed or tampered with.

If dissecting the definition, we can understand the characteristics of Blockchain further. First, blockchain is an ever/growing ledger, which means that it’s just a file that is going to store the information of all the transactions that happened, and they are going to happen in the future (Zheng *et al.* 2018).

Next it is a permanent record, which means that all the information that is store in blockchain is permanent and it cannot be altered or deleted in any way.

Further we understand that it is a secure storage for the information. It uses every advanced cryptography method to secure the data in highest levels possible. Moving on, the definition also shows that the data is stored in a chronological order (Leonhartsberger *et al.,* 2019). That is based on the time that the transaction happens. These and a lot more features of blockchain help in making the network tamper proof. So that the information on the network cannot be hacked or tampered in any possible way.

### 3.1.2 Technical Aspects of Blockchain

The internet has traditionally been running on client server model. So, what is the client server model? This is a network created between the main server computer and the number of client computers which are connected to the centralised main server. The main server computer stores all the data and information of that particular internet application. For example, let us consider a banking situation. Banks usually provide internet banking facility to its customers through the internet. The bank has a main server computer in which it stores all the information and data of the customers. The customer is provided with a login credentials, that is a username and a password with which he can use to login on his personal computer and access this information on the main server computer (Saberi *et al.* 2019). The computer which the customer uses to login to his account becomes the client of the main server computer. The server computer and the client computer interact with each other and provide the customer with the information and data he is looking for. Usually, a bank has thousands of customers who are using internet banking and thus there are thousands of client computers that connect to the main server computer to access the information and data. So, this is how the client-server model looks.

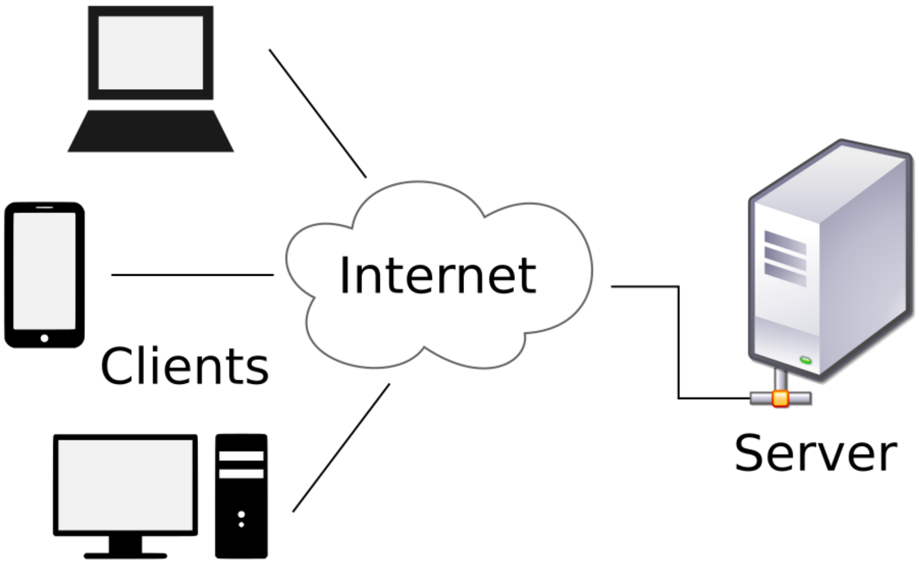


Figure 2: Client-Server Model (Source: Gnome-fs-client.svg: David VignoniGnome-fs-server.svg: David Vignoniderivative work: Calimo (talk) - Gnome-fs-client.svgGnome-fs-server.svg, LGPL, https://commons.wikimedia.org/w/index.php?curid=15782858)

This model enables thousands of businesses to provide internet-based solutions to the customers, where people can access their information using their login credentials. However, this particular system has proven to be prone to the hackers, viruses and other technical malfunctions. They have been extensive hacking operations by cyber criminals that affected corporations and governments all over the world and the cost of the damage has raised to millions and millions of dollars (Saberi *et al.* 2019) Hackers also got into banking infrastructure and stole credit card and other account information of millions of people all around the world. Governments and corporations are spending huge loads of cash to fund firewalls and other kinds of security protocols to protect their websites and data. But hackers are proving over and over again that they can bypass these protocols and access critical information. Moreover, this model is also affected by technical factors. If the main server computer is affected by some kind of a virus or some sort of a technical bug, the enter network will stop operating, because all the client computers are depending on the main server computer. Sometimes servers cannot handle huge traffic. This happens if too many client computers are trying to connect the server computer at the same time. These kinds of problems are not super problematic, but they definitely impact smooth flow of workflow (Saberi *et al.* 2019).

Moving on, blockchain is different. It works entirely different to the traditional client system. Instead of putting all the information and data on the centralised server computer, blockchain runs on the decentralized system of nodes. Nodes or individual computers that are spread all over the world all these nodes host and run the blockchain program. This system of decentralized nodes provides with a ton of advantages and improvements over the traditional client server model. First, there is a very small probability that the network will fail. Since in the older model the information is stored on the only one server computer, all the network will fail if that one server computer fails. However, in the case of blockchain, the information is not stored on one computer. It passes through thousands of node computers. So, if one node computer goes down, there won't be any effect on network, and it will still be operating. The only way when the blockchain network fails is by failing all the individual node computers that are hosting the network which would require events of global proportions and which is highly unlikely (Lemieux, 2016).

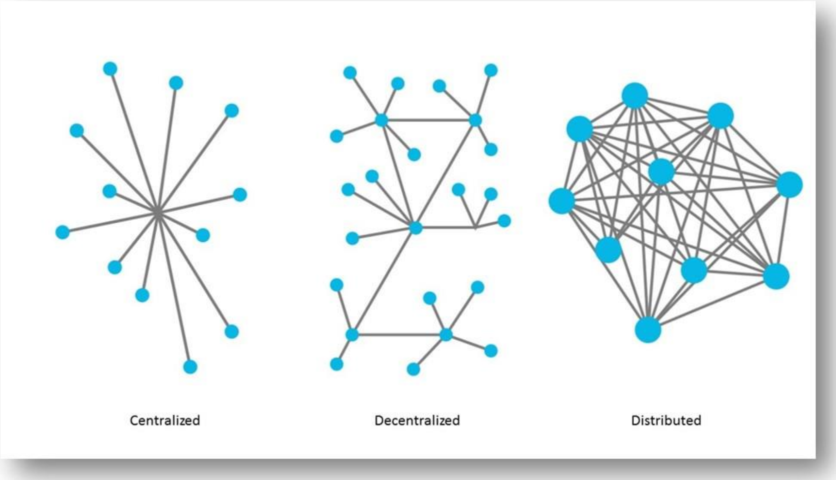


Figure 3: Types of Networks (Source: Christina Majaski. Distributed Ledgers. https://www.investopedia.com/terms/d/distributed-ledgers.asp)

Secondly, it is virtual impossible to hack a blockchain system. In the older client server model, the system uses only one server computer to store the information and data so the hacker only needs to hack into that one computer to bring down the whole network or steal the whole information. However, thousands of nodes running the blockchain network, the hacker will be requiring to hack into all the node computers simultaneously without being detected. So it is safe to say that the blockchain network is impossible to hack (Mougayar, 2016). Next, the information store in the blockchain network cannot be changed. In the case of a client server model, any person who has access to the server computer, can change the information or data store in the database. But in the case of blockchain network, the information on the network cannot be changed, because it is running on numerous node computers. Security is one of the biggest advantages of the blockchain technology and it has been proved to be more superior to the traditional system (Lemieux, 2016).

### 3.1.3 History & Background & Blockchain Ecosystem

*Origin*

1990s: The concept of distributed computing has been around since 1990

2009: Satoshi Nakamoto created bitcoin and introduced the concept of blockchain to create a decentralized ledger maintained by Anonymous consensus

*Transactions Era*

2011 – 2012: The deployment of cryptocurrency in applications related to cash

2012 – 2013: Currency transfer and digital payment systems

*Contracts Era*

2013 – 2014: Financial markets and applications using blockchain beyond cash transactions

2014 – 2015: Evolution of smart contracts

*Application Era*

2015 – 2016: Permissioned blockchain network solutions

2016 – 2017: Market evolution of development and exploration across industries

The technology of blockchain was originally developed to support the creation and development of bitcoin. As we are all aware, bitcoin is peer-to-peer virtual currency. We need to understand the development of blockchain, which has roots all the way in 1990's and paved the way to advent of a bitcoin. This will help in defining the features and characteristics of the blockchain technology (Lemieux, 2016).

During the 1990's people use some form of technology to edit pictures and alter them in the media. This process created a serious controversy and raised doubts which questioned the ethical and legal standards of the media. So in need to verify this digital information was created. Initially, programmers and scientists came up with the idea of time stamping a digital document. There were a few articles about this and it became viral because it questioned in a very fundamental way of how business is transacted with each other. They needed to find a way to verify when a document was signed or changed or altered in any kind of way (Pichler, *et al.,* 2018). They needed to make sure that the document could not be tampered with. Solution proposed was that rather than stamping the actual document itself, business should time stamp the actual data used in the transaction. This method prevented individuals from tampering the documents. This idea was later used in blockchain technology allowing it to act as a digital ledger and store the data and the time stamp of the transaction in such a way, that no one can tamper with them (Lemieux, 2016).

Also in 1990's, several papers were published by computer experts and data scientists explaining the need to improve the security capabilities on the internet. A shift towards more secured internet was necessary. The problem in established internet security protocols were exposed and it clearly showed how susceptible they are to hackers. On 31st October Satoshi Nakomoto released a white paper outlining the functions of his peer-to-peer virtual currency – the Bitcoin. Bitcoin runs on a secure system that uses both, the digital signatures and actual time stamps of the transactions. All these time stamp transactions would be hashed into a chain which cannot be altered or tampered without changing every previous transaction and thus make it virtual impossible to hack. Instead of having a centralised server computer which will run the network, bitcoin is run on a system of nodes as explained previously, nodes are just individual computers that people from all around the world who voluntarily provided to host the chain of the network. This provides the processing unit that is required to power the chain and maintain the network (Underwood, 2016).

In the client server model the hacker just needs to hack into only one computer which is the centralized server computer that stores all the information and data. But now in the blockchain network, hacking would be virtually impossible making it much stronger than traditional system. The important point to be remembered is that the blockchain and bitcoin itself cannot be hacked. But the wallets that people use to store the bitcoins can be hacked. So the people have to make sure, that the wallets are secured and intact. After the creation and implementation of the bitcoin, programmers started to realize the huge potential behind the blockchain technology and started to apply this technology into other applications. These other applications are also known as altchains.

### 3.1.4 Who is a Miner? What do they mine?

Miners are a group of people all over the world, which form the blockchain network, which in turn runs the bitcoin ledger. All the data of the network is stored in terms of blocks. Hence the name blockchain. Every 10 minutes a new block is added to the blockchain, which contains all the information of transactions that happened in the last 10 minutes. Like mentioned earlier, all these data is stored in chronological order which helps in implementing the security protocols of blockchain. Blockchain of bitcoin started all the way back on 3rd of January 2009 on which the very first bitcoin transaction happened. This very first block in a bitcoin blockchain is known as **“genesis block”**. From then all the transactions that ever happened on the network are stored on the blockchain in sizes of blocks (Underwood, 2016). Each block holds information on transactions that happened in the last 10 minutes of creating the block. Even right now, new transactions happen and get added to these blocks. Basically, anyone can become a miner. The only thing miners do is use their computers to process and confirm transactions that are happening on the network. Obviously, miners use very powerful computers with huge processing and graphical capabilities, which are specifically designed for mining bitcoins.

These miners solve the cryptographic-mathematical problems behind each transaction to successfully encode the transaction onto the network. For doing this, miners are rewarded with bitcoins. So, what it means is that miners earn certain amount of bitcoin for actually processing and validating the transaction. This is how new bitcoins are created in the network.

### 3.1.5 Hash & Hashing

In the previous topic I mentioned, that the miners solve the cryptographic-mathematical problems to encode a particular block onto the blockchain. Now I have to define the cryptography behind it (Underwood, 2016). What cryptographic-mathematical problem are they actually solving? We shall particularly talk about hash function called SHA256, which powers the cryptography of the bitcoin blockchain. The SHA256 stands for **secure hash algorithm** and it always have a fixed size of 256 bits. Hence the name. A part of a set of cryptographic functions developed by the NSA (National Security Agency). A Hash is a digital fingerprint of a set amount of data. It is a bunch of alpha-numeric characters that identify with a certain amount of data. When we use a hash generator, we can see what exactly SHA256 is. Let us take an example by using an online hash generator:

Data: This is my thesis.
Hash: 85343c9b9b7f57ff29978016424d727eff9d4e9155ba3ec4921a654b0c072679

Now even if I change a simplest of the detail in the data in the beginning of my statement, from a capital ***T*** to a smaller ***t,*** we observe that the hash of the new data changes completely:

Data: this is my thesis.
Hash: e6764cb1d8e97e18fee3bb9c80583064f52e8f438f18e9b17a6f3ab5c9c94b87

A hash of SHA256 always has a fixed length. It is always 256 bits. Secondly, a hash of the same data will always be the same. Next, a hash of a different sets of data is always different.

There is no way, two different sets of data will have the same hash value. Next, the SHA256 function is one-directional, which means you can convert data into a hash value but you cannot do the revers. You cannot get back into the original amount of data from any hash. Next, small changes in the data lead to significant changes in the hash value. Even if we change one character in the data, the hash value will change completely (Underwood, 2016).

## 3.2 Smart Contracts and Ethereum

One of the revolutionary technology that has born of the blockchain is smart contracts. Smart contracts facilitate exchange of items of value on the internet without a need of middleman or an escrow service. In actual sense the blockchain itself acts as a witness of contract when the two parties involved in the contract agree to draw a smart contract (Antonopoulos, A.M., 2014). The information in the contract turns into a block in the blockchain network, which is now visible to all the nodes of the network. However, the identity and the private information remains anonymous. Let me take a small example to understand how it works.

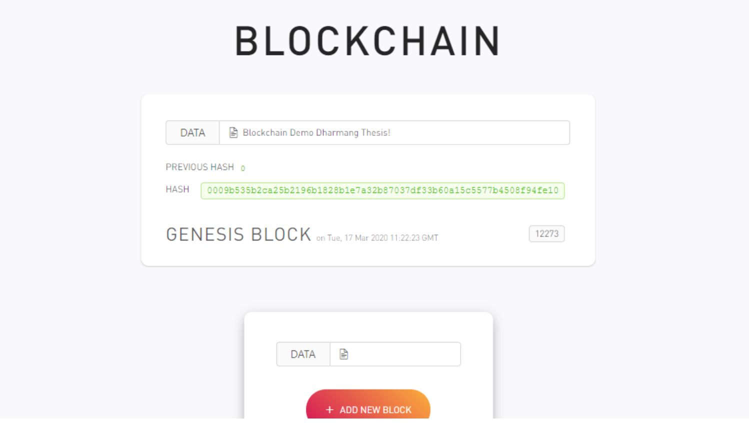
Imagine that Steve is selling a stock of a company and Bill wants to buy it. So both Steve and Bill will draw up a smart contract, sign it and date it exactly a week from today. Steve puts all the information that is needed to transfer the ownership of the stock to Bill and Bill deposits the money that should be paid to Steve (Bartoletti, and Pompianu, 2017). When the date of the contract arrives, the ownership of the stock is automatically transferred to Bill and the money is automatically paid to Steve. This example demonstrates how a smart contract works. This technology of smart contracts paved the way to Ethereum (Biryukov, and Pustogarov, 2015).

So what is Ethereum? Ethereum is an open source software that uses the smart contracts technology to facilitate development of decentralized applications (Cuccuru, 2017). Vitalik Buterin is the creator of Ethereum. He previously worked for bitcoin and realised that the potential is too large and so he developed this platform which allows programmers to develop their own blockchain network without actually creating an entirely new blockchain  Biryukov, and Pustogarov, 2015). Instead of doing that they just plug and play in an already existing ethereum blockchain. The virtual currency known as Ether is used to pay for the transactions that are utilizing the Ethereum blockchain network. People are also thinking about using the blockchain network or the blockchain technology to be used in voting. So rather than having to stand in line and vote, people can vote on their computers with zero possibility of fraud since we have already discussed it is impossible  to change or alter information  on the blockchain(Gerard,  2017).

# 4 Practical Part

## 4.1 Blockchain Proof-Of-Concept

Now that we know how the SHA256 Hash function works, let us now understand how this is used in encoding a block at the blockchain. As we have discussed earlir, the miners on the blockchain network are in a process of building blocks and encoding them onto blockchain. So let us see how a block is built. We shall use a web-app called blockchaindemo.io to understand how a block is built. Let’s just headover to blockchaindemo.io now.



DATA: Blockchain Demo Dharmang Thesis!

PREVIOUS HASH 0

HASH 0009b535b2ca25b2196b1828b1e7a32b87037df33b60a15c5577b4508f94fe10

GENESIS BLOCK on Tue, 17 Mar 2020 11:22:23 GMT 12273

Figure 4: Genesis Block of a Blockchain (Source: https://blockchaindemo.io/)

Now here is a block. The very first block on the blockchain is called a genesis block. So this block right here is a genesis block of all blockchain. Let us first understand the elements of a block. Every block consists of 6 elements. Let’s take a look at them. The first element of a block is index. Index is nothing but just a series number of that particular block. If we see the first block here, it is called a genesis block. In the next series of blocks, the index will show the serial numbers of those particular blocks.

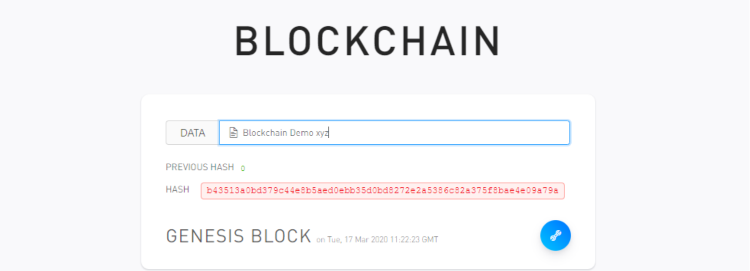
The second element is a time stamp. Right here in this block we have a time stamp of this particular block. This time stamp denotes the exact time of when this block is created. So on every block of the blockchain there will be a time stamp stating exactly when that particular block is created.

In the previous chapters we discussed that the blocks are added to the blockchain in a chronological order which means all these time stamps here in the block help in maintaining that chronological order on the blockchain (Underwood, 2016).

The third element of a block is data. This section here contains all the information of the transactions that happen. This is the actual piece of information that we want to store on the blockchain. It contains the transaction information and all the other details that go with it.

The next element of a block is hash. We learned that the hash is a digital footprint of the data that is stored here. So right here this hash is a digital footprint of the data that is stored in this section here. You can see here in this hash three leading zeros (Mettler, 2016). This leading zeros concept concept will help us in understanding if the block is valid or not. The next element here is the previous hash as the name suggests this section contains the hash function of the previous block. Here, since this is the genesis block which means there are no blocks spread to this, the previous hash is zero. However, when the next block is created, the hash of the genesis block will be stored as the previous hash in that block. Every succeeding block will store the hash of its previous block. This makes it possible to create chain relation of all the blocks on the blockchain and this is very important (Mettler, 2016).

The next element of the block is nonce. Here is the nonce of genesis block. A nonce is just a number satisfies the validity of the block. Let's just take a look at the hash for a second. We can see that it has 3 leading zeros. I stated earlier that these leading zeros help us in understanding if the block is valid or not. For example here this hash has 3 zeros. So this is the valid block.



BLOCKCHAIN

DATA Blockchain Demo xyz

PREVIOUS HASH 0

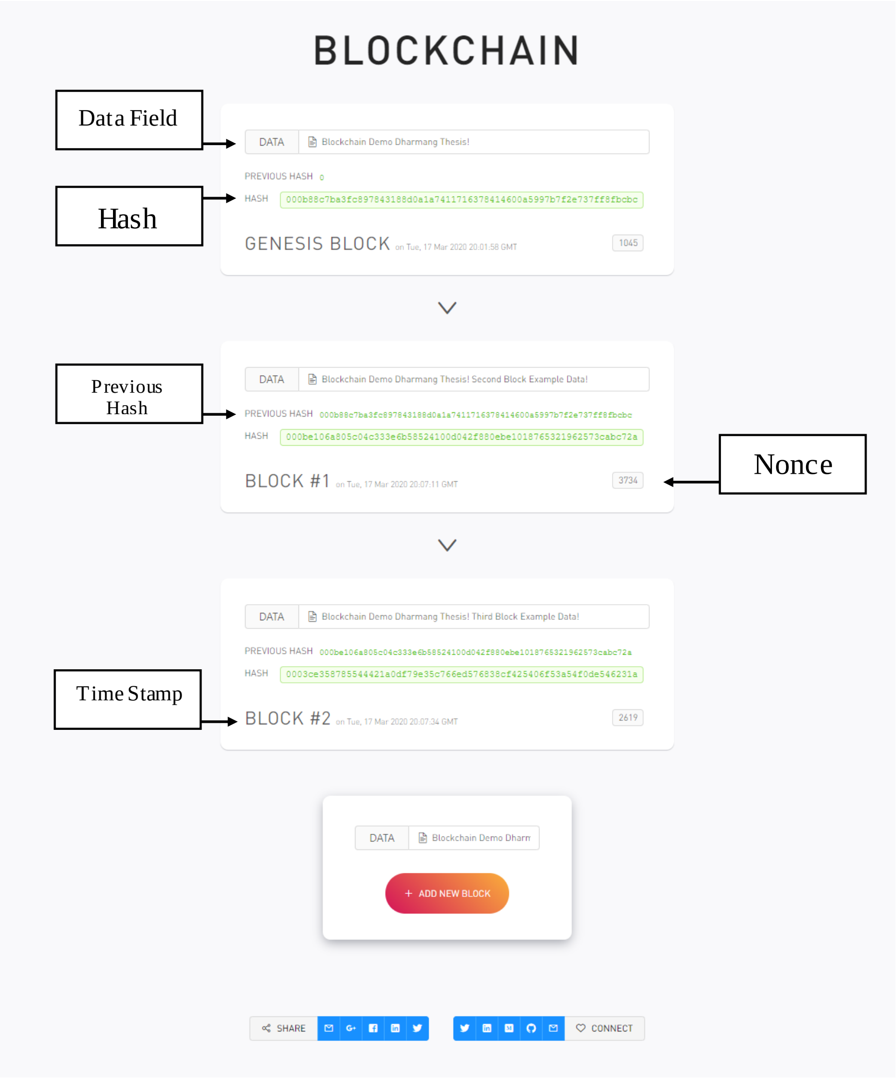
HASH b43513a0bd379c44e8b5aed0ebb35d0bd8272e2a5386c82a375f8bae4e09a79a

GENESIS BLOCK on Tue, 17 Mar 2020 11:22:23 GMT

Figure 5: Changed Hash Value for Modified Data (Source: https://blockchaindemo.io/)

If I change the data a little bit, we can see that these data generated a very different hash and we can also see that it does not have the 3 leading zeros anymore. Which means that this block is not valid. Now our task is to make this block valid. We need to find out the way to generate a hash with 3 leading zeros because only then we can make sure that the block is valid. Now, how do we do that. We do that by using this element called nonce. Nonce stands for number used once. Nonce is just a random number which helps us in creating a valid hash with 3 leading zeros for this amount of data here (Mettler, 2016). We need to figure out an exact nonce number which will generate a hash with 3 zeros and make this block valid. The way we figure out what the exact nonce number is by mining the block. So when we click on the mine button, the computer uses its processing power and runs all combinations of numbers from one all the way to millions to find the exact number that will make this block valid. So when I click here, the nonce number is found and it generated a hash value with 3 leading zeros and thus made a block valid. The most interesting thing here is that even if we changed a slight details on the data, all the index or the nonce will get a clompletely different hash and will not have the 3 leading zeros. It will make it an unvalid block. Let me change the data once more, and now this data generated a completely different hash and we can see that this block is invalid now because the has doesn’t have the 3 leading zeros. Now, let us mine it. And as we can see, we found the exact nonce number that satisfies this block and it generated a hash with 3 leading zeros and that made this block valid. This is how the SHA256 cryptography structures the validity of a particular block.

Now that we have understood the various elements that create a block, we understood a cryptographic function that validates the block, we shall go ahead and take a look on how all these blocks are linked together to create an ummutable blockchain. Immutable means that which cannot be changed.



BLOCKCHAIN

DATA Blockchain Demo Dharmang Thesis!
PREVIOUS HASH 0
HASH 000b88c7ba3fc897843188d0a1a7411716378414600a5997b7f2e737ff8fbcbc
GENESIS BLOCK on Tue, 17 Mar 2020 20:01:58 GMT 1045

DATA Blockchain Demo Dharmang Thesis! Second Block Example Data!
PREVIOUS HASH 000b88c7ba3fc897843188d0a1a7411716378414600a5997b7f2e737ff8fbcbc
HASH 000be106a805c04c333e6b58524100d042f880ebe1018765321962573cabc72a
BLOCK #1 on Tue, 17 Mar 2020 20:07:11 GMT 3734

DATA Blockchain Demo Dharmang Thesis! Third Block Example Data!
PREVIOUS HASH 000be106a805c04c333e6b58524100d042f880ebe1018765321962573cabc72a
HASH 0003ce358785544421a0df79e35c766ed576838cf425406f53a54f0de546231a
BLOCK #2 on Tue, 17 Mar 2020 20:07:34 GMT 2619

DATA Blockchain Demo Dharm

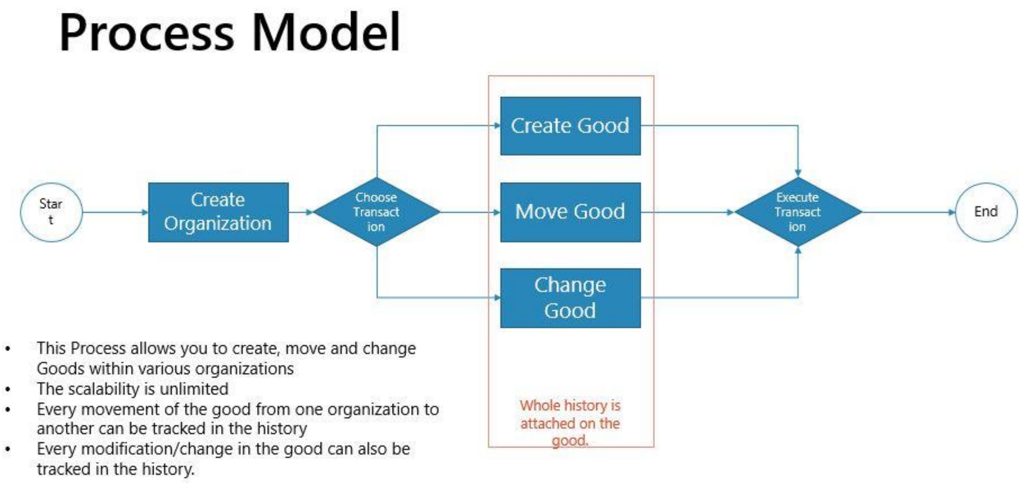
Figure 6: Anatomy of Blocks in a Blockchain (Source: https://blockchaindemo.io/)

Here we have a set of blocks in this blockchain: the genesis block, the block number 1, 2, 3, 4, etc. All the elements like index, time stamp, data, hash, previous hash, nonce are all present in all these blocks. We have the index which shows the serial number of that particular block (Mettler, 2016). We have the time stamp, that denotes the exact time when that particular block is created. We have different datafields, we have hash functions with 3 leading zeros, which means all these blocks are valid, we can also see that the hash value of the particular block is used in a previous hash section here in a very next block. Every block on a blockchain is cryptografically tight to the next block and this relation continues throughout the blockchain even when it has billions of blocks in it. In the genesis block we can see that the previous hash is zero. This is because there are no block before it. In the block number 1 we can see that the hash of the genesis block is used as a previous hash here. Similarly in a block 2, the hash of the block number 1 is used as a previous hash. In block no. 3, the hash of the block 2 is used as a previous hash and this follows on forever. This is what makes the blockchain immutable. If you change the content of any block, it will breake the validity of all the blocks next to it. A change in one block will not only make it invalid, but it will also break down all the blocks that are created after that particular block. This is because all the blocks in a blockchain are cryptografically tied together. Now we have to fix this block 1 in order to make it valid. We do this by figuring out the nonce number that can satisfy this block. So we noded to do that. First of all we need to mine this. We click on mine and the computer has generated out the nonce number which generated a hash with 3 leading zeros hence the block is valid now. Let me use this process to all the remaining bl`ocks to find out the exact nonce numbers that generate that hash values with 3 leading zeros to make all the blocks valid. So far we have spoken about the concept of 3 leading zeros in the hash which is required to find out if the block is valid or not. This concept of leading zeros is called the Difficulty level. The difficulty level is tied into the blockchain and it increases as more and more mining computers are connected to the blockchain network. This means the computers will take more and more time and more processing power in order to generate a nonce number which can satisfy and validate the block. Previously we learned that miners solve cryptographic-mathematic problems to validate a block. So the cryptographic-math problem is actually problem of finding the exact nonce that satisfies and validates the block. This whole system makes the blockchain network completely secure and immutable. If any hacker or intruder tampers with any of the blocks, all the blocks from that particular block to the end will become invalid. So, if anyone wants to temper with blockchain in this way, they will need to mine all the blocks again all the way to the front, faster than the rest of the miners in the world. They will need to have at least 51 percent of the total hashing power of the network under their control and they also need to do this completely under 10 minutes because new blocks get added to the blockchain every 10 minutes. That’s why it is virtually impossible to hack or tamper with the blockchain network.

## 4.2 The Hyperledger Composer

The Hyperledger fabric is not a public network per se as it grants access to only concerned parties linked to a specified framework/sector wherein data privacy or confidentiality is sine qua non. In effect, any prospective user of this network must first authorized and authenticated before gaining access.

It, however, remained highly decentralized and trusted; this is not unconnected to the fact that it is modular blockchain network. Moreover, it is this tendency that impacts impressive (unlimited) scalability on the network. The users eventual constitute a channel which is a subset of identifiable stakeholders that with unhindered access to data and are able to maintain a shared ledger unto which the (channel's) transactions are stored.



Process Model

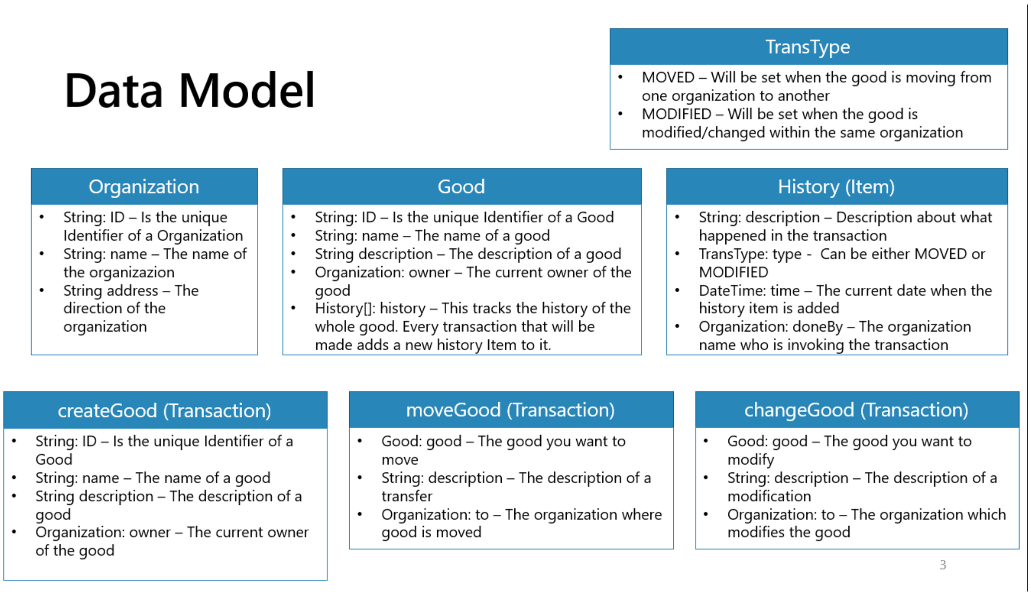
- This Process allows you to create, move and change Goods within various organizations
- The scalability is unlimited
- Every movement of the good from one organization to another can be tracked in the history
- Every modification/change in the good can also be tracked in the history.

Figure 7: Process Model of My Blockchain (Source: Author)

Going further, the execution runtimes, JavaScript SDK and connection profiles are among the essentials that are required to effectively implement the hyperledger composer. For one, the execution runtime in this thesis is hinged on distributed ledger and this is being linked with using cryptographic certificates. The JavaScript SDK enable developers to adequately manage and interact with the network with the aid of new applications created through node.js. On the other hand, the REST server uses loopback connector to create the open API that are required for the business network.

Beyond all these tools, the CLI also help in the management and deployment of business network definitions - the business definitions entail components such as the stakeholders, goods (assets), transactions and access control rules - while the playground web user interface is vital for ascertaining if a business definition will run on the execution runtime. In deploying the network, the information sourced from the fabric administrator is a prerequisite for creating another admin identity (PeerAdmin) vested with the responsibilities of installing and creating chaincode. The Yeoman code generators and VSCode extension are the tools that are needed for respectively generating the network skeleton and detecting errors while highlighting syntax.

The components which are vital for creating an efficient/interactive network usually run in the docker containers. These components include the two peer nodes and a single certificate for each of the organizations (i.e., Org1 and Org2), and also a single order node. Noted that the two pairs of peer nodes mentioned earlier must belong to a channel with a specific tag.



Data Model

TransType
- MOVED – Will be set when the good is moving from one organization to another
- MODIFIED – Will be set when the good is modified/changed within the same organization

Organization
- String: ID – Is the unique Identifier of a Organization
- String: name – The name of the organizazion
- String address – The direction of the organization

Good
- String: ID – Is the unique Identifier of a Good
- String: name – The name of a good
- String description – The description of a good
- Organization: owner – The current owner of the good
- History[]: history – This tracks the history of the whole good. Every transaction that will be made adds a new history Item to it.

History (Item)
- String: description – Description about what happened in the transaction
- TransType: type - Can be either MOVED or MODIFIED
- DateTime: time – The current date when the history item is added
- Organization: doneBy – The organization name who is invoking the transaction

createGood (Transaction)
- String: ID – Is the unique Identifier of a Good
- String: name – The name of a good
- String description – The description of a good
- Organization: owner – The current owner of the good

moveGood (Transaction)
- Good: good – The good you want to move
- String: description – The description of a transfer
- Organization: to – The organization where good is moved

changeGood (Transaction)
- Good: good – The good you want to modify
- String: description – The description of a modification
- Organization: to – The organization which modifies the good

3

Figure 8: Entity Diagram of My Blockchain (Source: Author)

The peer nodes are critical to the validity and secured nature of the network, and they can function as:

- A committer whereupon the peer acts to commit transactions to the ledger thereby contributing immensely to the ledger being updated and sustaining its integrity.
- An endorser whereupon transactions are stimulated upon the execution of chaincodes, leading to the validation of the result.

The orderer node, on the other hand, functions to determine the order that the transactions that will be added to the ledger will follow.

It is only after the organizations must have arrived at a consensus on the chaincode and the policies that will guide the activities in the channel, that the end-user will be able to invoke a transaction which the endorser will then stimulate by executing the chaincode.

Other tools that are required include:

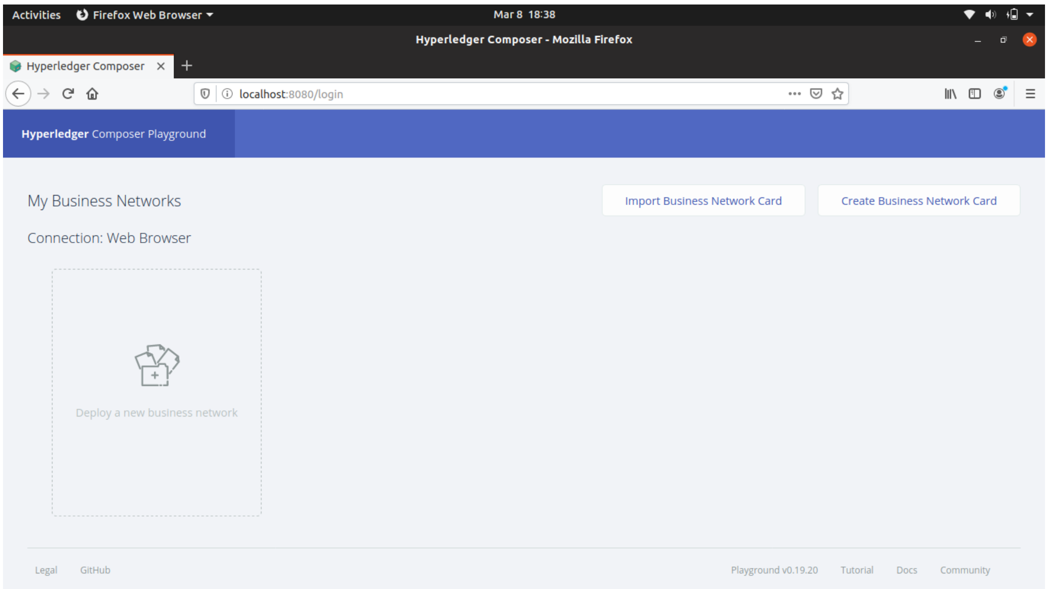
**Cryptogen-tool:** The cryptogen-tool is a tool that is very helpful in the creation of certificates and private keys that are needed for signing transactions and validating members of the network.

**Configtxgen-tool:** This is vital for the generation of the genesis block of the business network.

**Endorsement policy:** This is more like a set of instructions/rules that the peers responsible for the execution of transactions are expected to follow. It guides the peers on the process to follow in order to properly endorse a transaction.

**Building a network of trust:** Blockchain is primarily connected with trust as it allows transactions to flow through a decentralized system. Ordinarily (i.e., without blockchain), in the events whereby there are different stakeholder in the way a transaction plays out, there exists a high probability of non-conformity with the standard (laid-down) principles guiding that transaction. This is however curtailed with the implementation of blockchain. For instance, the logistics that encompasses the transportation/delivery of pharmaceutical products - or any other good - is known to be a complex undertaking that requires individuals who may have conflicting and or ulterior motives. Having a blockchain system in place first cut off the need for these ‘middlemen’ individuals and also ensures that the transactional flow is in no way tampered with while a specific good is being moved or modified. Again, the reliability of this system is further buttressed by the fact that stakeholders coming on board can easily refer to the history of the transactions previously executed.

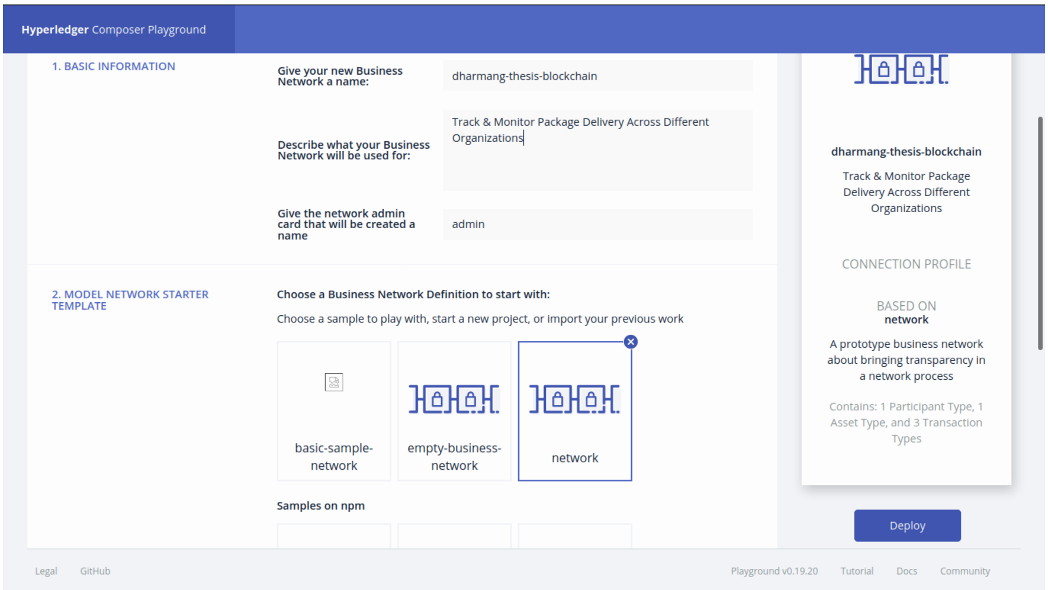
### 4.2.1 Procedure involved in deploying a hyperledger business network


Activities
Firefox Web Browser
Mar 8 18:38
Hyperledger Composer - Mozilla Firefox
Hyperledger Composer
localhost:8080/login
Hyperledger Composer Playground
My Business Networks
Import Business Network Card
Create Business Network Card
Deploy a new business network
Legal
GitHub
Playground v0.19.20
Tutorial
Docs
Community

Connection: Web Browser

Figure 9: Landing Page for the Deployment of the Blockchain (Source: Author)

Every step taken in the course of deploying the hyperledger (business) network is geared towards establishing its confidentiality and sustaining its security.



1. BASIC INFORMATION

Give your new Business Network a name: dharmang-thesis-blockchain

Describe what your Business Network will be used for: Track & Monitor Package Delivery Across Different Organizations

Give the network admin card that will be created a name: admin

2. MODEL NETWORK STARTER TEMPLATE

Choose a Business Network Definition to start with:

Choose a sample to play with, start a new project, or import your previous work

dharmang-thesis-blockchain

Track & Monitor Package Delivery Across Different Organizations

CONNECTION PROFILE

BASED ON
network

A prototype business network about bringing transparency in a network process

Contains: 1 Participant Type, 1 Asset Type, and 3 Transaction Types

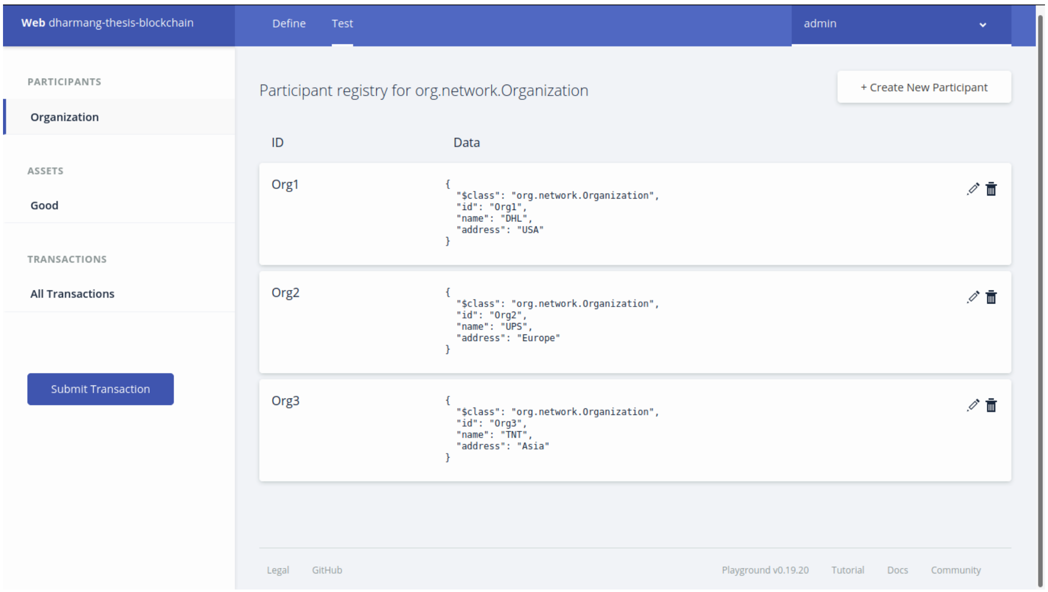
Figure 10: Selection of Type of the Blockchain Required (Source: Author)

So, with the blockchain network configuration already carried out and basic installations [like the composer development environment] in place, the next lines of action will be tailored to the deployment proper. It has already been established that the hyperledger composer solution network in this study involves three primary stakeholders - or rather organizations. These organizations will be tagged ‘Org1’, ‘Org2’ and ‘Org3’.

Org1: Refers to the owner of the good(s) that will be involved in the transaction.

Org2: Refers to the facilitator and transporter of the good(s) that will help mediate the transaction.

Org3: Refers to the stakeholder that will invoke the transaction. In other words, the one that will receive the goods.



Participant registry for org.network.Organization

| ID | Data |
|---|---|
| Org1 | {<br>"$class": "org.network.Organization",<br>"id": "Org1",<br>"name": "DHL",<br>"address": "USA"<br>} |
| Org2 | {<br>"$class": "org.network.Organization",<br>"id": "Org2",<br>"name": "UPS",<br>"address": "Europe"<br>} |
| Org3 | {<br>"$class": "org.network.Organization",<br>"id": "Org3",<br>"name": "TNT",<br>"address": "Asia"<br>} |

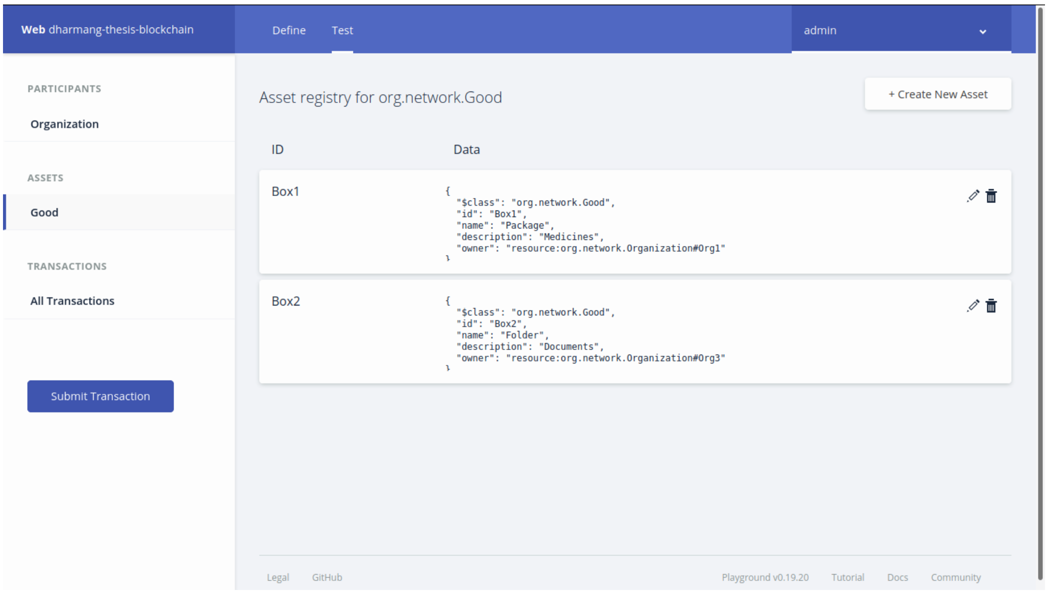
Figure 11: Creating New Participants in the Blockchain (Source: Author)

Going forward, the procedure is given as follows [under the following headings]:

### Stakeholder Accessibility

Bearing in mind that the network is not opened to everyone, it is needful to establish a network in which the two stakeholders can interact with using the Membership Services Provider (MSP). The title for each of these stakeholders is then configured with their certificate and private key files stored in a specified directory.

### Customization and Connection profile



Asset registry for org.network.Good

| ID | Data |
|---|---|
| Box1 | { "$class": "org.network.Good", "id": "Box1", "name": "Package", "description": "Medicines", "owner": "resource:org.network.Organization#Org1" } |
| Box2 | { "$class": "org.network.Good", "id": "Box2", "name": "Folder", "description": "Documents", "owner": "resource:org.network.Organization#Org3" } |

Figure 12: Creating Entities of Transactions in the Blockchain (Source: Author)

On the basis of the fact that the organizations that will be involved in the transaction are not nameless or generic, it is important that a connection profile [bearing each organization's certificates and private keys] be set up. This profile will eventually define the set-up of the network, highlighting the peers, certificate authorities, participating organizations, orderers and the channel that constitute the network.

### Locating the certificates and private keys

Starting with Org1, search out the certificate [for Org1] from the directory in which they were stored and name them after the organization in consonance with the connection profile. After this has been done, we move to locate the private key - which is used in signing the message (transaction) - of the same organization in the subdirectory in which it exists. Likewise, these processes will thereafter be implemented with Org2. It should however be noted that hashing of the message using the hash function, SHA256 must have preceded the signing of the message with a particular private key. This is a critical aspect of securing the network in order to ensure that the messages are not tampered with.

### Creation of business network cards

The business network card is required for connecting with the hyperledger composer which now runs in the docker container, and it can be made available to the participants [in the network] to perform transaction. The card is basically valuable for creating identity. Therefore, to create a business network card for both Org1 and Org2, a predefined command is run with reference to the connection profile specific to the organizations involved.

With the cards now created, an identity that can interact with the network is forged and the organizations can then transact with the possibility of a digital signature being appended by the (stakeholder's) certificate.

Each of the created business card network is thereafter imported into a wallet.

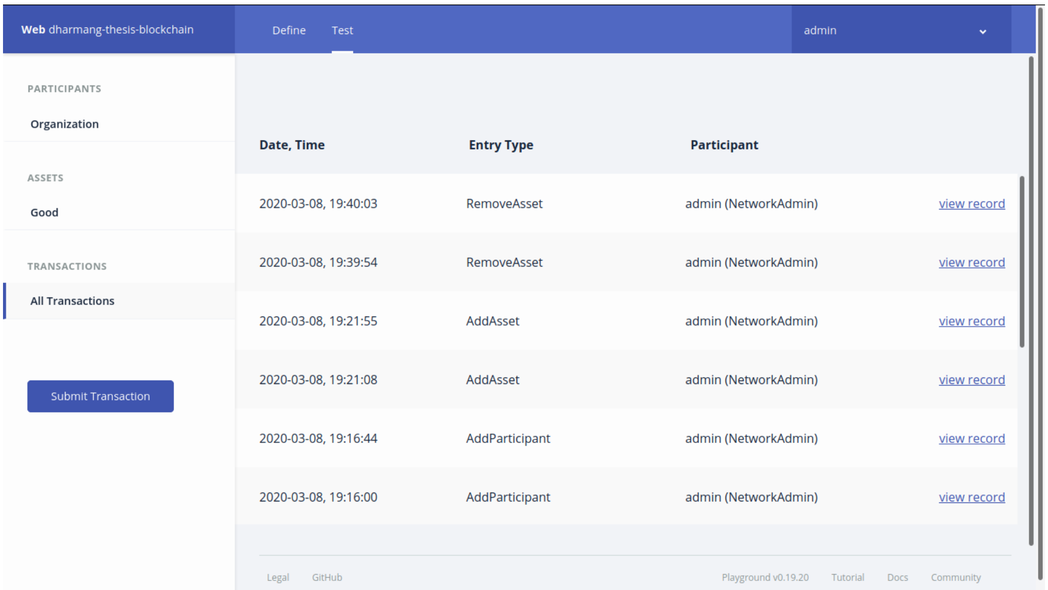
### Installation of business network onto peer nodes

A command is now run to install the network onto peer nodes for each of the organizations yet with reference to their specific connection profiles.

### Creating/establishing an endorsement policy

For the specificity of the business network in view, it is expedient that the default endorsement policy that is inherent with the blockchain be made redundant or done away with for one (endorsement policy) that will allow the stakeholders endorse a transaction before such is committed to the ledger. By implication, establishing an endorsement policy is sacrosanct to the successful deployment of the business network following a predefined order. Nonetheless, it has to be stated that there are two possibilities attainable when the endorsement policy is factored; it is either the participants agree to endorse a particular transaction or not - in the case of the latter, the business network will ultimately reject the (proposed) transaction.

### Defining the network administrators



| Date, Time | Entry Type | Participant | |
|---|---|---|---|
| 2020-03-08, 19:40:03 | RemoveAsset | admin (NetworkAdmin) | view record |
| 2020-03-08, 19:39:54 | RemoveAsset | admin (NetworkAdmin) | view record |
| 2020-03-08, 19:21:55 | AddAsset | admin (NetworkAdmin) | view record |
| 2020-03-08, 19:21:08 | AddAsset | admin (NetworkAdmin) | view record |
| 2020-03-08, 19:16:44 | AddParticipant | admin (NetworkAdmin) | view record |
| 2020-03-08, 19:16:00 | AddParticipant | admin (NetworkAdmin) | view record |

Figure 13: History of the Transactions of the Blockchain (Source: Author)

This is a key step taken towards laying out the responsibilities of the participants of the network. It is thereby necessary to specify the administrators for both Org1 and Org2 by retrieving their certificates. The administrators so selected will be responsible for bringing other participants on board from their respective organizations.

The hyperledger blockchain network - just like a typical blockchain technology - is known to be neutral and unbiased; this is due to the fact every administrator involved in it has equal rights and can interact with the network using his/her identity.

### Application in pharmaceutical supply chain

Ordinarily, the movement of goods from one organization (the manufacturer) to another (wholesaler) involve many complexities wherein the possibilities of manipulations in agreement and adulteration of products are not unlikely. All these border on the issue of trust, and this (trust) factor has often led to a number of losses. With blockchain technology however, such realities are taken care of as the issue of trust is adequately addressed. And, according to Puthal et al. (2018), this trust issue is effectively addressed due to the fact that blockchain technology is:

- Decentralized: There is no major controlling force or personnel seeing to its operation; plus, the need for a third-party intermediaries, who might complicate the transactional process, is cut off. Every participant has equal privileges and/or rights to execute certain laid-down actions.

- Irreversible: Once a transaction has been effected, with the peers endorsing it, there is no going back. Additionally, the transaction can be tracked and the stakeholders can always refer to the history where every transaction is recorded.

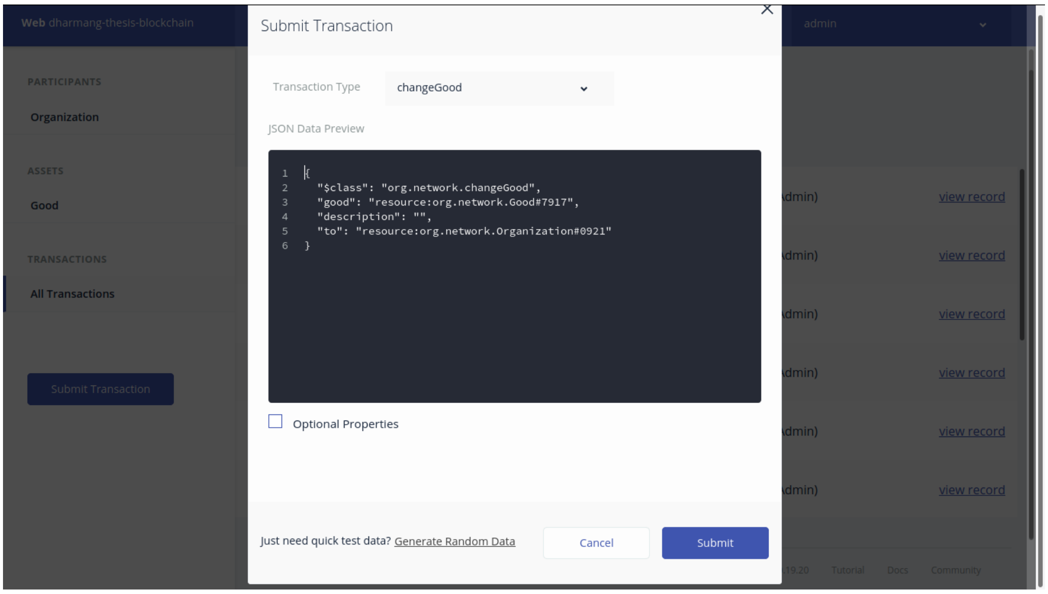
- Immutability: This is closely related to its irreversibility. With the hash function already accompanying each transactional message, it is not possible for any entity to alter or tamper with the network. What is even more interesting is that any attempt to tamper with a transaction does not go unnoticed (Mingxiao et al., 2017).

- Persistent: Overtime, blockchain technology has not been found to fail in ensuring that every transaction carried out on it seamlessly flows through a trustworthy network; right from the point of ordering to the point of receiving the item (good).

As the third-party intermediaries get cut off, the blockchain technology is much capable to take care of several activities entailed in the supply chain of pharmaceutical goods. In essence, it can aid in moving goods [after the agreement for such transactions must have been entered]; helps in verifying the authenticity of the cargo or medium through the goods are transported; ensures proper documentation of modification orders, receipts, purchase orders and other financial/accounting instruments, and also assist in keeping records thereby limiting the risk that may arise from legal matters (Mckenzie, 2018).

### Setting up the business network on playground

To set up the business network in this thesis on playground, it is important that I first delete the default contents in the script files.



Submit Transaction

Transaction Type: changeGood

JSON Data Preview

```
{
  "$class": "org.network.changeGood",
  "good": "resource:org.network.Good#7917",
  "description": "",
  "to": "resource:org.network.Organization#0921"
}
```

□ Optional Properties

Just need quick test data? Generate Random Data

Cancel

Submit

Figure 14: Code to Execute the Type of Transaction (Source: Author)

- For the purpose of the network, the following components will be created:

  - Participants: Organization that owns the good, the one to which the good is moved and the one that modified the good.

  - Asset: (Pharmaceutical) good, history of transaction (which can serve as a receipt).

  - Transaction: Create good (by owner) Move good (to a wholesaler), Modify good (by an organization).

  - Events: Using the ID of the participants.

  - Access control rules: Highlight the permissions of the participants.

- The enum for every participant is then defined.
- Based on our model file, the flow goes thus:

```
Enum Receiptstatus {Start
Create organization (owner)
Choose transaction
Create good
Move good
Deliver wholesaler
Wholesaler receive good
End
}
```

```
Enum Receiptstatus {Start
Create organization (owner)
Choose transaction
Create good
Modify good (by wholesaler)
End
}
```

- Our model file defines three participants in the network using:

  String: ID – Is the unique Identifier of a Organization

  String: name – The name of the organization

  String address – The direction of the organization

- Define the evident asset showing details on the date/time a transaction took place, the description and type of transaction that occurred, and the participants that were involved in the transaction. This is highlighted in our model file as follow:

  String: description – Description about what happened in the transaction

  TransType: type - Can be either MOVED or MODIFIED

  DateTime: time – The current date when the history item is added

  Organization: doneBy – The organization name who is invoking the transaction

  Asset evident identified by

```
evidentId {
String evidentdescription
TransType
DateTime lastUpdate
ParticipantType from
ParticipantType to
String fromId
String toId
ReceiptStatus Status
}
```

- Define the asset (good). The important information that can be used in distinguishing the good from others are given, as well as the organization manufacturing it, and the history that concerns the particular good. This is highlighted in the model as given below:

String: ID – Is the unique Identifier of a Good

String: name – The name of a good

String description – The description of a good

Organization: owner – The current owner of the good

History[]: history – This tracks the history of the whole good. Every transaction that will be made adds a new history Item to it.

```
Good identified by assetId {
String assetId
String assetname
Owner OwnerId
History historyinfo
}
```

- Define the transaction and event carried out by the owner of good and implement these in the script file.
- Having ascertain that the receipt status is at 'START', implement the 'create good' function.
- Query the blockchain to confirm the validity of the input of the fromId and toId parameters.
- Create evident and add it to the receipt.
- Update the receipt and emit the event from the blockchain.

The processes above show a sample how the business network in the model file will be deployed on playground. It intimates on how the peer-to-peer communication is established in order to ensure that the network remains trustworthy even as the standard is maintained all through. These would have been difficult to achieve in a conventional setting with two parties basing their business transaction on mutual agreement alone.

# Discussion

## 4.3 Summary

Since it is important that all parties that will be involved in a blockchain network follow certain laid-down rules, it becomes equally essential that the protocol flow through a clearly defined path. This informs the need for creating a flow chart that communicates this. To begin with, it is expedient that we specify where the goods will be coming from; such data are entered into the blockchain system and are ultimately made available to the nodes therein. Furthermore, information about the specific good, how it will be managed, as well as the kind of transaction(s) to be carried out [with such goods] is (are) also provided. Besides carrying the blockchain data, nodes also play a significant role in ascertaining the validity of a transaction and also propagate the transaction history across other nodes. More specifically, nodes monitor the voting process leading to the execution of a particular transaction.

All these are clearly displayed in the data model following after the process model, which more or less, serve as the layout guiding the operation. One will see, upon looking closely at the chart here, that it permits the movement and/or modification of good after such must have first been created from its owner. And, the data model details the identities and description of the transactions, as well as the organizations that were involved with the date and time clearly stated.

Plus, all these transactions can be seen by each party [via nodes] through the history provided thereof. This sort of possibility may be seen as encouraging some degree of transparency, but the secured nature of blockchain network is quite vast than this.

## 4.4 Limitations of Blockchain Technology

So far we have learned about how awesome blockchain technology is, we understood how this can actually improve the internet and various applications and make them much safer, faster and smarter. However, there are certain limitations to blockchain technology which will make it not suitable for certain institutions (Antonopoulos, A.M., 2014). We shall go ahead and understand the various limitations that effect blockchain technology.

Since blockchain is relatively a new technology, the knowledge of this subject is not yet complete. There are several misconceptions and a serious lack of awareness regarding this technology which is severe back drop for people and corporations to start using it. In new technology with a lack of awareness leads to less programmers or developers working on it. There is a serious lack of professional blockchain developers. The workforce is low for people to actually implement this technology in extensive levels. This is actually kind of a bummer (Gerard, 2017).

The main feature of blockchain is being tamperproof. Noone can change or alter the information that is once stored on the blockchain. This is the feature that makes blockchain so secured and bitcoin so successful. However, in certain usecases, people may want to go back and change or modify the information on the blockchain. For those kinds of applications blockchain isn´t really the way to go. Because it doesn´t allow any kind of modifications or alteration of information once it is stored on the blockchain.

Public and private keys – this is again an advantage that can become a problem sometimes. As we know, blockchain uses a very high level military great encryption to facilitate the security protocols. There are two kinds of keys –public and private keys (Antonopoulos, A.M., 2014). The private keys are the ones that people use to access their bitcoins on the network. However, if someone loses their key, bitcoins are locked away and sometimes there might be no way to get them back. Even if there is the way, it might not be very practical (Luu, Chu, Olickel, Saxena, and Hobor, 2016).

As discussed earlier that blockchain runs on the decentralized network of nodes. These nodes are thousands of computers spread across the world on which the blockchain network or the blockchain software is run. When we look at this scale, a blockchain network to run, uses a significant amount of energy on processing power. This actually exceeds the traditional systems by hundred and sometimes thousands of values. We already learned that once a miner finds the nonce that validates a block, the rest of the mining community verifies if the solution is actually right. Blockchain uses all the nodes on the network to process and verify this block of information before adding it to the blockchai (Gerard, 2017). But when we are building a larger blockchains with thousands of blocks being added every day, it usually means that the time being taken for processing the block and verifying it will be a lot more.

## 4.5 Misconceptions

We also need to understand some of the most common misconceptions that people have regarding blockchain technology and bitcoin. There is only one blockchain. In the general public he majority think that the bitcoin is the only blockchain (Cuccuru, 2017). The actual truth is there are hundreds, if not thousands of blockchains and more are being built every day. Bitcoin is just one blockchain and each blockchain is designed to solve a different purpose. There has also been a widespread misconception that bitcoin can be easily used for money laundering and other criminal activities, since it is known to be anonymous. First of all, bitcoin is not anonymous. It is pseudonymous. Most blockchains are public and they are traceable (Luu, Chu, Olickel, Saxena, and Hobor, 2016). In fact bitcoin is the most traceable currency right now on the planet. In 2007 a darknet marketplace is known as Silk Road was engaging in criminal activities like selling drugs and other kinds of criminal activities (Atzei, Bartoletti, and Cimoli, 2016). However, the FBI was able to back trace bitcoin transactions.

They cracked down the website and arrested the people behind it. People started believing that bitcoin is only used for illegal and money laundering purposes, however it´s not actually true. All transactions that are on the blockchain are traceable and mostly bitcoin can´t be used for illegal purposes. All blockchains are public (Cuccuru, 2017). Again, the bitcoin blockchain is public, but not all the blockchains are public. There are some completely private and sometimes semi-private blockchains. On the public blockchain, all the transactions carried on the network can be viewed and participated by anyone (Atzei, Bartoletti, and Cimoli, 2016). However, on private blockchains only people with respective keys can actually see and participate in the transactions.

The end of Fiat currency. Some people are assuming that bitcoin is going to replace all fiat currencies in the world (Velner, Teutsch, and Luu, 2017). However, this is impossible for now, because blockchains that are being built now are not capable of running the whole financial sector. Blockchains are slow. They cannot run financial operations at the levels of speed in which banking structures are run (Luu, Chu, Olickel, Saxena, and Hobor, 2016).

However, we can be optimistic and wait for blockchain to evolve into something much capable. Applies to finance sector only. There is also a misconception that blockchain technology can only be applied in a financial sector. As explained before, blockchain technology exceeds bitcoin or any other financial aspect.

Blockchain as a foundational technology is being used in several industries like real estate, health care, government organisations etc. (Velner, Teutsch, and Luu, 2017). There were also ideas of implementing blockchain technology for verification of documents, identification of people, fraud detection and also in voting system.

# 5 Conclusion

Rising measure of elements' activities is being re-appropriated, outsourced and businesses have changed chiefly and transformed into worldwide systems and global networks with built up worldwide operations. In-house production tasks and errands have changed the sourcing assignments, moving obligation to the administration of outside temporary workers. Logistics & Supply Chain industry span over several stages, over various areas, a large number of members are included, and various requests as well orders should be handled frequently spreading over an all-encompassing timeframe. Hence, challenges emerge when managing universal acquisition. Distinguished as one of the basic components of organization's technique and strength, the essentialness of acquisition as an inventory network practice has raised significantly. Business model and operations are an intricate procedure, the significance of which remains in its noteworthy capacity to improve the entity's upper hand.

Notwithstanding the past digitalization endeavours, low degree of straightforwardness, transparency and cross-system joint effort portrays production processes. Excess and redundant inner arrangements and simple gaps present between frameworks inside and over association's limits, enable just constrained deceivability into different system capacities. Visibility deficiency has been recognized as the root cause of dangers in expanded supply chains, particularly connected with the battle of acing information flows and data streams. Exchanges that combine countless stakeholders involved are slow and insufficient. Besides, bottlenecks are existent inside the various business procedures that are important to the continuation of business activities.

Complex operational & financial transactions in logistics and supply chain businesses can possibly be essentially disrupted by the use of creative blockchain innovation. The possibilities blockchain brings to such systems have already been, as of now, inspected and arrangements have already been proposed by spearheading ventures as well as different industries, albeit scholarly assessment is rare. The effect on singular supply network processes, be that as it may, has been skipped from the existent scholastic just as non-scholarly writings or literatures. Because of the vital significance of the individual business procedures, blockchain's importance for ironing out the transactional creases has been researched.

The capability of blockchain as an answer for the transactional procedures is considerable. The innovative technology has a solid ability to change the way sourcing and value-based elements of an operation are executed today. Recognized blockchain capacities improve generally perceivability and give total transparency in the system, just as, command and control over potential dangers, and disarray and errors in the correspondence of communication are decreased. Numerous advantages for running a smooth operation emerge from the implementation & execution of the solution, tended to, in areas of provider determination and the executives, improvement of sourcing practice, cost and time decrease, streamlining of the money related transactions, request for inventory and executive management, automation and upgraded risk administration. Moreover, numerous difficulties tended to as far as the transactional procedures and basic bottlenecks for procurement tasks can be moderated by the distributed ledger innovation. The blockchain offers an incredible chance to set up integrated virtual mix.

Most advantages, however, happen to substances working exceptionally broadened supply systems. For any organization that participates in generous business activities with a business-to-business contract subject to more than one level of providers, blockchain is a proper arrangement. Rearranging the tasks and the management, makes the whole procedure progressively proficient. In this manner, generally the network intricacy is brought down.

Be that as it may, investement in the beginning into the technology is high, because of the expense of the blockchain as well as the change of effectively existent organization processes and inner frameworks. Future possibilities of the blockchain, allude as a definitive innovation for supply chain coordination, helping organizations to drive their incentive through their supply chains. Today, blockchain innovation for organizations is still in the phases of early advancement, with numerous companies exploring different avenues regarding the designing of the most appropriate solution. However, the technological desires are colossal, considered to furnish organizations spearheading the arrangement with noteworthy and competitive gains.

# 6 References

Mingxiao, D., Xiaofeng, M. Zhe, Z., Xiangwei, W. & Qijun, C. (2017). A review on consensus algorithm of blockchain. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, 2017, 2567-2572. doi: 10.1109/SMC.2017.8123011.

McKenzie, Baker. "Lexology." 2018. Blockchain for Supply Chain Management: The Future of Logistics? Available at: <https://www.lexology.com/library/detail.aspx?g=a91330ea-99a9-45ac-bd39-0272a6dcd3e3>.

Puthal, D., Malik, N., Mohanty, S., Kougianos, E., & Das, G. (2018). Everything you wanted to know about the blockchain: its promise, components, processes, and problems. ResearchGate. doi: 10.1109/MCE.2018.2816299. Available at: https://www.researchgate.net/publication/326102908.

Scherer, M. (2017). Performance and scalability of blockchain networks and smart contracts.

Antonopoulos, A.M., 2014. Mastering Bitcoin: unlocking digital cryptocurrencies. ;Reilly Media, Inc.

Atzei, N., Bartoletti, M. and Cimoli, T., 2016. A survey of attacks on Ethereum smart contracts. IACR Cryptology ePrint archive, 2016, p.1007.

Bartoletti, M. and Pompianu, L., 2017, April. An empirical analysis of smart contracts: platforms, applications, and design patterns. In International conference on financial cryptography and data security (pp. 494-509). Springer, Cham.

Biryukov, A. and Pustogarov, I., 2015, May. Bitcoin over Tor isnt a good idea. In 2015 IEEE Symposium on Security and Privacy (pp. 122-134). IEEE.

Cuccuru, P., 2017. Beyond bitcoin: an early overview on smart contracts. International Journal of Law and Information Technology, 25(3), pp.179-195.

Dwyer, G.P., 2015. The economics of Bitcoin and similar private digital currencies. Journal of Financial Stability, 17, pp.81-91.

Gerard, D., 2017. Attack of the 50 foot blockchain: Bitcoin, blockchain, Ethereum & smart contracts. David Gerard.

Luu, L., Chu, D.H., Olickel, H., Saxena, P. and Hobor, A., 2016, October. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 254-269).

Velner, Y., Teutsch, J. and Luu, L., 2017, April. Smart contracts make bitcoin mining pools vulnerable. In International Conference on Financial Cryptography and Data Security (pp. 298-316). Springer, Cham.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B., 2017, June. Blockchain technology innovations. In 2017 IEEE Technology & Engineering Management Conference (TEMSCON) (pp. 137-141). IEEE.

Lemieux, V.L., 2016. Trusting records: is Blockchain technology the

answer? Records Management Journal.

Pilkington, M., 2016. Blockchain technology: principles and applications. In Research handbook on digital transformations. Edward Elgar Publishing.

Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L., 2019. Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), pp.2117-2135.

Sikorski, J.J., Haughton, J. and Kraft, M., 2017. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy, 195, pp.234-246.

Underwood, S., 2016. Blockchain beyond bitcoin.

Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018. Blockchain

challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), pp.352-375.

Bürer, M.J., Capezzali, M., de Lapparent, M., Pallotta, V. and Carpita, M., 2019, June. Blockchain in Industry: Review of key use cases and lessons learned. In 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-7). IEEE.

Leonhartsberger, K., Lettner, G., Chasparis, G., Vallant, H., Marksteiner, S. and Bieser, H., 2019, January. Decentralized Energy Networks Based on Blockchain: Background, Overview and Concept Discussion. In Business Information Systems Workshops: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers (Vol. 339, p.244).Springer.

Mougayar, W., 2016. The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons.

Pichler, M., Meisel, M., Goranovic, A., Leonhartsberger, K., Lettner, G.,

Chasparis, G., Vallant, H., Marksteiner, S. and Bieser, H., 2018, July.

Decentralized energy networks based on blockchain: background, overview and concept discussion. In International Conference on Business Information Systems (pp. 244-257). Springer, Cham.

Biswas, K. and Muthukkumarasamy, V., 2016, December. Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), p.71.

Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., 2016. Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), p.71.

Mettler, M., 2016, September. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) (pp. 1-3). IEEE.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H., 2017, June. An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.

# 7 Appendix

This is the transcript of the interview that I conducted with Mr. Rajan Kumar Upadhyay, who is heading the Digital Labs for DHL Group, based in Singapore. He heads all the Blockchain related projects and internal startups for DHL.

Me: Hello Mr. Rajan, good afternoon. Thank you so much for taking out time for this interview.

Him: Good Afternoon, Dharmang. It's my pleasure to help you with your thesis. Tell me, how can I help you?

Me: Basically, what I am trying to do and what we have been discussing with my supervisor is that currently, blockchain has so much potential and that potential outside cryptocurrencies are not fully examined. There are alternative solutions existent, for example directly by IBM or articles are existent describing outcomes of blockchain implementation into supply chain in general. But, what we are trying to focus on is how the blockchain would affect trusting different business partners, vendors, customers and other stakeholders in general. Whether communication with supply partners would be enabled in more efficient manner, or how transactions in terms of deliveries and paperwork will be handled. So basically, what we are trying to do, is to discover what potential impact blockchain would have for traditional business models, where the element of trust is vital.
If you don't mind, can I record this phone call for research purpose later on?

Him: Yes, sure. I understand what you are trying to accomplish here, so let's begin.

Me: So basically, the thesis is about injecting the element of trust in traditional business models using the blockchain technology. The thing is that I am also supposed to have a use-case scenario of a company, where I can prove it in my thesis as my thesis statement how the things have changed for logistics company for a supply chain business, for their operational processes before using a blockchain and after using a blockchain or something related to that and including a smart contract as well. So this is all its about and I wanted to get your insights, what you actually think? Is blockchain technology in your opinion able to add value to a supply chain in general terms like for example financial transactions are better or operational transactions are stream-lined or better than before? Do you think that?

Him: Yes actually. I see, basically the supply chain can be the most appropriate case, especially for the blockchains, so the reason because the supply chain grows with the various channels, the various tunnels and the various exchanges, you can say. There is a lot of middleman which is involved in-between and if you´ll see from the sourcing to and delivery, you know, the eternal life cycle, there is a lot of touchpoints, where the trust is needed and not only trust, but I think the smart contracts are those things that can bring some automation in place of trust and that’s where I feel the blockchain is significant into supply chain.

Me: True. So do you think that when this intermediaries and these middlemen, when they are eradicated or when they are removed from the whole cycle, is it going to impact them negatively or is it going to impact the businesses negatively?

Him: I see there is impact. Because the psychology is shifting. The business psychology as you can see and on the other side of the current situation, we will take an example, the corona threat that we have, what is really lacking in today’s situation is the trust, right? And I think the people they are looking for some authentic and trustworthy information, they are making sure that the product that they are buying is from authentic sources, especially we will take an example of these masks and these medical supplies. In these cases I feel the importance of blockchain is very evident, right? That is one part of it. On the other side that you mentioned, the adoptability, I feel this is more than changing the process than the technology because once you´ll see this process that people get to really get out of the traditional legacy, way of doing things. I think they need to get into some sort of automation and smart contract and the financial transaction where we can bring trust into this and we have some tokenization mechanism there can be more trust and all those things you know especially todays grave scenarios are very evident and that cannot be avoided.

Me: Ok, so according to you and according to your experience, the clients and the companies who are open to consider the implementation of such solution that you just mentioned into their day-to-day operations, is it going to be very smooth process or is it going to take a lot of awareness and updating the people, updating the base technology within the company to implement these measures?

Him: So I will see in the two aspects. One respect is the big players, especially the companies like DHL, Fedex and all those, I think that they will have a big struggle. Because they are kind of resistant to the change. If you really go with the blockchain and if I´ll see public blockchain space when we are talking about the openness, we are talking about the consensus from the public, something like that, we will talk about the public blockchain, I think the ownership of these companies might lose control of authority. I think that´s the reason you will see there is kind of race going on one of the public blockchain space between these companies, who will set up this public blockchain first. There is a lot of some lobbying in logistic world which is already going on. I think you might have heard about IOTA and those kind of things. So that´s one side of this you know. I think that is where the true value is for public blockchains.
The other aspect, is that the threat, in a sense like they are resistant to change on one side, on the other side we cannot really change the entire business model to all these different psychologies. This is not going to happen very soon, but I think eventually you will see there will be a shift in the mind-set, then at the same time I think the market and this even the technologies they are not mature. So these technologies will reach to certain maturity before enterprise started hopping on it. So I think both the sides, businesses, they really want to get into it that because they see that the whole world is getting into it and they might lose the market space or market share if they do not take the step earlier.

Me: So they want to keep themselves updated and not fall out of the competition.

Him: Yeah, exactly. I think that more important is to start early, then they have more advantage, if these companies do not have the market share or the share of that public space they might lose the bigger part of it. So I think that´s the one key area where they have to change as they are resistant to change and the market is volatile and fast-paced, and the blockchain is not very mature, I think you realise that the market, especially the blockchain is suffering with how the shift in transactions happen, how slow the miners are, and many other things. For enterprise, it is not yet ready to adopt them and at the same time the blockchain is not very mature as that, so the enterprise will risk the business. So slowly I think the change will be constant but very gradual.

Me: So when we talk about this downside, how do you think that we should be or the enterprise should coop up by first spreading the awareness and getting people on board. How do you think we can tackle this downside?

Him: I think this is basically, I think the large enterprises, and I am talking about the importance to bring this capabilities because I think we are saying that the blockchain may not be the immediate technology. You know, you can get into that possibly and start making revenues right away, it will take time. There are certain part of the ecosystem which is already matured, for example we are saying the applications for the blockchain which is already mature, that is the bitcoin, ethereum, and at the same time, there is another part of the eco space which is still experimental, still explorative in the nature, for example we are talking about distributed apps, we are talking about smart contract, lets take an example, we are talking about how the consensus work, we know all these things how the synchronisation of different, protocols and how they are linked to the different networks there are a lot of exploration which is going on.

Me: So you are saying that blockchain is much more beyond than just cryptocurrencies, right?

Him: It is, it definitely is. I think the cryptocurrency is just one transactional part of it. Specifically in the supply chain space, I think that the supply chain or the side is very demanding, you will see the global trades are going up constantly and the volume of it is going up, especially we are talking about these parcels and all those and at the same time the psychology towards the blockchain, that is common, I think that makes it more trustful and trustworthy environment and there is a lot of maturity which is needed for enterprises to adopt these technologies. So I think that´s where the gap is, especially the enterprises I feel they need to invest into two ways. The one thing they need to carry out what they have, that today operations and at the same time they need to bring automations by removing certain these middlemen, I am not saying that you can forcefully go to the blockchain, but slowly start adopting certain piece of the blockchain, into your work space, you know I would say into your business space.

Me: So basically what you mean to say is that blockchain as an eco-system can be incorporated in a business model, modularly. If I have to ask this question like if blockchain is collaborating to large extent with smart contracts and if these are already established because of the blockchain, then can blockchain lead towards automation of the processes and help to streamline the activities between the vendor and the vendee?

Him: Exactly, I think that´s the purpose, because blockchain is not only facilitation but removing of those bottleneck processes, removing those middlemen, you know by having the smart contracts in case. So bring the automation in it. I think that´s what I see as another efficiency of having a blockchain. One thing is also the trust, the second is the distributed nature of the information, and the third thing is the automation.

Me: But when we are implementing all these changes, so do you think that can blockchain assist and mitigating the risks related to already established business processes or are there some new risk that can emerge while trying to implement these changes for automation and everything?

Him: Actually, well, since you asked for the question about the processes. I think that this is the real reason why the logistic industries a little bit struggling. Why I am saying the processes because usually if you see the transactional space of the blockchains is very much matured. So if you see how people understand bitcoin, almost every technical person understands it. The whole ethical, you know the background of it. But if you ask how they understand the distributed apps works, how this consensus mechanism works, how the blockchain, especially in the automation space works, the people have a very different responses. Very different emotions I can say. The reason is because this particular piece is not very mature you know. From the one side we are saying that they you know the blockchain technologies which are in the private blockchain so I can say space like the private permissive or private non-permissive, which is actually private blockchains which can actually engage as a basically more like a lobbying between two companies you know to understand from that aspect.

And the second space you are talking about the public the blockchain space where we are saying, there is no central authority, no control mechanism, we are talking about the public consensus, something like how bitcoin works. So this is kind of two different thoughts which is going on how to still keep the ownership on this but at the same time how we can bring the trust and the transparency like the bitcoin does in the blockchain space. I think it will take some time to really synchronise this gap in the future and I think at the same time all these psychology, the processes, you know, that will come to some maturity before enterprises can start adopting it.

Me: OK, so do you think that with the blockchain technology companies are stimulated to outsource more of that value added services then?

Him: I will say no. The outsourcing is never a solution, because sooner or later the blockchain is not going to be a technology. I think the blockchain is going to be the whole ecosystem. So I feel you cannot divide it. So you need to bring in capabilities to cater those technologies and let your business understand because it´s not about just a technology, it´s about processes, it´s about automation, it´s about how the legal works, how the financial works, it´s about the synchronisation between the business units, it´s about many things. This is the whole psychology and that is the reason why you cannot outsource it. So this is more like a build versus buy or build versus borrow. It depends how you really want to make it. I possibly feel that these enterprises they need to slowly build the capabilities in-house and they need to start investing in these process automations, they start investing in the technology or the blockchains and let your people up-skill on this. So that sooner or later once the technologies reaches a certain maturity then more and more processes you can start adopting within it.

Me: So when we talk about this, then according to you, what will be some of the decisive factors for an enterprise or a company to actually consider the use of blockchain for their business processes, like what will be the decisive factor for them to incorporate the blockchain technology into their business sooner than later?

Him: So there can be many factors for that. The one thing is of course you can bring a trust into this, so for example if I am buying certain medicine let´s say online then what or how the trust factor I can take is necessary. If there is a blockchain, I can see the actual source of where these products were brought and I can see the various stages of tracking, I know this is very authentic source you know. I can mine it. I think it´s the first value I see, the value in the sense like bring more traceability in the trust, so that's an authentic product, there's an authentic delivery, all these things are happening, I think that can be the one. The second area can be where I clearly see the blockchain is already mature is adopting some token based, some transaction based mechanisms. For example payment transaction, take an example. That´s what I see, I think there is another economy space which is growing up is shared asset of tokenisation. I am not sure you heard about this, this is also coming into the blockchain very aggressively. So once I say this asset tokenisation what it means let's say one shipment might have, you know, ten different small items, and each one, the cost of that is being shared, you know, by the token. So I will give an example, maybe you can understand this little better. Like in UK, especially the real estates, this is getting very common, let's say that the builder has to start building or some shopping complex, take an example, so what they can do, they can go to the market, they can issue a token and then everyone buys the token and he can get that investment which is needed to make the shopping complex. So usually what happens is, there is one shopping complex but the ownership of that shopping complex is distributed by that token. So those who owns more token, has more of the ownership into the shopping complex. Interestingly, the shared economy concept is also gaining traction in the form of an asset tokenisation and I think this is also growing up as another space in this eco-system.

Me: Wow! This is so interesting that I need to do more research into this particular field.

Him: Yeah, exactly. Let me take another example, let's say that the shared economy is really growing up. Even within the DHL, the supply chain unit is taking a lot of interest in this field of shared economics, including the procurement and warehouse and many other things. So I think the distribution of this can be done with asset tokenisation so that the people who get the token, can own that particular piece of the process, or that piece od area or that piece of services via the tokens. So ideally what happens is that one warehouse will have thousand owners and each one can have their tokens as a proof of ownership.

Me: When we are talking about operational activities of a business there are current technologies existent such as enterprise resource planning, supply chain management software, electronic data interchange and so many more. Do you think that blockchain has feasibility to replace all of these and does it actually make sense to replace them? Are these going to disappear with the implementation of blockchain or blockchain will just play a supporting role?

Him: No, the blockchain will play a disruptive role over here. The reason why I am saying this because, you'll see the current business model, the way it looks like right now, that what is really missing is the transparency, in terms of cost, in terms of process smoothness and the lobbying or transparency with some advisory. Transparency is the big piece which is missing. Some of my colleague has got some special privilege but I did not get any special privilege, this thing is not visible at all in the market, the trust is entirely missing. I think for that reason I see that the blockchain is really going to bridge that gap. Because it works in a transparent way, by not relying on the information provided by you, but rather on the information that I mine. So whatever you are saying is correct and there is no middlemen and things are automated. That's also one of the reason why I don't have to deal with the lobbying. Since these smart contracts are self-executable so I really don't bother about the performance and everything is in place.

Me: How does it actually work if I as a big company decide to implement blockchain into my SC. Do I need to get all of the suppliers agree on that and agree also on the implementation policy?

Him: No, not really. As you might have known that there are already a lot of blockchains built specially for supply chains and for example there are a few blockchains which are government initiatives. I'll give you an example, Dubai has already set up their own custom national blockchain so anyone who has to pass through Dubai to integrate their applications into the master national blockchain. So the government see the value in being traceable and the trust factor of course. The second thing I would like to highlight is the private area, take DHL for example, DHL can be considered as a pioneer in developing blockchains for supply chains and especially cross-border shipments. Recently, I have been contacted by a unit in DGFF for setting up a new blockchain, but for some reason that project didn't move forward. That was related to a blockchain on Norway's salmon fisheries. Let's say today, if you buy a salmon from the market, we really don't know that if the salmon is authentic or whether the source is organic or inorganic, I don't know. You simply buy it or take it. So here if a blockchain placed, you can actually see which shipment company actually delivered it to your shop, across different locations, customs, everything you can check there. In fact you can see from the very sourcing of the egg, where the egg was formed and which egg was formed into a salmon that you are eating now. So traceability of the root-cause is the main point. It is possible by a chain of blockchains. So there can be classifications, there can be shipment, there can be sourcing, there can be manufacturing, all those things can be connected to a blockchain.

Me: Thanks for the insight. Are there some other aspects in businesses that can be addressed with blockchain that we have not mentioned yet?

Him: I think till now, we have covered mostly everything about business processes, that defines almost everything that an enterprise needs or is arise by a company's pure existence for its application layer. Of course I feel that there is a lot, but given the time constraint and the purpose of your thesis, its pretty much all. Considering a fact that we have covered a big part of an operational model is important because if you need to change your business direction, you really have to change your operational model.

Me: I agree. So that would be it Rajan, thank you so very much for your time and insights. I really appreciate it.