University of Economics, Prague

Faculty of Informatics and Statistics

Analysis and Design of a New Supply Chain Management Concept in Pharmaceutical Industry with Blockchain

MASTER´S THESIS

Study program: Applied Informatics (ISM)

Field of study: Information Systems Management

Author:
Efe Adalıer

Supervisor: Ing. PhDr. Antonín Pavlíček, Ph.D.

Prague, April 2019

Declaration

I hereby declare that I am the sole author of the thesis entitled “Analysis and Design of a New Supply Chain Management Concept in Pharmaceutical Industry with Blockchain”. I duly marked out all quotations. The used literature and sources are stated in the attached list of references.

.

In Prague on……... Signature

Acknowledgement

I hereby wish to express my appreciation and gratitude to the supervisor of my thesis, PhDr. Ing. Antonín Pavlíček, Ph.D.

I am very thankful to my dearest teacher Zeynep Maraş and my brother Ege Adalıer for proofreading my work.

Also, I am very grateful to my parents who never stopped supporting and encouraging me during my studies at the University of Economics.

Abstract:

Blockchain is a revolutionary technology and a new approach of sharing data securely between computers, thus it can have a huge impact in the industry and change business models in an efficient and innovative way.

The aim of this research is to analyze whether blockchain technology can be integrated in pharmaceutical supply chain processes in order to improve the control over operations to initiate efficient and secure delivery of medical products.

The research gives information about historical and technical background of blockchain, defines pharmaceutical supply chain processes and identifies the use cases of blockchain concepts along with pharmaceutical supply chain processes by documentary analysis as well as case studies of three companies.

During the research it was discovered that blockchain features can make big improvements in pharmaceutical supply chain. Establishing a private blockchain network between organizations involved in supply chain can solve counterfeit drug problem by tracking drugs from production till end user. Integration of IOT (Internet of Things) devices with blockchain can enable continuous monitoring of drugs during shipment from one point to another to ensure the regulatory conditions are met and drugs are transported according to the required conditions. Smart contracts can be used for efficient procurement and secure the terms without the requirement of trust between two parties. Cryptocurrency can be used as a payment method for an efficient finance management and remove the need for a third party. As a result, new framework of business processes in pharmaceutical supply chain is designed with these concepts and cryptocurrencies are evaluated from the point of transaction per second, transaction confirmation time and volatility.

Keywords:
Blockchain History, Blockchain Technology, Pharmaceutical Supply Chain Processes, Pharmaceutical Supply Chain Risks and Regulations, Blockchain and Pharmaceutical Supply Chain, Blockchain Advantages, Blockchain Risks, Blockchain Limitations.

Table of Contents

List of Figures

List of Abbreviations

API	Active Pharmaceutical Ingredients
BPMN	Business Process and Model Notation
BLE	Bluetooth Low Energy
CPU	Central Processor Unit
DSCSA	Drug Supply Chain Security Act
ERP	Enterprise Resource Planning
EU	European Union
FDA	Food and Drug Administration
GDP	Good Distribution Practices
IOT	Internet of Things
IT	Information Technology
NFC	Near Field Communication
NONCE	Number Used Once
MRN	Material Receipt Note
P1	Proof One
P2	Proof Two
RFQ	Request for Quotation
SHA	Secure Hash Algorithm
SU	Serialized Unit
TD1	Trading Partner One
TD2	Trading Partner Two
TPS	Transactions per Second
TCT	Transaction Confirmation Time
WHO	World Health Organization

1. Introduction

1.1 Motivation

Blockchain gained its popularity by cryptocurrencies. Especially by the end of 2017, extreme rise in the Bitcoin value led many people to be aware about this technology. But for many, there are a lot of misconceptions to understand the difference between cryptocurrencies and blockchain. Blockchain is much more than a digital currency; it is a new way of sharing and tracking data which may have significant impacts on human life, business models and changes in industrial operations. According to Swan (2015) blockchain technology is revolutionary as much as the invention of the internet. It is a form of a comprehensive information technology with its technical aspects and applications for any form of digitally registering assets, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property, homes, cars); and intangible assets (votes, ideas, reputation, intention, health data, information, etc.). Furthermore, blockchain is a new organizing model for the discovery, valuation, and digitally transfer the discrete units of anything, and potentially for the coordination of all human activity at a wider range than has been possible before.

Blockchain is listed in Gartner's top ten strategic technology for 2019 to point out how it will change business operations in an effective way. *"Blockchain allows companies to trace a transaction and work with untrusted parties without the need for a centralized party (i.e., a bank). This considerably lower the business friction and has applications that began in finance, but have expanded to government, healthcare, manufacturing, supply chain and others. Blockchain could potentially lower costs, reduce transaction settlement times and improve cash flow. Blockchain will create $3.1T in business value by 2030."* (Panetta, 2019)

1.2 Research Purpose and Goals

The research purpose and the goal of this thesis is to design the process of pharmaceutical supply chain management by blockchain. This can be done by analyzing blockchain in a granular level by focusing more on specific features in order to aim the best solution for supply chain management in the pharmaceutical industry. The aim is to understand if blockchain can take the pharmaceutical industry to the next level by designing a new concept of supply chain management to solve today's problems, in order to improve efficiency and to increase security and reliability of the medical products.

This will be done by understanding the following major key points;

- Blockchain algorithm.
- Pharmaceutical supply chain processes.
- Problems, risks and challenges in pharmaceutical supply chain management.

- Blockchain capability to solve these problems.
- Advantages and disadvantages in blockchain.

1.3 Research Limitations

The blockchain is a new technology and still evolving. It is still under research and there is an ongoing development pursued by many companies and institutions, yet, the usage is very limited in business. Most of the available pieces of information are based on theories rather than practical applications. There are only a few companies which can implement blockchain technology into their business.

1.4 Structure of the Thesis

The structure of the thesis consists of three main parts; to understand and to gain insight regarding the blockchain mechanism, identifying pharmaceutical supply chain processes and designing pharmaceutical supply chain processes by blockchain features.

Chapter 2 explains the literature review approach along with the sources utilised, gives information about blockchain history, technology and its important concepts. Chapter 2 also defines the pharmaceutical supply chain processes along with the risks and challenges and analyses the advantages and disadvantages of blockchain technology.

Chapter 3 includes the methodology of three case studies for three companies, all of which provide different solutions with blockchain for pharmaceutical supply chain.

Chapter 4 combines the blockchain technology with pharmaceutical supply chain by integrating important blockchain concepts into the processes and designs the business process in addition to analyzing the most suitable cryptocurrency for blockchain.

Chapter 5 summaries the conclusion of the research.

2. Literature Review

The goal of this chapter is to provide information about conducted literature review for collecting information on blockchain history, algorithm, key concepts and business processes of pharmaceutical supply chain. The sources are listed below to initiate a search for collecting and analyzing information.

For hash functions, cryptography, creation of a single block, blockchain working mechanism, private and public keys, proof of work, decentralized network, smart contracts cryptocurrency, advantages and disadvantages of blockchain;

- Book "Blockchain: Blueprint for a new economy" (Swan, 2015)
- White paper "Bitcoin: A peer-to-peer electronic cash system" (Nakamoto, 2008)
- Article "A distributed ledger for supply chain physical distribution visibility" (Wu et al., 2017)
- Report "Blockchain technology overview" (Yaga, Mell, Roby, & Scarfone, 2018)
- Journal "Blockchain platform for industrial internet of things" (Bahga & Madisetti, 2016)
- Book "The law and legality of smart contracts" (Raskin, 2017)
- Book "Blockchains and smart contracts for the internet of things" (Christidis & Devetsikiotis, 2016)
- Research Paper "Formal verification of smart contracts: Short paper" (Bhargavan et al., 2016)
- Book "Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money" Gates, M. (2017).
- Book "Supply chain finance and blockchain technology: the case of reverse securitisation" Hofmann, E., Strewe, U. M., & Bosia, N. (2017).
- Book "On the secure hash algorithm family. Cryptography in Context" Penard, W., & van Werkhoven, T. (2008).
- Book "Cryptography and network security: principles and practice". Stallings, W. (2005)

For Internet of Things;

- Journal "Internet of Things (IoT): definitions, challenges and recent research directions" (Ali, Ali & Badawy, 2015)

For Zero proof knowledge;

- Journal "The knowledge complexity of interactive proof systems" (Goldwasser et al., 1989).

For Hyper Ledger Project and Hyper Ledger fabric;

- Book "Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You" (Dhillon, Metcalf & Hooper, 2017)

For Pharmaceutical Supply chain business processes, risks and challenges;

- Book “Threats and Opportunities for European Pharmaceutical Wholesalers in a Changing Healthcare Environment” (Cmolik, 2012)
- Book “Supply chain management in the drug industry: delivering patient value for pharmaceuticals and biologics” (Rees, 2011)
- Journal “Supply Chain Management of the Pharmaceutical Industry for Quality Health Care Delivery: Consumer Perception of Ernest Chemists Limited as a Pharmaceutical Service Provider in Ghana” (Amegashie-Viglo & Nikoi 2014)
- Journal “Supply Chain Management” (Dubey & Kumar, 2007)

Along with the sources above, below are the most common key words to search information in databases;

- Blockchain history
- Blockchain technology
- Pharmaceutical supply chain processes
- Pharmaceutical supply chain risks and regulations
- Blockchain and pharmaceutical supply chain
- Blockchain advantages and disadvantages

Blockchain history search term is used to collect and provide brief information regarding the evolution of blockchain.

Blockchain technology search term is used to gain insight to blockchain fundamentals, algorithm and development in key concepts that can be useful to improve efficiency in pharmaceutical supply chain.

Pharmaceutical supply chain processes are investigated to identify each step of business process.

Pharmaceutical supply chain risks and regulations are investigated to understand if previous findings in blockchain can solve these obstacles.

Blockchain and pharmaceutical supply chain keywords are used together to aggregate blockchain concepts with pharmaceutical supply chain processes and provide an integration of a new management model to these supply chain operations.

Beside these sources, three case studies were carried out. These studies are based on companies that are integrating blockchain with pharmaceutical supply chain processes.

First case study is Mediledger Project developed in 2017 by an American company, Chronicled, in partnership with Pfizer, McKesson, Genentech, AmerisourceBergen and,

Abbvie. Company is using blockchain technology to prevent counterfeit medicines and track legal change of ownership of prescription medicines from manufacturer to the end user.

Second case study is a Silicon Valley based technology company, Syncfab, established in 2013 in United States, aiming to simplify supply chain management and create a transparent blockchain procurement platform within the manufacturing supply chain.

Third and last case study is a Swiss based company, Modum, aiming to focus towards the pharmaceutical industry and enabling companies to meet EU requirements on pharmaceutical products through the supply chain by using blockchain technology.

2.1 Blockchain

2.1.1 History and Evolution

One of the strengths of blockchain is how to secure the data in case of any update or modification. It has a unique process to create data transactions and the idea is coming from the importance of privacy which can be found in the Cypherpunk manifesto written by Eric Hughes (1993).

The logic behind is to certify a digital document (text, audio, video etc.) when it is created or modified. Indicated by Haber & Stornetta (1990) a solution to this problem was introduced by time-stamping the bits of the document by digital signature and cryptographically secure hash functions that were introduced in ‘How to Time-Stamp a Digital Document’.

The concept of blockchain introduced in October 2008 along with the very first application; Bitcoin, a digital currency which can be used for the payments between individuals and operates without a central authority (Iansiti & Lakhani, 2017).

This concept was explained further in a document named as ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ written by Nakamoto (2018) as a purely peer-to-peer version of electronic cash which would allow online payments to be sent directly from one party to another without going through a financial institution.

Even though blockchain became popular by Bitcoin and other cryptocurrencies, it is well understood that there are more capabilities than it only being used as a digital currency by further developments. Swan (2015) explains these developments by dividing them into three categories as blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 focuses on digital currency, blockchain 2.0 focuses on the contracts, both of which are being used for advanced financial transactions and blockchain 3.0 is further than just being a payment system but the set of applications that can be used in government, health, science, literacy, culture, and art.

Blockchain 2.0 and 3.0 are the important steps that can provide further improvements to the supply chain management in the pharmaceutical industry using smart contracts or tracking and securing medical products during shipment which will be detailed in the following sections.

2.1.2 Algorithm

It is important to understand the blockchain mechanism before analyzing its use for supply chain management in the pharmaceutical industry. This section will introduce a brief explanation of how blockchain works from a technical point of view.

Wu et al. (2017) describes blockchain as "*A distributed public database (ledger) that maintains a continuously growing list of transactions which are organized in blocks and secured from tampering".* It is connected by blocks and each block consists of a Block Header, Timestamp, a special number called Nonce (Number Used Once), Data, and the Previous Hash. Each block is connected to each other by a hash which is created by a hash function.

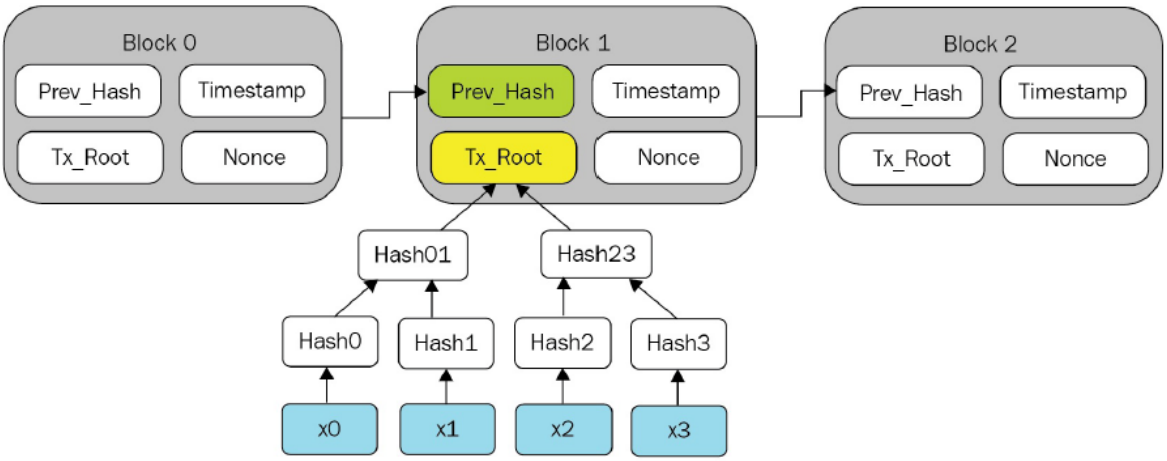

Figure 1: Blockchain Structure (Source: Mukhopadhyay, M. 2018)

2.1.3 Hash Functions

Nakamoto (2008) explains blockchain's success by solving two important problems that could not be solved before;

1) Data transactions between two entities without the requirement of a trusted third party, a peer-to-peer payment of digital cash avoiding the requirement of a financial institution. The trust is based on the mathematical logic behind the algorithm.

2) Avoiding double transactions without the requirement of a trusted third party.

In the current system, all the transactions are controlled by a central authority, for example, a bank, to avoid double payment.

The secure transfer of data between individuals without the requirement of third-party organizations is done by hash functions and trust is created not because of the individuals but mathematical logic behind it which was a big challenge previously.

"A hash function is a function which takes an arbitrary length input and produces a fixed length `fingerprint' string." (Penard & van Werkhoven, 2008). In other words, a hash function is a way of converting data into a fixed length string which is called hash. The hash function will always result in the same output for the given same input. Any change in input will change the hash completely. This input is created from the nonce and the data in the block. (Swan, 2015)

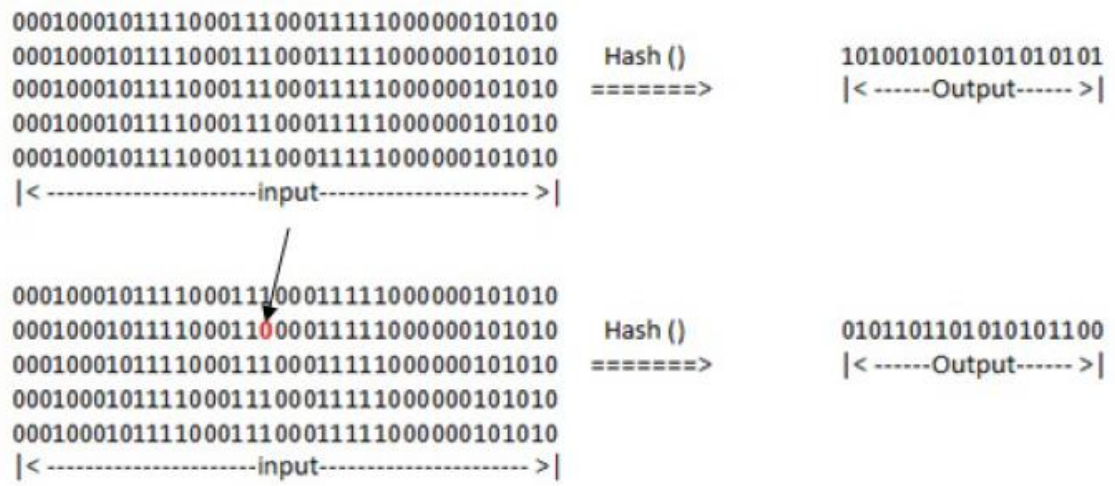

Figure 2: Hash function with input and output (Source: Mukhopadhyay, 2018)

Nakamoto (2008) took advantage of cryptography by SHA256 hash functions not only to create a password but to extend its logic into blocks and create a blockchain by creating digital signatures.

Cryptographic SHA256 hash function is used to convert the input into an output string of fixed length with 256 bits. It is almost not possible to compute input from output in the SHA256 hash function (Stallings, 2006).

An example of hash created from word "Blockchain" with SHA256 algorithm is;

625DA44E4EAF58D61CF048D168AA6F5E492DEA166D8BB54EC06C30DE07DB57E

An example of "blockchain" with lower case b using SHA256 algorithm will be completely a different hash;

EF7797E13D3A75526946A3BCF00DAEC9FC9C9C4D51DDC7CC5DF888F74DD434D1

A small change in input completely changes the hash generated (Gates, 2017).

2.1.4. Public and Private Keys

Private and Public keys are important for the limitation of data sharing between peers in the blockchain network. This will be helpful to understand how companies in the same supply chain can set up a network between each other to transfer only the relevant information related to the business but at the same time to keep private ones for themselves to avoid any kind of business intelligence leakage. Especially in the pharmaceutical industry, companies should pay extra attention to share any kind of medical information since they are regulated by strict privacy rules (Wu et al., 2017).

As previously mentioned in the blockchain algorithm, every transaction has a digital signature to prove authenticity. Stallings (2005) explains that a digital signature works with two different but connected keys; a private key to create a signature and a public key that another peer can use to check this signature. The private key is like the password and the public key is the proof of the ownership of this password without sharing it with anyone. This process is called asymmetric encryption. Asymmetric encryption uses the RSA algorithm to generate a public and private key that are mathematically linked to each other. Public keys can be used to encrypt data and only the matching private key can be used to decrypt it. Even though the keys are linked together they cannot be derived from each other. In other words, a private key cannot be derived by knowing the public key.

According to Stallings (2005), everyone in the network can be allowed to know each other's public key but the private keys should be kept secret. Public keys are also the addresses where the information is sent. The process starts with both parties sharing their public keys with each other. The sender encrypts sensitive data with receiver’s public key before sharing it. The receiver can unlock the data with own private key because it is already encrypted by his or her public key by the sender. Since they use asymmetric encryption, only the receiver can decrypt the message. The strength and the security of the asymmetric encryption rely on both parties in order to keep their private keys well protected.

If an attacker steals the sender's private key, it can be used to decrypt all messages that are intended for the sender. However, the attacker cannot decrypt messages that were sent by the sender because that requires receiver’s private key. Asymmetric encryption is used in a lot of places where security really matters (Stallings, 2005).

2.1.5. Proof of Work

Creating a chain of blocks by linking each block to the previous by a hash is generating a sequence of records but this approach is not solely enough to prevent double transactions. A

method is required to avoid an attacker to generate a fake block and to create the same digital asset twice before the actual block is validated into the blockchain. This method is introduced by Nakamoto (2008) as proof of work.

Proof of work is the process of finding the nonce which is associated with the block to get the hash to start with leading zeros. In other words, SHA 256 function applied to data and the nonce creates a special hash with several zero bits and proof of work to find the nonce which is related with the correct hash. The nonce is bonded to the data. Any change in the data will also completely change the hash. In this case, a computational work should run to find a new proof of work, a new nonce that enables the hash of the altered list together with this nonce starts with leading zeros. The number of zeros is changed periodically and is dependent on the block difficulty. The block difficulty is increased as there are more block creators involved into the blockchain network (Nakamoto, 2008).

As mentioned previously, a hash function can convert any kind of data of any size into a fixed length string of numbers or characters.

Following examples represented by Gates (2017) to show the creation of a blockchain by hashing transactions into blocks and sending bitcoin from peer to peer. The very first block ever created is block number 0, which is also known as the genesis block.

Block #0

Number of Transactions:	1
Timestamp:	Jan 3, 2009 7:15:05 PM
Bits:	1d00ffff
Size (bytes):	285
Nonce:	2083236893
Next Block:	1

Block Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Block #1

Number of Transactions:	1
Timestamp:	Jan 9, 2009 3:54:25 AM
Bits:	1d00ffff
Size (bytes):	215
Nonce:	2573394689

Block Hash: 0000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Previous Block:	0
Next Block:	2

Block #2

Number of Transactions:	1
Timestamp:	Jan 9, 2009 3:55:44 AM
Bits:	1d00ffff

Size (bytes): 215
Nonce: 1639830024
Block Hash: 000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd
Previous Block: 1
Next Block: 3

Each transaction is signed with a private key by the owner of the transaction.

A block must be validated and can be added to the blockchain only if a miner can solve its nonce by computational power.

The genesis block does not have a reference block as it is the starting block, thus the hash of previous block is 0.

Each validated block is added into blockchain after the mining process and linked to the previous block by its hash thus this creates the blockchain (Gates, 2017).

Block #0
Hash of Previous Block: 0
Hash of Current Block:
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Block #1
Hash of Previous Block:
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Hash of Current Block:
00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Block #2
Hash of Previous Block:
00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Hash of Current Block:
000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd

Every transaction from any block can be followed all the way back to the very first block to view the history of data and this functionality leads pharmaceutical companies to track the originality of the products and avoid counterfeit medicines which will be explained in Chapter 5 (Gates, 2017).

2.1.6. Decentralized Network

Swan (2018) describes the blockchain like a ledger in a peer to peer network. As mentioned before, each block includes transactions and are connected to each other by hash. Every peer has a copy of this ledger.

Anyone who uses computational power can create a block. Block creators receive the transactions from peers, collect them in a block and run the computational power to find the nonce which is associated with the hash of this number starts with several leading zeros. Once the nonce is found, the block is broadcasted to the peers and added to the blockchain. Each peer blockchain is updated by this new block. There is no central authority and each peer must keep their own blockchain. Once all the peers are agreed on a trustworthy blockchain, a decentralized unity is formed (Swan 2018).

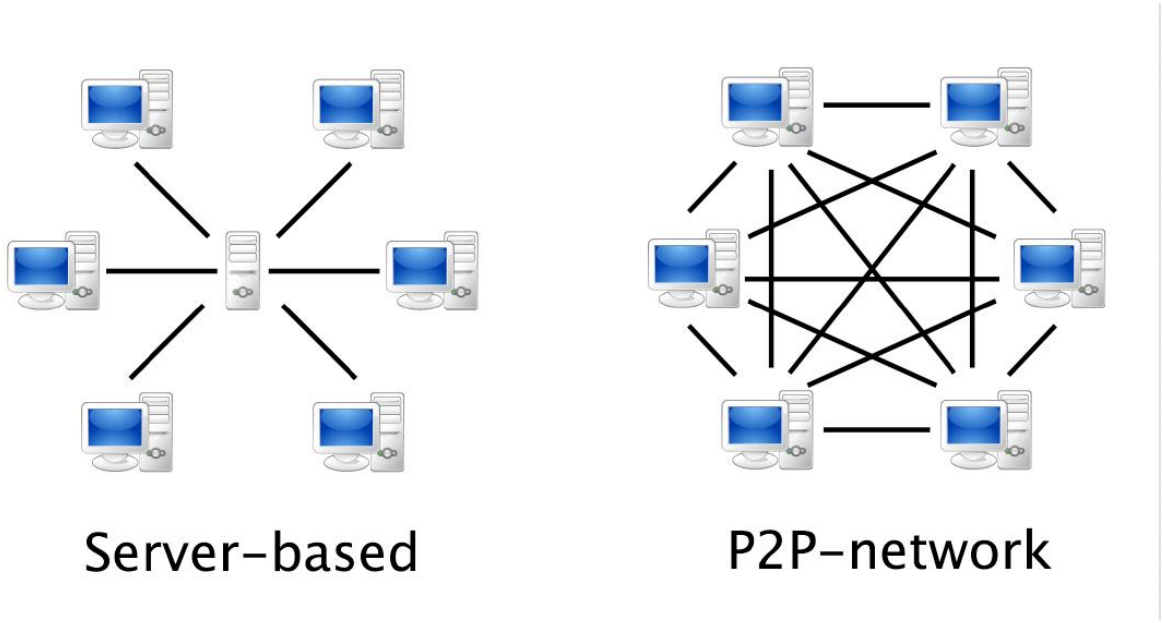

Figure 3: Centralized (Server-based) vs Decentralized (Peer to Peer) Network (Source: bitcoinwiki, 2018)

2.2 Key Concepts for Designing Pharmaceutical Supply Chain

2.2.1. Cryptocurrency

Yaga et. al. (2018) indicates that cryptocurrency is a virtual currency to carry out a transaction digitally and it can be an important asset to be used as a payment layer in the supply chain industry due to its advantages. Virtual currencies are completely independent of government control or any central authority. To be able to process a transaction, organizations do not need to go through a bank.

Bitcoin is the first and one of the most popular digital currency. All transactions on peer to peer network are held on blockchain ledger and publicly get recorded whenever a new transaction occurs. The ledger is distributed among all the peers in the network. Everybody who has the copy of this ledger is notified for every new transaction taking place on the network. For a transaction to occur in the first place, a peer must have a digital wallet on the network. This wallet will include the private key and the public key. The very existence of these two keys is crucial to the whole cryptographic nature of cryptocurrencies as explained in the previous part. They are required for each transaction to be securely encrypted and be

authenticated. In order for a peer to send some amount of digital currency to another peer, the transaction must be signed by peers' private key which functions as the digital signature to prove the peer's identity. Only after signing the transaction by private key, it can be sent to the network by the public key. The public key acts as a verifying mechanism to clarify the message which was indeed marked by correct digital signature and associated with the correct private key. The verification of transactions is done by miners by finding the correct nonce. Once the transaction is sent to the network and announced to the blockchain ledger, miners are tasked to do the computational process to verify the validity of each individual transaction and to ensure no fraudulent transactions are take in place. This process is called mining. After a transaction is verified by a miner, every node must add to its ledger and transactions become part of the blockchain. For this job the miners are rewarded with cryptocurrency which is called transaction fee. By this way, a network of independent actors is economically motivated to maintain the legitimacy of the transaction history. Anybody with enough computational power can be a miner (Yaga et. al., 2018).

2.2.2 Smart Contracts

The term smart contract was first used by Nick Szabo in 1997 long before blockchain was created. (Raskin, 2017)

Smart contracts are the digital forms of contracts that can be applied to the supply chain as an agreement between the buyer and the vendor. They are form of scripts that self-executed in certain conditions that runs an automated workflow included in a blockchain network (Christidis & Devetsikiotis, 2016).

As previously explained, there is also no trusted third-party authority for smart contracts to be executed. The script is programmed in a way to keep all the funds until a certain goal is achieved. The funds are transferred to the parties according to the conditions in the contract. They can be delivered to the peer who completed the required task successfully or returned to the investors in case of a failure. The funds are controlled only by the programming code. The framework to code smart contracts is called Ethereum and uses a programming language, Solidity, a similar one to the JavaScript. This framework provides a distributed platform called Ethereum Virtual Machine to transfer digital assets within this network (Bhargavan et al., 2016).

According to Bhargavan et al. (2016) smart contracts are immutable and cannot be changed. They are also distributed and broadcasted to the blockchain network and validated by all the peers in the network. A single peer cannot manipulate the contract due to the logic explained in the previous security section.

2.2.3 Internet of Things

Internet of Things is the technologies to enable devices connect with each other over the internet. These devices can interactively sense, communicate and collaborate with each other,

and remotely be controlled by their sensors and share the real time data with people or with other devices (Ali, Ali & Badawy, 2015).

Internet of Things integrated together with blockchain is an infrastructure to take supply chain operation to the next level. This concept is also able to overcome the problems faced in today's pharmaceutical supply chain operations. For instance, IBM Watson IoT Platform provides a service to track shipped items (Kshetri, 2017).

More specific approaches related to pharmaceutical industry will be explained in following chapters.

2.2.4 Zero Knowledge Proof

The information is widespread due to computers and privacy and security become more and more important, therefore the use of cryptography is crucial.

Zero knowledge proof is a useful technique introduced by Goldwasser, Micali & Rackoff (1989) to be used in cryptography. It is a method by which one party can prove to another party that a given statement is true without sending the actual information. It is a way of proving something without revealing any information about that thing itself. That is where the zero knowledge comes from.

With this idea Goldwasser et. al (1989) claims that a zero-knowledge proof is not in the question of how to secure the information, it's rather the question of how to give out the idea that the information is known without giving out the information.

Zero-knowledge proof emerged out of research into what is known as interactive proof systems. An interactive proof is a process by which two parties are typically known as the prover and the verifier engage in some sort of back-and-forth process by which they come to some conclusion so that the prover either proofs a statement or fails to prove. In other terms, the prover must keep interacting with the verifier to convince that validity of an assertion is correct. In an example, the prover knows the method of guessing coin toss but wants to prove it without revealing the method. Prover can prove this to the verifier by guessing coins correctly. Zero knowledge proof does not give a 100% proof, but the matter is minimizing the probability that prover is cheating. Probability can be very small, but it can never reach zero. This form is called interactive because the prover has to perform a series of actions to convince the verifier of a certain fact is true. The disadvantage in this form is the challenge in transferability. The prover must repeat the entire process again for each verifier (Goldwasser et al., 1989).

Goldwasser et al., (1989) introduces that the other form of zero-knowledge proof is non-interactive. A non-interactive proof allows delivering proof that can be verified by the verifier by themselves. Blockchain uses non-interactive proof through private and public keys. The verifier encrypts the message by prover’s public key and prover can decrypt it by using his

own private key, there for continuous interaction is not required. That is how each node in blockchain agrees on each transaction and reaches to consensus.

2.2.5 Hyperledger Project and Hyperledger Fabric

Every business or industry is unique. According to Dhillon et. Al (2017) an application standing for the commercial purpose must be personalized, private and permissioned only to authorized stakeholders, unlike the Ethereum, blockchain which runs on a very generalized protocol to develop smart contracts for everything that runs on its public and permissionless network. In a public blockchain network, each node is aware of every transaction and it is not possible to ensure the security of confidentiality and privacy due to its public nature. Business transactions must be executed only between the related organizations with a common goal and exclude any unauthorized users. Even within the shared network, organizations will require to segregate their confidential data like their production capacity with the ones that are required to run the operations like purchase orders. For example a private network will be required in a supply chain industry, only to connect related parties which could be a manufacturer, distributor, wholesaler and customers like pharmacies or hospitals.

Blockchain, on the other hand, is a decentralized network with an open ledger where all the nodes are aware of all the transactions. This is a risky situation for the company's confidential data.

Linux Foundation has a solution to establish privacy in a blockchain network. Hyperledger is an open-source development platform under the Linux Foundation where any developer can build blockchain related technologies. Hyperledger based solution providers and users focused on advance blockchain technology for cross-industry use in business. Hyperledger vision is to create a community and provide frameworks that enable developers across the globe to develop robust blockchain based commercial solutions for businesses (Dhillon et. al, 2017).

Acknowledged by Dhillon et. al (2017) one of these frameworks is called Hyperledger Fabric, a private blockchain network in an enterprise to make transactions between multiple businesses more seamless and efficient and to accommodate each custom requirement. Hyperledger fabric has a modular design which means that businesses can plug in different functionalities to suit their needs.

The concept of Hyperledger based private network Dhillon et. al (2017) indicates that parties can directly connect and accomplish transactions according to their business contract without revealing the terms to other unauthorized nodes. Every transactions history is recorded in the ledger. Organizations can name transfers as any item like medicines or vaccines, categorize them and set their values. Any state change of an item is recorded as transactions on the ledger.

Hyperledger fabric enables to modify items using by programs called Chaincode. Chaincode can define an item or items and the transaction instructions for modifying those items.

According to Dhillon et. al (2017) this is required to set up the business logic. Smart contracts that are executed on the fabric ledger runs Chaincode. Instead of each organization having their own business logic in their current database, the businesses share the common logic, and all agree and approve the changes in the ledger.

Dhillon et. al (2017) state, each member in the Hyperledger Fabric private network can communicate with the ledger using chaincode either by installing a new contract with a new business logic or by displaying transactions that were already defined in previous contracts.

Hyperledger fabric provides a membership identity service to enable permissioned networks that manage user identities and approve all participants on the network. A node will send the transaction only to the address of relevant nodes, which are involved in the deal where their membership will be authorized by a membership service. Only then will the Hyperledger network connect both parties directly.

Permissions can be assigned to different levels according to specific operations. A specific user can be permitted to view a chaincode application but be restricted from deploying a new chaincode. This can be done by assigning roles to nodes. There are two types of roles; peer nodes that are responsible for executing and verifying transactions and ordering nodes that are responsible for ordering transactions and distributing the correct history of events to the network. Multiple transactions are processed simultaneously to increase efficiency and scalability by nodes and the network consensus can be established for customized business logic by ordering nodes to create a single true record of transactions.

Hyperledger Fabrics ledger consist of two components; a blockchain log to store the unchangeable record of transactions and a database to record the blocks current state.

The purpose of the log here is to track an item’s source as it is transferred between different parties. Tracking an items source means to reach the information of where and when it was created as well as every time it was transferred.

Tracking an items source is extremely important in the pharmaceutical supply chain industry to be able to prove its legitimacy.

In typical databases, cooperating businesses individually keeps records only in the current state of an item but not all the history of it, therefore, tracking item’s source is almost impossible and records are incomplete. Organizations choose this approach to keep their privacy. A distributed ledger means that every party in a business network can access all the transactions even if they were not involved in the transactions themselves. This is not acceptable for businesses as they do not want to reveal their data or transactions to other parties or their competitors.

Dhillon et. al, (2017) mention that Hyperledger Fabric has a solution to this through private channels. These channels restrict messaging paths that can be used to provide transaction privacy and confidentiality for specific subsets of network members. All data transactions on a channel are invisible and inaccessible to any network members who do not have granted

access to that channel. This allows business to keep their privacy while accessing all the transaction history of an item.

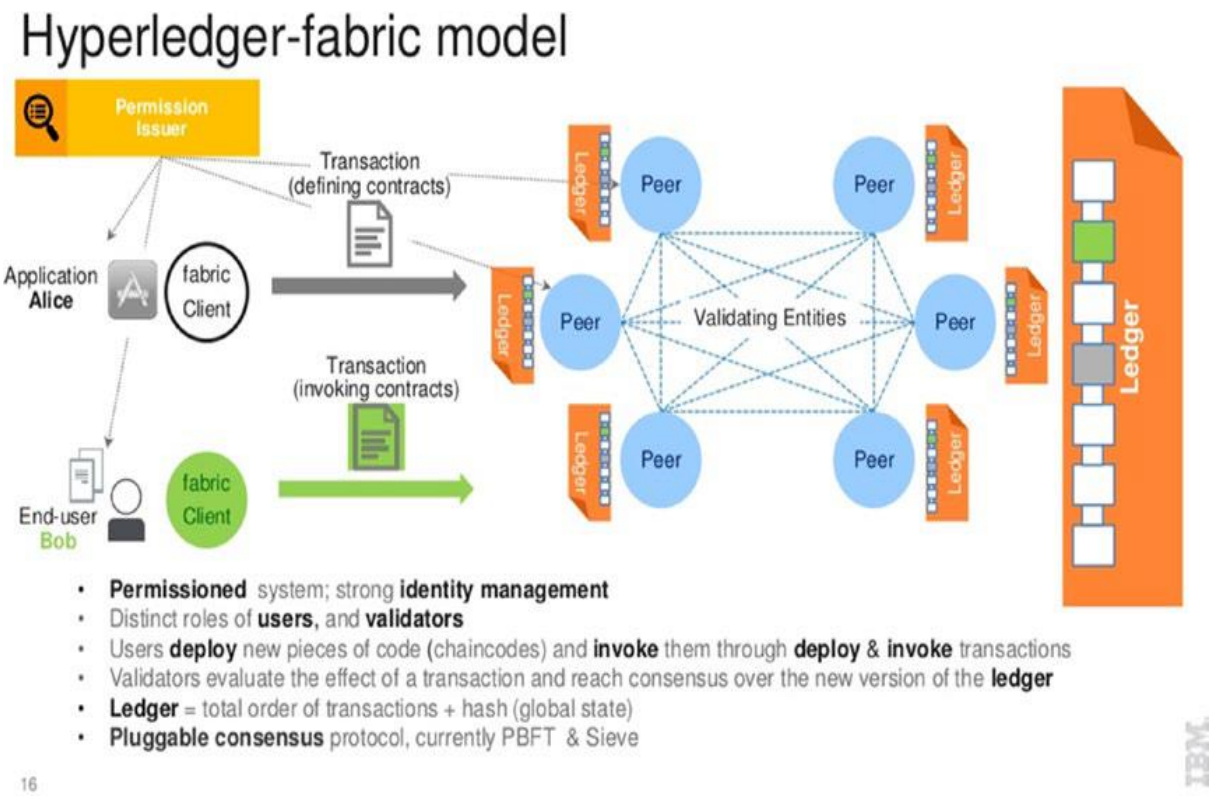

Figure 4: A summary of the main features offered by Fabric (Source: Dhillon et. al, 2017).

As a summary, Hyperledger fabric is a design framework that enables the following functionalities;

- Organizations in the network can define item types and a consensus protocol for ordering transactions.
- Permissions can be set to give access only to authorized parties and their role in the network.
- To increase efficiency, nodes are divided into two types; peer nodes and ordering nodes. Peer nodes verify and process transactions and order nodes logging and recording those transactions in a chronological order.
- Fabrics ledger contains records of the network's current state which can be querie and the log of transactions stored as a blockchain to track each item.
- Status of the items is updated and transferred using chaincode in the form of smart contracts installed and executed in the network.

2.3. Pharmaceutical Supply Chain

2.3.1. Business Processes

According to Cmolik (2012) a market is established by determining the requirement of a pharmaceutical product. A field representative or a sales person gets the approval from the clinics or hospitals before making the product available.

Cmolik (2012) explains the pharmaceutical supply chain process of a manufacturing company begins when the marketing team brings the order. If the finished goods are available in the warehouse, then they are dispatched to the distributor within the country or exported from the country. However, if the finished goods are unavailable, then the order is sent for the production.

The production department is responsible to manufacture the medicine based on the order. Medicines are produced in batches. A batch is the quantity of medicines that would be produced at once and a batch size refers to the medicines produced in one batch.

Higher batch quantities are efficient to have maximum utilization of the machines. Medicines must be tested before they can be dispatched. Testing is done in the quality control department. In parallel the quality assurance of the medicine is also done by the quality assurance department. Once the testing is done the finished product or the final medicine is sent to the warehouse.

The production of a medicine begins with the production department to decide and schedule the batch production. This planning is done based on the availability of raw material or production machines to avoid clashes in production planning on the scheduled date.

The production department asks for the raw material from the inventory store. If the pre-tested and approved raw material is available with inventory it is issued for production, but if the raw material is unavailable, then it is purchased. Once the order is purchased, it is received in the inventory store through a materials receipt note (MRN) and sent for quality control. After quality control testing, the material is sent for production. The quality assurance and quality control departments would be performed at every stage of production.

This process is the same for primary packing material such as vials plugs and seals and secondary packing materials such as cartons and boxes.

Once the production is complete with testing, the batch is released to the warehouse. This process is called batch release which is done by the quality assurance department that is all about the production cycle of a pharmaceutical company.

All the financial transactions are done within the company recorded by the accounts and finance department. This involves the management of cash and credit of the distributor, the management of the inventory store and the salary of company employees.

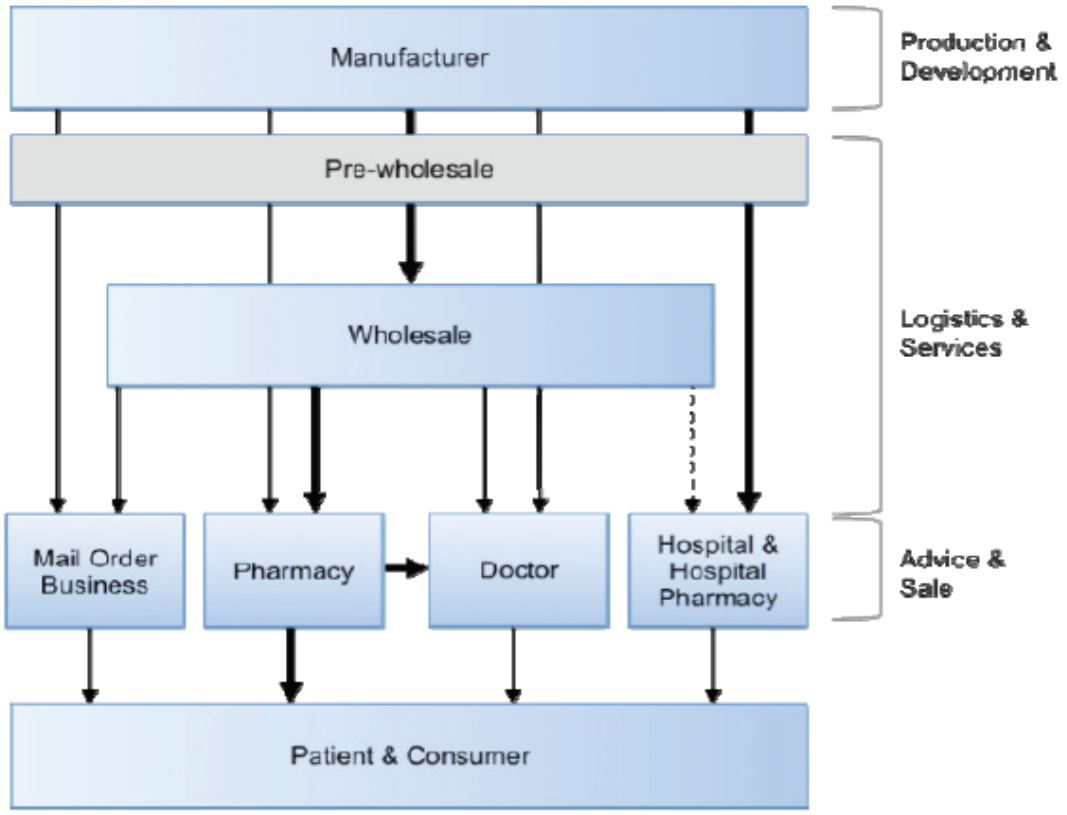

Figure 5: Pharmaceutical Supply Chain (Source: Cmolik, 2012)

2.3.2. Information Technology

Rees (2011) indicates that all the parties involved in this chain such as manufacturers, market distributors or wholesalers need software to track their materials, cash flows and to simplify their trade. There are a lot of processes in a pharmaceutical company and the order of those processes is crucial for operational excellence where an ERP (Enterprise Resource Planning) comes into use.

According to Rees (2011) ERP integrates every department in the company and brings all the processes together in single software instead of having multiple softwares for each process. The stages of a process are divided into sub-stages to minimize the use of software by a single person. As an example, a purchase order entered by the marketing department is not entered again in the software by any other department. This avoids duplicate data entry and ERP can also provide linking with the software used by trader. This feature enhances the communication process and the work flow of the pharmaceutical company. Below figure is the representation of information flow between departments.

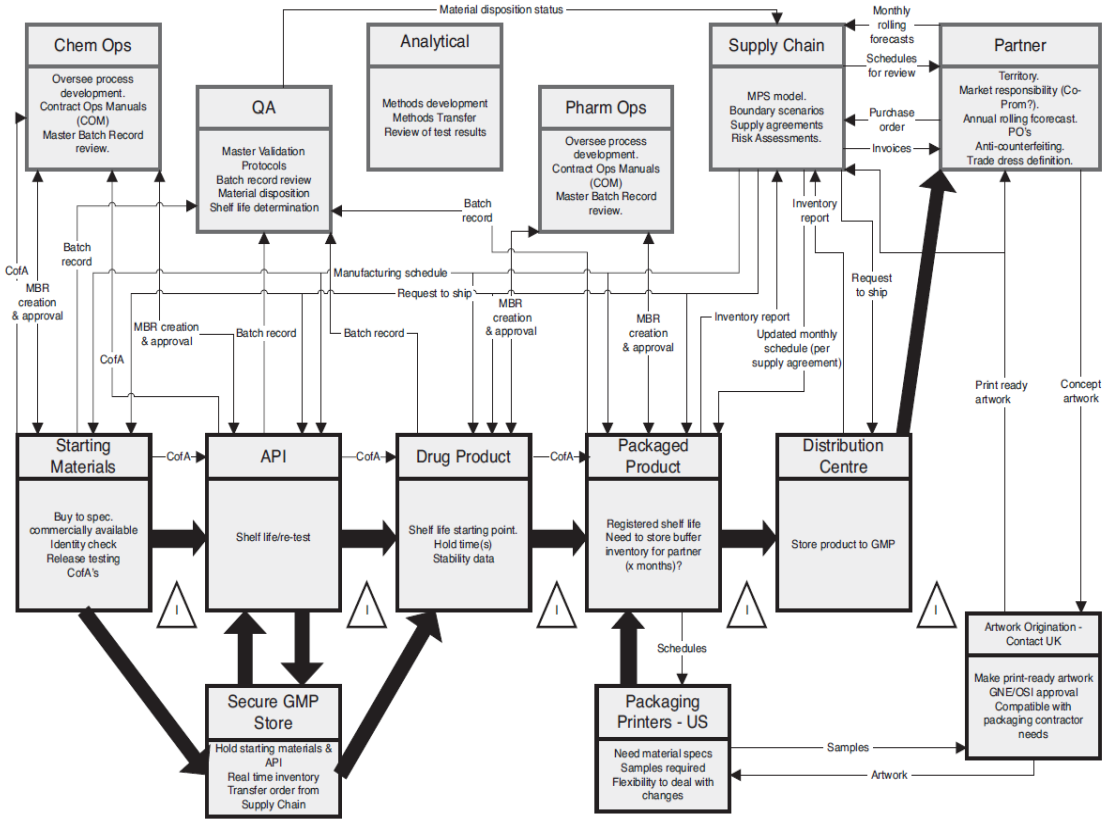

Figure 6: Information flow between departments (Source: Rees, 2011)

SAP is one of the leading German software companies to integrate business process into one software and take the first steps of ERP. SAP R/3 is the actual version of the software to develop a fully integrated ERP across all the business processes, including financial and cost accounting, sales and distribution, materials management, manufacturing, and warehouse management even human resources management. SAP is widely used by many of the organizations including Bayer. Bayer announced the introduction of SAP R/3 in the mid 1990's as the standard software for their global business in UK (Rees, 2011).

Today SAP has further developments to use all the aspects of technology and taking ERP to a next level. This also includes the integration of blockchain. *"SAP Leonardo is a new digital innovation system from SAP. It delivers software and microservices that enable customers to leverage future-facing technologies like the Internet of Things, machine learning, blockchain, analytics, and Big Data*" (Schmitz, 2019).

2.4. Risks and Challenges in Pharmaceutical Supply Chain

Supply chain industry has been exponentially and globally growing over time. More and more developing countries have been involved in the course of time and products are not directly delivered from the manufacturer to the end user, but they need to be shipped through different channels which make supply chain operations more complicated. These complications create a lot of quality concerns and a faulty act can fail all the process (Quayle, 2006).

2.4.1. Counterfeit Drugs

The control over supply chain is relatively difficult for the manufacturers due to diversity of outsourced pharmaceutical products all around the world. Criminal activities are increasing as the growing production and distribution are extending to emerging markets. There is a lot of money involved in fake drugs and many distributors and wholesalers are involved in the supply chain, which makes distribution a very complicated process. Tracking items is difficult and inventory discrepancy can be high. Emerging market regulations are complicated, and changes often make it more challenging to comply (Manners-Bell, 2017).

Counterfeit drugs are one of the biggest problems in pharmaceutical industry. According to the World Health Organization (2018) 'Substandard and falsified medical products' report, 10% of drugs in developing countries can be fake and they can cause sickness or death. They are produced under bad conditions by unqualified personnel and contain harmful materials.

World Health Organization (2018) declares that it is very hard to detect and understand the difference between a genuine product and a fake drug. They are almost visually identical. Current methods to identify a counterfeit drug can be; examination of packaging, misspellings and grammatical errors, controlling the production, expiry dates and ensuring that any details of the outer packaging matches the dates shown on the inner packaging, checking the color and smell. By the exponential increase on the internet access, social media channels can also promote fake drugs and make it easier to be distributed and supply it to a global marketplace. They are produced in many different countries and all the regions are affected by this issue. Patients reach fake drugs in case of limited access to quality and safe medical products or unavailability of proper governance or technical capacity.

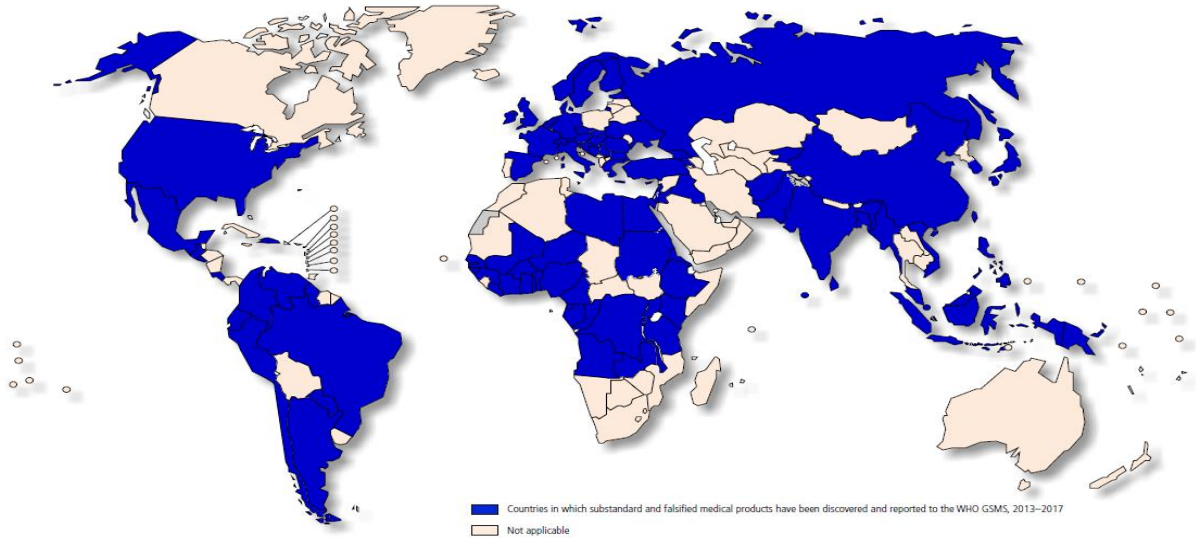

Figure 7: Countries in which substandard and falsified medical products have been discovered and reported (Source: WHO, 2017)

The biggest companies in the industry are deeply impacted by counterfeit drugs as well. Blanchard (2010) gives the following examples to underline the seriousness of the situation:

McKesson, as a pharmaceuticals distributor and provider of health information technology, medical supplies, and care management tools purchased fake Serostim, a drug to treat AIDS patients in year 2000.

AmeriSourceBergen, a drug wholesaler company, bought more than $4 million worth of heavily diluted Epogen, a medication for patients with anemia who are on dialysis in 2001 and 2002.

Cardinal Health, a health care services company, bought $2.4 million worth of tainted Procrit, another anemia drug in 2002. In 2007, hundreds of people got ill, dozens of whom died due to contaminated heparin, a blood-thinning drug provided by the drug manufacturer Baxter International.

The pharmaceutical market is a trillion-dollar global market with a very complex supply chain network. Global Surveillance and Monitoring System for substandard and falsified medical products reported by WHO (2017) clearly explain the complexity of the supply chain. *"A tablet taken in Germany may be made in Egypt from ingredients imported from India, Brazil and Spain, packaged in foil that came from China, inserted into a box designed for the United Kingdom of Great Britain and Northern Ireland, and shipped to Liverpool by way of Dubai. A trader in the United Kingdom, taking advantage of fluctuations in the foreign exchange rate, might legally repackage the medicines with information written in German and ship it to Munich."* This complexity is an open gateway to the substandard and falsified medical products and makes it harder to take situation under control. Fake drugs also make diseases impossible to treat because the infections become drug resistant. This can happen even in a well-regulated country. *"There is clear evidence that resistance to the most important antimalarial medicine, artemisinin, first appeared in a part of the world where at one point between 38 and 90% of the artemisinin medicines on the market were substandard or falsified"*. Patients who are affected by fake drugs spend more money in long term for a proper treatment. The estimated expenditure on substandard and falsified medical products is US$ 30.5 billion.

As per the Global Brand Counterfeiting Report (2018), the amount of total global counterfeit is bound to reach 1.82 Trillion USD by the year 2020.

Following are the key figures summarizing of the problem by SANOFI (2017) to clarify the impact of counterfeit products for the human health and economy.

Key Figures:

- 1 out of every 10 medicines sold in the world is a counterfeit. This number can reach up to 7 out of 10 in some countries.

- In 2015, out of 40 million products intercepted by European Customs, 25.8% of health products in circulation seized were counterfeit medicines. A total of 895,324 medicines were seized.

- $US 200 billion in 2014 versus 75 billion in 2010 reflect the scale of the profits pocketed from counterfeit medicine. The number is higher than that drug trafficking.

- For every $US 1,000 invested in the trafficking of counterfeit medicines, criminal organizations pick up a likely return of $US 500 000.

- In 2016, 103 countries collaborated in Operation Pangea IX to fight illicit online pharmacies. It led to the closure of 4,932 websites and the seizure of more than 12.2 million fake and illicit drugs, valued at approximately $ 53 million.

2.4.2. Regulations

Medical products must be securely transported and kept under certain conditions to avoid excessive temperatures, incorrect handling or poor hygiene. Without doubt, quality, effectiveness and safety of the medicinal products must be maintained. Due to high regulatory requirements, a seamless and transparent supply chain is very important for pharmaceutical companies. However, they face complex challenges. Multiple parties are involved; supplier, second tier supplier, wholesaler, pharmacy and hospital, and they all use different and often disparate IT systems which make the exchange of data difficult (Manners-Bell, 2017).

Since globalization evolves in parallel with the risks and the complexities, governments take further steps by regulating the pharmaceutical supply chain in detail.

The European Commission (2013) has set up guidelines to regulate Good Distribution Practices (GDP). Through GDP, the supply chain of medicinal products must be controlled during the global shipment and the quality of medicinal products should be maintained with a quality management system. Transport risks must be systematically identified and assessed. Warehouses and vehicles must be clean dry, and temperature must be controlled. Important information about the medicinal products such as product name, batch number and expiry date must not be lost. Packaging must be appropriate and trained personnel should ensure that all required transport conditions are maintained. Should something unplanned happen during transportation, the damage must be fully documented and investigated. Corrective and preventive actions should be taken to restore the quality of the impacted medicinal products.

In parallel with the European Commission, United States Food and Drug Administration (FDA) also published a Drug Supply Chain Security Act (DSCSA) on November 27, 2013 which outlines the steps to build an electronic, interoperable system in order to identify and to trace certain prescription drugs which are distributed in the United States. This will enhance FDA’s ability to help protect consumers from exposure to drugs that may be counterfeit,

stolen, contaminated, or otherwise harmful. The system will also improve detection and removal of potentially dangerous drugs from the drug supply chain to protect U.S. consumers.

Additionally, the DSCSA directs FDA to establish national licensure standards for wholesale distributors and third-party logistics providers, and requires these entities report licensure and other information to FDA on annual basis.

FDA targets to amend the federal drug, act with respect to human drug compounding and drug supply chain security, and for other purposes. This act sets out the steps for establishing an electronic, interoperable system to identify and monitor certain prescription drugs. According to this act, all the wholesale distributors and third-party logistics providers must comply with national licensing standards and notify the FDA of their licenses and other information annually.

The goal is to put the procedures of controls on operating procedures as well as from IT procedures to allow the exchange of the information at the item level and address each touch point, where, when and who is responsible for these drugs in the supply chain. The IT system should support verifying the legitimacy of a product, detect illegitimate products in the supply chain and facilitate to recall those products.

In case of an event like a negative impact of the drugs on consumers, the responsible company should have those procedures in place to continue their business. The implementations must be completed by 2023, 10 years after the enactment of the Drug Supply Chain Security Act. Companies will need to look at their IT systems and supply chain and work closely with their logistics departments. Below figure is the demonstration by Sayah, Wittkamp & Stoffels (2018) to show the need for digitalization to track shipments in logistic sector.

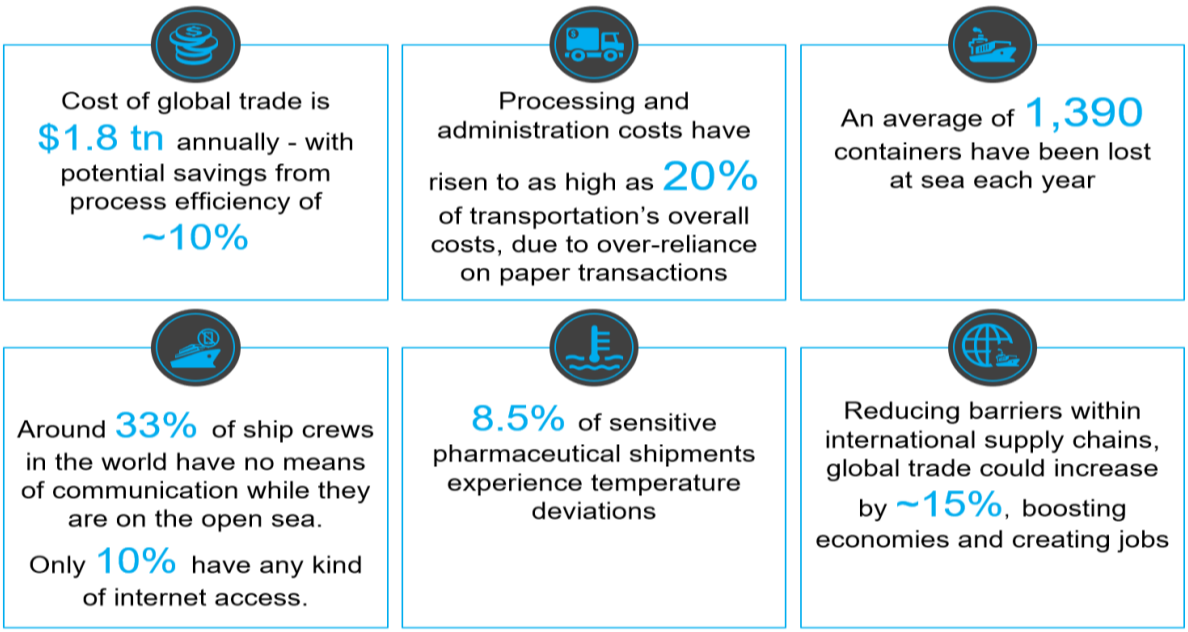

Figure 8: Important figures in logistic sector that blockchain can aid (Source: Sayah et. al., 2018)

One of the important points is that 8.5% of sensitive pharmaceutical shipments experience temperature deviations which can cause economic losses, regulatory charges or furthermore casualties and health problems in case of continuing distribution till the end user unless they are spotted and returned to the manufacturer.

2.4.3. Data Management and Security

Amegashie-Viglo and Nikoi (2014) explain that supply chain is the network of organizations with various activities to produce value by delivering service and products to the end user as well as related information flows, through improved supply chain relationships to achieve a sustainable competitive advantage. Business processes can be improved to achieve effective supply chain management by increasing the data accuracy and reducing the operational complexity.

The pharmaceutical industry is a global business that requires a secure and efficient supply chain. Modern pharmaceutical products are dependent on ingredients and raw materials from all around the world. It is getting harder to sustain control over the internal operations of an organization with its external environment.

Each partner involved in the supply chain must coordinate their activities with other organizations, healthcare providers and patients otherwise the supply chain can become a tangled web. Beside this complexity, pharmaceutical industry is hampered by loads of information and a general lack of timely and reliable data as a result of historical business models and trading practices.

Pharmaceutical supply chain must clearly prioritize regulatory compliance and safety of products, but also must use the advantages of information to be more responsive to the needs of end users.

Data management in pharmaceuticals supply chain is challenging but it can be rewarding with proper management. Amegashie-Viglo & Nikoi (2014) state that *"Companies that excel in supply chain operations perform better in almost every financial measure of success. Supply chain excellence that improves demand-forecast accuracy leads to 5% higher profit margins, 15% less inventory, up to 17% stronger "perfect order" ratings, and 35% shorter cash-to-cash cycle times."*.

According to Chopra and Meindl (2005) excellence in the supply chain means aligning operations with consumer demand to become 'demand driven'. To strongly and reliably enhance patient safety and to become more demand driven, the pharmaceutical supply chain needs a ubiquitous technology framework that includes:

1. Item-level data management,

2. Standards for available data and how they will be accessed and maintained,

3. Data sharing infrastructure to accommodate cost efficient management and retrieval of data,

4. Reliable trust environment to determine who can access information if information provided can be certified as authentic and what can be done with the information provided or accessed.

Dubey and Kumar (2007) indicate that supply chain operations are mostly managed by integrated business information at transaction level like purchase orders, sales, shipments and payments. Even though transaction level management provides some insight about operations, item level data management can improve the ability of organizations to control product movements within these transactions and provide more visibility on end-user demand, contract compliance and reverse logistics. One solution is to have unique identifiers in each product label or package with the support of technologies such as barcodes that enable packages to carry a unique identifier. When combined with an infrastructure of readers, it can provide data about the events related to product. As the blockchain did not formerly exist, the suggestion was to store data in an event repository; either a single central item event repository or a network of local event repositories across geographies or business units within an enterprise.

The actual requirement indicated by Chopra and Miendel (2005) is not only to achieve item level data management but to be able to link item level data to events and monitoring outside the organization. To be able to leverage item-level data across enterprises, standards are needed to ensure computer systems or software's exchange information between devices by different enterprises.

According to Dubey and Kumar (2007) data must be shared across the supply chain to achieve measurable benefits but traditional systems cannot manage this volume of data for business to business communications.

The following diagram is the idea of an infrastructure by Dubey and Kumar (2007) based on the assumption that manufacturers, wholesalers, pharmacy chains and hospitals integrate their own item level data management capabilities.

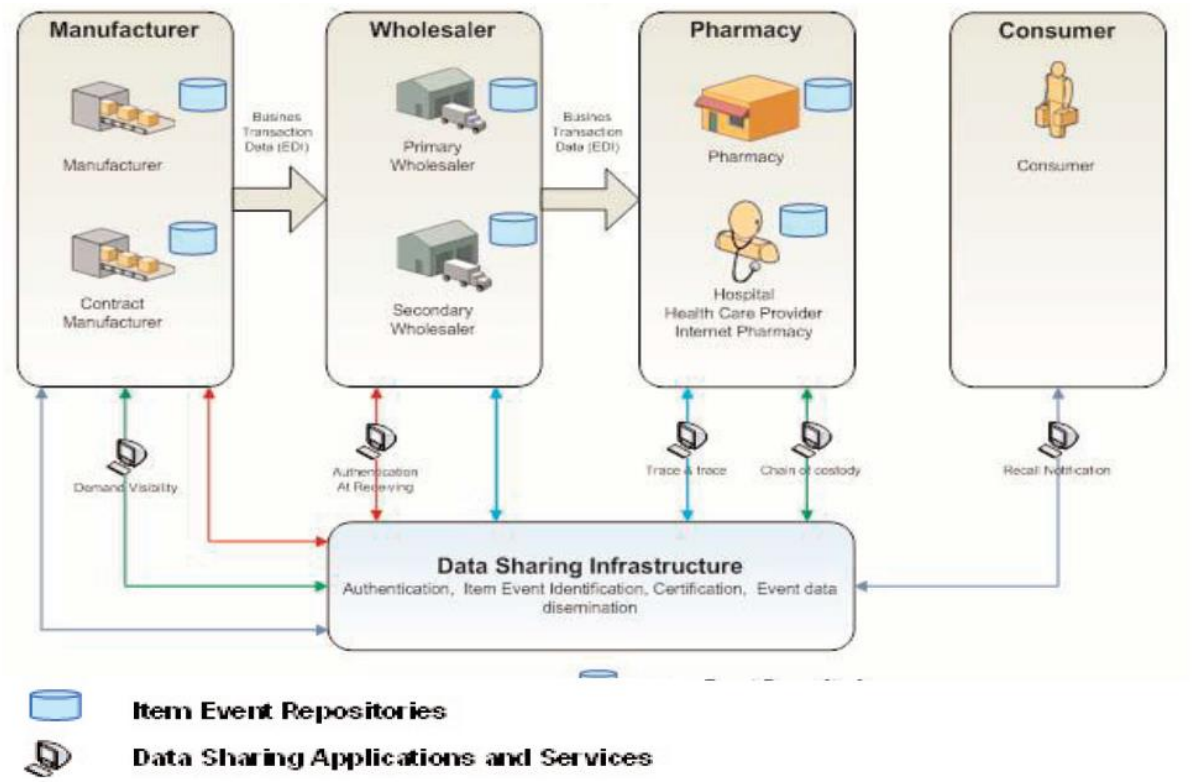

Figure 9: Data flow infrastructure idea to track products at item level before invention of blockchain (Source: Dubey & Kumar, 2007)

One of the biggest concerns of the information technology professionals within the pharmaceutical industry is to reveal data to any other organization beyond their immediate trading partners as an impact of these data sharing structures on current business models. Information sharing within supply chain industry should maintain trust in the system to protect crucial and valuable information from misuse or unauthorized access. This is one of the key points to the success and trust management (User authentication, access control and data protection) which is a challenging task to establish in network-based data sharing pharmaceutical supply chain. (Chopra & Miendel, 2005).

Manners-Bell (2017) identifies another challenge in data security to protect data from any type of external facts which can occur from a human error, natural catastrophes or a cyber-attack due to centralized data center architecture. Companiy operations can be heavily disrupted in case of any loss or damage on servers, data centers, IT infrastructures. In total cost terms, the nine mostly costly recent natural disasters are shown in the next table.

Rank	Year	Natural disaster	Total cost
1	2011	Tohoku, Japan earthquake	$309 bn
2	2005	Hurricane Katrina, North America	$200 bn
3	2008	Sichuan earthquake, China	$146 bn
4	2012	Hurricane Sandy, North America	$71 bn
5	2011	Thai floods	$46 bn
6	1992	Hurricane Andrew, North America	$32 bn
7	2008	Hurricane Ike, North America	$30 bn
8	2010	Chile earthquakes	$25 bn
9	2004	Hurricane Ivan, North America	$20 bn

Figure 10: Natural disasters and their economic impacts (Source: Manners-Bell 2017)

Barr (2016) emphasizes an example from pharmaceutical industry about an explosion happened in West Virginia at Bayer Pharmaceutical plant in 2008 which caused production shutdown and thereby significant loss of profits. A federal investigation revealed that the lack of response from the company had exposed members of the first response unit as well as the entire local community to extremely serious risks. Such circumstance consequently damaged the company's reputation.

The research program of the World Economic Forum (2013) recommends that all of the organizations involved in supply chain should play a role in developing the structures and processes to expand the use of data sharing platforms for risk identification and response.

In 2004, a minor short circuit hit British Telecom. The resulting IT failure caused 130,000 users' telephone, fax and internet systems to lose connectivity; 31 bank branches closed due to stalling of data centers, automated teller machines collapsed and emergency hotlines were inaccessible. Stated by Barr (2016) the damage due to this minor short circuit was estimated more than US$ 7 million per day.

2.5. Analyzing Blockchain

2.5.1. Blockchain Advantages

All the transaction in the blockchain network are secured by strong cryptography. Furthermore, the transparent nature of the public ledger maintained by a blockchain network makes it secure and auditable as everyone on the network knows about all the transaction and the transactions cannot be disrupted. According to Bahga & Madisetti (2016) this transparency can also reduce any corruption in smart contracts as code is both visible and automatically executed. This leaves the room for individuals or organizations to alter it to their advantage.

Bahga & Madisetti (2016) indicate that blockchain technology enables a trustless peer-to-peer network where the peers do not need a trusted intermediary for interacting with each other. Since a blockchain network is not controlled by a central authority, all of the transactions are verified and validated by a consensus among the peers; hence, there is no need of trust between each other.

Blockchain network is resilient to failures as it is a decentralized network with no single point of failure. Every node in the network has an identical or almost identical copy of the ledger. This ensures that if a node is compromised or damaged it can always be restored and receive a complete copy of the database from the system through the form of a sub database. The blockchain itself is an immutable and durable ledger, thus, the transactions cannot be altered or deleted once they are recorded on the blockchain because it would invalidate all the child locks whose ancestors have been altered.

Decentralization also makes blockchain a secure system. A malicious peer can try to send a fraudulent block to a specific peer to swindle without publishing this block to other peers. To be able to do this, the malicious peer should compute the right proof of work before other block creators. The victim peer will also receive an identical block from other block creators. The blockchain will split into two. The fraudulent blocks coming from the malicious peer and actual blocks coming from the block creators. According to the logic behind, the victim peer always takes into consideration the longest chain. Malicious peer must compete with other bock creators to keep its own fraudulent blocks ahead of the blockchain. To be able to do that, the malicious peer should have most of the computing power so that he can create the longest chain and outpace the honest block creators. In other words, any hacker needs to have more than 50% of CPU power among all other block creators to manipulate the system which is almost impossible to held this much of computational power (Bahga & Madisetti, 2016).

According to Bahga & Madisetti (2016) blockchain is also highly scalable due to its nature as it is maintained by a network of peers the computing capability of the network scales up as more and more peers or miners join the network. Blockchain is also fault tolerant. If for some reason a node or a set of notes is shut down, the whole network will not be affected because

the remaining nodes will continue working as usual, assuming there are sufficient accurately operating components to maintain the service.

Automation can be effectively used via blockchain, for example IOT devices to communicate with each other and do transaction autonomously or running smart contracts to reduce the time and save costs associated with managing and enforcing them, making them more efficient as they can be cheaper and faster to run through this form of automation. People can also set up their own contractual agreements peer-to-peer, thereby limiting the arbitrary power of centralized organizations. Smart contracts can also deliver certainty to guarantee a very specific set of rules and outcomes that are predetermined by all parties (Bahga & Madisetti, 2016).

Rometty (2017), Chairman, President, and the CEO of IBM, estimates that the application of blockchain to global supply chains alone could result in more than $100 billion in efficiencies and could add improvements in provenance and traceability of pharmaceuticals and food.

2.5.2. Blockchain Disadvantages

Blockchain is in at a very early stage and there are not many projects fully broaden out and developed which also is part of the whole lack of awareness, therefore, the true value of blockchain is yet unknown. There is also a limited available pool of technical talents and shortage of developers that are specialized in blockchain.

As mentioned before blockchain is built on cryptography and cryptography implies that there are public and private keys. In case those keys are not kept safe, the risk of losing funds or business data is possible.

Swan (2018) explains that if there are not enough accurately operating components to maintain the service, the processing of transactions will be slow. The blockchain network has a potential issue with slow transactions that it can process only one transaction per second (tps) with a theoretical value of maximum of 7 tps where other transaction processing networks are VISA (2,000 tps typical; 10,000 tps peak), Twitter (5,000 tps typical; 15,000 tps peak), and advertising networks (>100,000 tps typical). Each blocks' processing time to be validated is at least ten minutes for security reasons and can be much longer for larger transactions where again, as the comparison metric, VISA takes seconds at most.

Before adding a new block or transaction, every node in the network verifies the authenticity of the item via mining which consumes a huge amount of computational power. This process requires a lot of electricity and resources are wasted as mining draws an enormous amount of energy. According to Swan (2018) the estimation to spent per day is $15 million.

There is a limitation by automating the execution of a smart contract as they are dependent upon formal rules with very specific inputs and leave little room for a variety of occurrence where the rules may need to be slightly altered because of unexpected circumstances. In case

of an unpredictable or unforeseen event, rules sometimes need to be flexible and adaptable to accommodate and this is one advantage of having human supervision as people are much more capable at judging such circumstances and responding appropriately to complex unpredictable events.

The degree to which an event can be automated is relative to the kind of environment that is being operated in, and in more complex situations is often needed to be under control of a governing body to intervene when necessary. This creates new complications surrounding governance that are still to be figured out.

Wüst & Gervais (2018) indicate another risk in the IOT system that can be manipulated by misplacing devices to mislead temperature measurement. As explained previously, pharmaceutical products can be tracked to ship under certain climate conditions and to meet regulations via IOT sensors. However this control depends if the sensors are placed correctly. A malice contractor can place sensors in a limited cool place to fake records sent to blockchain as all the shipment of products met required conditions.

2.6 Determination to Adopt Blockchain Technology

Determination to adopt blockchain is an important decision for organizations to choose the type of network. Below is the comparison of performance between permissionless blockchain, permissioned blockchain and a central database.

	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW, some PoS	BFT protocols (e.g. PBFT [5])	None
Centrally managed	No	Yes	Yes

Figure 11: Difference between permissionless, permissioned blockchains and a centralized database (Source: Wüst & Gervais 2018)

Wüst & Gervais (2018) also introduce a flowchart as a useful tool to determine whether the blockchain is a technical solution to problem. First step is to decide whether organization needs to store state. If no data needs to be stored, then blockchain is unnecessary. If yes, then the second question is whether there are multiple writers. If there is only one person or entity making changes, then a blockchain is not helpful. A regular database provides better performance because of throughput and latency. If there are multiple writers, can the organization use an always online trusted third party? If yes, then the trusted third party can be delegated as a verifier and blockchain is not required. If there is no trusted third party, are

all the writers known? If a set of riders are not fixed and not known, then one should use a permissionless blockchain. If they are known, are all riders trusted? In case all the writers are trusted, blockchain is unnecessary. A database with shared access can serve in this situation. If there is no trust, then using a permissioned blockchain is required. If public verifiability is required meaning anyone can read the contents of the chain, then a public permission block chain should be used. A private permission blockchain is used when limited participants can read the chain.

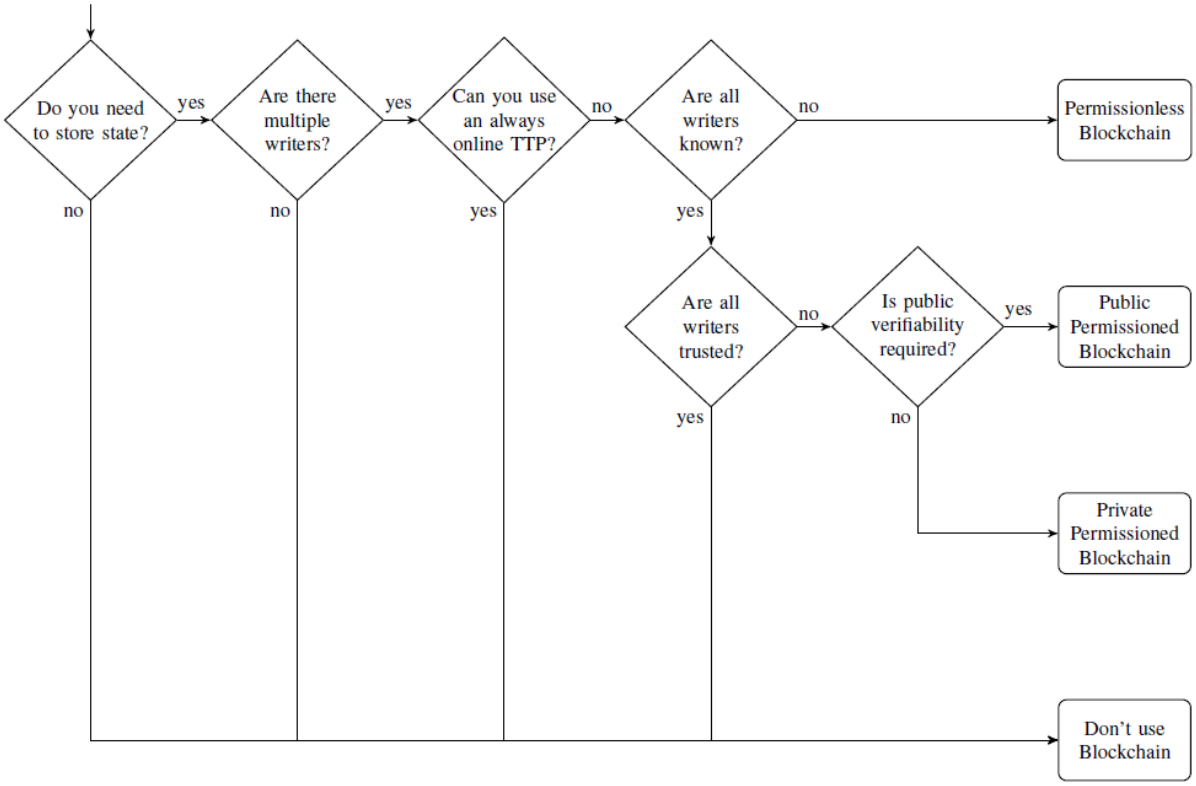

Figure 12: Flowchart to determine whether a blockchain is the appropriate technical solution to solve a problem (Source: Wüst & Gervais 2018)

3. Methodology

This chapter will introduce case studies about three technology companies that are providing solutions for pharmaceutical supply chain industry by using blockchain technology

3.1. Case Study: Mediledger Project

Mediledger is a project developed by an American company called Chronicled in partnership with Pfizer, McKesson, Genentech, AmerisourceBergen and Abbvie at 2017 using blockchain technology to prevent counterfeit medicines and to track legal change of ownership of prescription medicines from manufacturer to the end user. The solution that they are proposing in the Mediledger Project 2017 Progress Report is an immutable ledger to register proof of transactions using a smart contract which executes the business rules. The system is compatible with FDA's DSCSA requirement to establish product identification with a unique product identifier, product tracing; allows manufacturers, distributors to provide tracing information in shared ledger, product verification; to verify product identifier regarding its legitimacy, detection and response; to report suspicious or counterfeit drugs, notification; by creating a shared system to notify FDA and other stakeholders when an illegitimate drug is found.

The technical solution provided by Mediledger is hosting a private information by distributed ledger in the participants supply chain ecosystem. A private permissioned ledger is only used by the participants that maintain its integrity and provide a trusted network for pre-approved traders. As the transaction occurs in the supply chain, manufacturer or trading partner (TD1) sends a private message of serialized unit (SU) together with a mathematical proof (P1) to the next trader (TD2) in the supply chain. Once the proof of TD1 is validated against the proof of TD2, TD2 prepares its mathematical proof named P2, and the transaction is entered in the block. This way a chain of immutable transactions are recorded in the shared ledger for each trader in the supply chain who has a true copy of the transaction. The private message in the distributed ledger technology resolves the identification problem, the smart contract verifying the proofs and resolves the verification problem, the immutable ledger of transactions resolves the traceability problem.

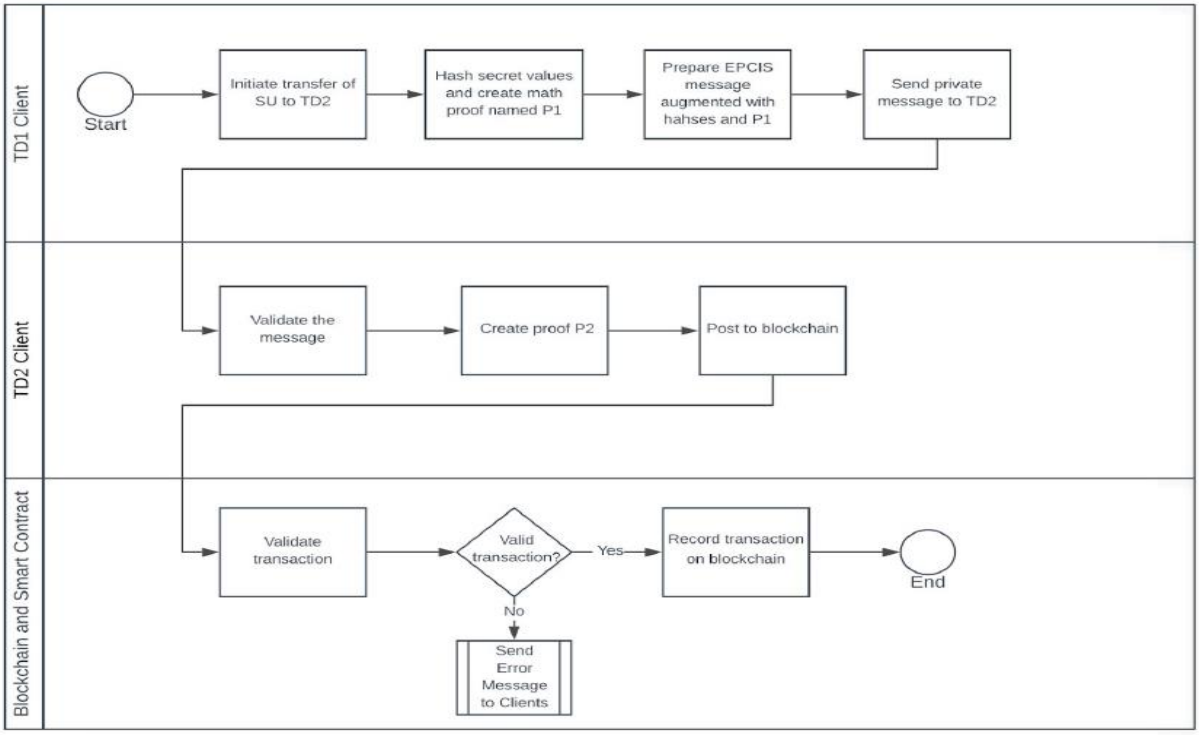

Figure 13: Mediledger Project Business Processes (Source: The MediLedger Project Progress Report, 2017)

The verification mechanism occurs by zero proof knowledge which is to validate the authenticity of the traders by verifying P1 and P2. If the proof of TD1 does not match the proof of TD2, the transaction cost will not be recorded in the ledger and notification will be sent back to the traders. This ensures that the verified traders enter validated transactions into the block and the counterfeit drugs cannot be entered.

Due to many participants in the block minimal, data goes into the block just enough to maintain governance and compliance with the regulatory views. Only relevant transactions such as information and shipping information are included. It is also preferable for each company within its own ERP system may store additional information that would only be visible to them and will not go into the block, therefore, issues of confidentiality and data privacy are maintained.

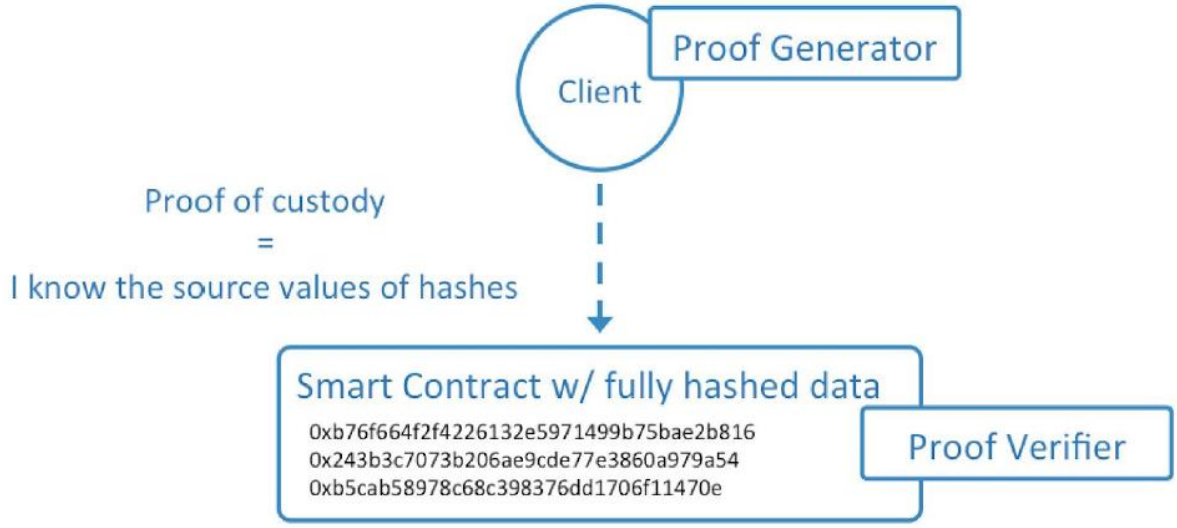

Figure 14: Zero-knowledge proof to authenticate transactions in the chain (Source: The MediLedger Project Progress Report, 2017)

3.2. Case Study: Syncfab

SyncFab (2018) is a Silicon Valley technology company established in 2013 based in United States aims to simplify supply chain management and create a transparent blockchain procurement platform within the manufacturing supply chain. SyncFab created a smart manufacturing decentralized application and connects supply chain buyers directly with their manufacturing suppliers peer-to-peer for streamlined procurement on the blockchain and eliminating the brokers.

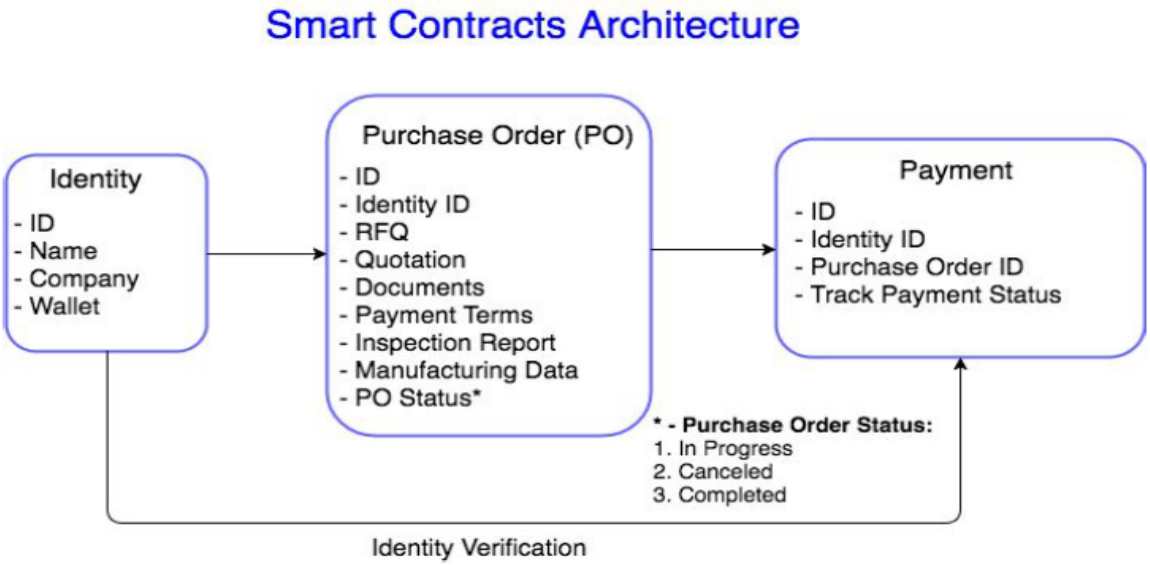

Figure 14: Syncfab Smart Contracts Architecture - Decentralized Manufacturing V15 (Source: Syncfab, 2018)

Buyers will be able to search and procure products on the blockchain using the decentralized application to secure and streamline orders by initiating smart contracts that fit their requirements or specifications for a particular time, material, location and budget. These smart contracts will be self-executing according the terms of conditions and if the turnaround time is properly met, then the components of the financial value of that contract will unlock.

Following are the steps of decentralized procurement transaction flow;

- Identity Contract is created by buyer to hold contact information's, wallet, order history, and buyer evaluations.
- Account Contract is created by manufacturer to hold contact information's, wallet, order history, manufacturer evaluations and operational capabilities
- Purchase Order Contract is created by buyer to hold request for quotations (RFQ) details for suppliers to bid on a service or product, manufacturer requirements and all related documents on the ledger.
- Most suitable manufacturers with required machine capabilities are filtered based on the RFQ in the ledger.
- RFQ is sent to the matching manufacturers to bid their price for the product or service.
- Buyer receives the bids an approves the most suitable manufacturer.
- Purchase Order Contracts status is updated to Production state after the approval and agreement.
- Every data regarding machine condition or production status will be logged in to Purchase Order Contract.
- Manufacturer issues an inspection report to the buyer after the production is completed.
- Buyer approves the report and a Payment Contract is created between the buyer and manufacturer.
- Manufacturer approves the Payment Contract.
- Buyer creates a Purchase Order Contract for logistic company to deliver the products.
- Purchase Order between the buyer and manufacturer updates status to "Completed" on the ledger.
- Purchase Order Contract with the logistic company updates its status to "Completed" and updates to the ledger after arrival of the products.

- Purchase Order between the buyer and manufacturer updates status to “Completed” on the ledger after the completion of payment from buyer to manufacturer and recorded to the ledger.

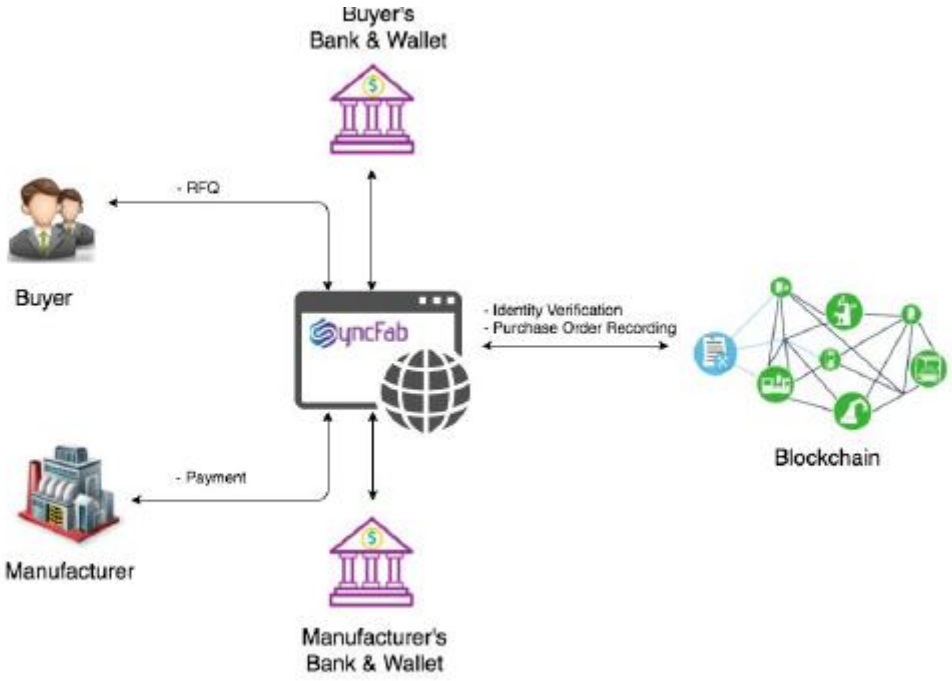

Figure 15: Procurement Transactions with Blockchain. (Source: Syncfab, 2018)

3.3. Case Study: Modum

Modum (2017) is a Swiss based company aiming to focus towards the pharmaceutical industry and it enables companies to meet EU requirements on pharmaceutical products through the supply chain by using blockchain technology. Modum solution is to use IOT that can record environmental conditions of the shipped goods that are subject to regulatory conditions while in transit. This gives them the ability to guarantee that there has been no factors that would have compromised the quality of the goods.

Modum has a few components to their system. The first one is the pharmaceutical quality temperature logger which basically monitors temperature during the transport and then it will communicate wirelessly to a mobile application via Bluetooth low energy (BLE) or via a Near field communication (NFC) chip allowing electronics to be able to share data with one another.

The dashboard is the second component with the serves for the users to set or monitor conditions according to smart contract and get warned if the threshold for measurement was broken. This also gives them the ability to track shipments, view data visualization analytics and those can be used to perform statistical calculations on historical data. Their mobile application can be used to pair temperature laws with their respective shipments initialize shipments and visualize the recorded data.

In the long term Modum is planning to expand the application use of its technology by integrating additional sensors that track not only temperature but also humidity moisture lights and other environmental variables. Modum has been successful with their pilot tests. They have a wide range of partnerships including SAP, Amazon, University of Zurich, University of St. Gallen.

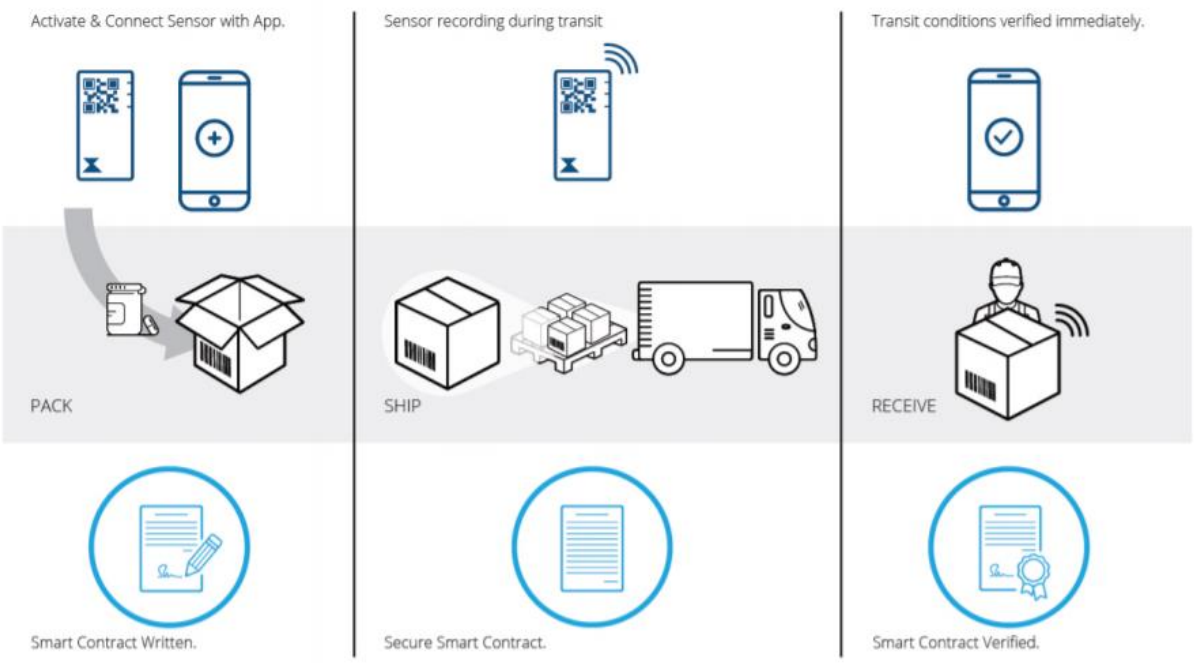

Figure 16: Shipment process of Modum system. (Source: Modum, 2017)

4. Designing Pharmaceutical Supply Chain Framework with Blockchain

As a foundational technology, blockchain can underpin different pharmaceutical supply chain functions by solving the biggest problems in the industry. This chapter will introduce blockchain usage and benefits in pharmaceutical supply chain processes and provide complete design and framework of an optimized supply chain network together with blockchain.

4.1 Production

Use of blockchain can start at production stage. The core idea behind blockchain technology is to track all transactions of an asset in a distributed ledger of cryptographically secure and time stamped records, thus enabling the digital transfer of values directly without requirement of any third party. Implementation of blockchain to pharmaceutical supply chain at production stage will enable drug tracking to prevent counterfeit drugs.

Schöner et. al. (2017) indicate that counterfeit drug problem caused by unsecure supply chains and blockchain can work as a drug supply platform with manufacturers as well as with customers being able to track pharmaceutical products throughout the whole supply chain by ensuring drug identification, tracing and verification of the medical products. Each product will be tagged by a hash code at the packaging stage including all the required information like manufacturer, production date, batch number etc. and this data will be transferred to the trusted blockchain network. Therefore, tracing the authenticity of drugs moving through the complex distribution network of pharmaceutical supply chain will be much easier by registering those products into blockchain once they are manufactured.

Another benefit of drug tracking is to prevent drug abuse. Blockchain can be used in a prescription drug monitoring program for controlling drug shopping. According to Dhillon, Metcalf & Hooper (2017) Mayo Clinic claim patients buy drugs, especially narcotics with same prescription from multiple healthcare practitioners. Mayo Clinic relates this with poor timeliness of data since there is no existing centralized system where a pharmacy can upload prescription data into the system to be available for other practitioners. Blockchain back end structure can be a solution for all transactions to be available immediately to all members in the network. Another cause is the reliability of data. Centralized database has a single point of failure unlike blockchain due to its decentralized architecture. The final reason is the complexity of data retrieval as the current data retrieval model and the compatibility with existing hospital systems is completely broken. Synchronization between hospitals and the databases used by pharmacies are very rare and databases are not updated properly. This process could be universal by blockchain with a common back end access point. Clinicians would be able to check blockchain for patient records to find out their active records. This will help clinician to check if the patient is asking same drug from multiple sources and if there is any double transaction for the same prescription.

A trusted network can set up allowing different parties to store information knowing that only authorized members can see it and the information cannot be altered once it has been entered for pharmaceutical orders. The authentic drugs can hand over to an authorized party at each

transfer point to ensure that it is still the original product and has all the information given by the manufacturer, thus cannot be changed with any fake drug. Within this trusted network, all transactions are always available to all members of the network. This means status of each drug in the supply chain is visible at any time to authorized parties, including the source of the drug and the current location of the drug.

Using only a public ledger or a private ledger is not feasible to meet supply chain requirements. Data sharing must be done by using both private and public ledgers where private ledger will be used between trading partners to keep sensitive data and public ledger will be used to contain all the tracking information for all the shipment and hash value of each private event.

The following scenario is created by business process and model notation (BPMN) which is a distribution framework of four participants; a raw material manufacturer, Active Pharmaceutical Ingredients (API) manufacturer, wholesaler and pharmacy. The purpose of the process is to track and detect counterfeit drugs and to inform legal entities. Blockchain is structured as public and private network. Private network is required for the confidential information between direct trading partners like contractual agreements. This kind of data should not be seen by other partners.

The flow starts by raw material manufacturer getting the production order. After successful quality control, batch ID of the raw material is posted to the public blockchain whereas the contractual agreement between API manufacturer recorded to the private network 1. This private network is accessible only by the raw material manufacturer and by the API manufacturer. Once API manufacturer gets the shipment, the origin of the product is confirmed from public blockchain network by scanning QR codes and comparing the physical batch ID with system batch ID. In case there is a mismatch, legal entities will be informed otherwise the flow continues with production, quality control and packaging. Once the final product is produced, product ID is recorded to the public blockchain and contractual agreement between API manufacturer and wholesaler is recorded to the private network 2. Again, the confirmation is done by the wholesaler once the shipment is received for counterfeit detection, product ID is recorded to the public network and contractual agreement is recorded to the private network 3.

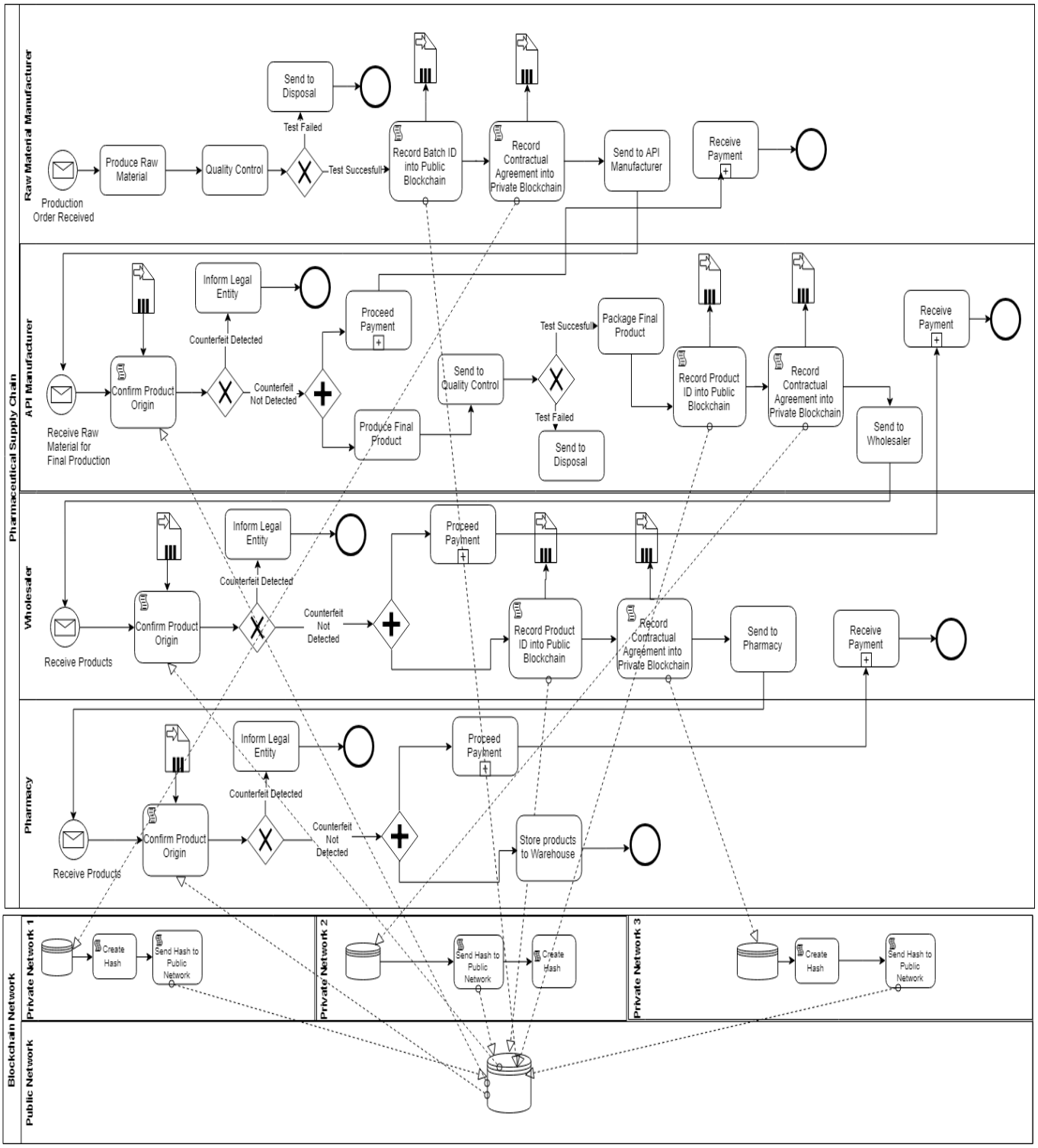

Figure 17: Process for tracking origin of the product and prevent counterfeit drugs

4.2 Procurement

Pharmaceutical supply chain includes a massively complex set of contractual agreements between manufacturers, logistic companies, pharmacies, hospitals that are created and enforced by centralized organizations like insurance companies and banks which themselves

are supported by the ultimate centralized authority in the system. All the parties are almost completely dependent on third-party organizations to maintain and enforce those contractual agreements (Hofmann, Strewe & Bosia 2017).

Hofmann et. al. (2017) explains the process of procurement today, starts with a buyer creating a purchase order for the items that have been agreed for a price and sending this purchase order by paper or electronically. The vendor who receives the purchase order creates his own version of documentation which might be called as the sales order and fulfills it by providing the goods. Once the goods are received, the buyer creates his own records with a goods received note where the vendor refer to the same process and keeps records by a delivery note. Then an invoice is created by the vendor and sent to the buyer by keeping a copy. The buyer checks the invoice against the goods received note by purchase order and only if all things match, then the payment is arranged via bank. Vendor checks that payment against all records to ensure that everything is in order. All this process is due to the lack of trust between parties since the human factor is involved and there are multiple versions of truth with a great deal of duplication of effort. A purchase order and a sales order are the records of the same documentation, a good received note and a delivery note record are the same event and two separate records of an invoice is just a simple duplication.

Smart contracts feature these same kinds of agreements whether to act or not, they remove the requirement of the trusted third party between members involved in the contracts. This is because a smart contract is both defined by the computer code and executed or enforced by the code itself automatically without discretion. Therefore, blockchain as smart contract technology can be used as the procurement stage to remove the reliance on centralized systems and enable people to create their own contractual agreements that can be automatically enforced and executed by the computer code. As an example, a smart contract can be programmed on the blockchain to create a purchase order to buy goods with certain conditions.

By using blockchain concept, the process would be the same but instead of parties sending documents to each other, records can be kept in the blockchain with a single entity and both parties arriving a consensus on what was being ordered. Same as the purchase order, the records can be registered in the blockchain after the delivery and both parties would agree that the delivery had indeed happened, and they would not have two separates of records of a single event. The next step is to send invoice but in blockchain scenarios there is no requirement for an invoice. The purpose of the invoice is to confirm that the previous events happened, and the order was made and fulfilled. Smart contract can completely remove the necessity of an invoice because the previous events registered in one place are already enough to initiate the payment and that can happen instantly by a cryptocurrency without requirement of a bank.

Procurement through smart contract would be more efficient by avoiding the requirement for a middle organization, having a single source of truth for both parties, without the requirement of physical transaction proofs like goods received note, import or export documentation and prevent delays in the processes.

Following figures are created to represent the class diagram and the process model of smart contract creation.

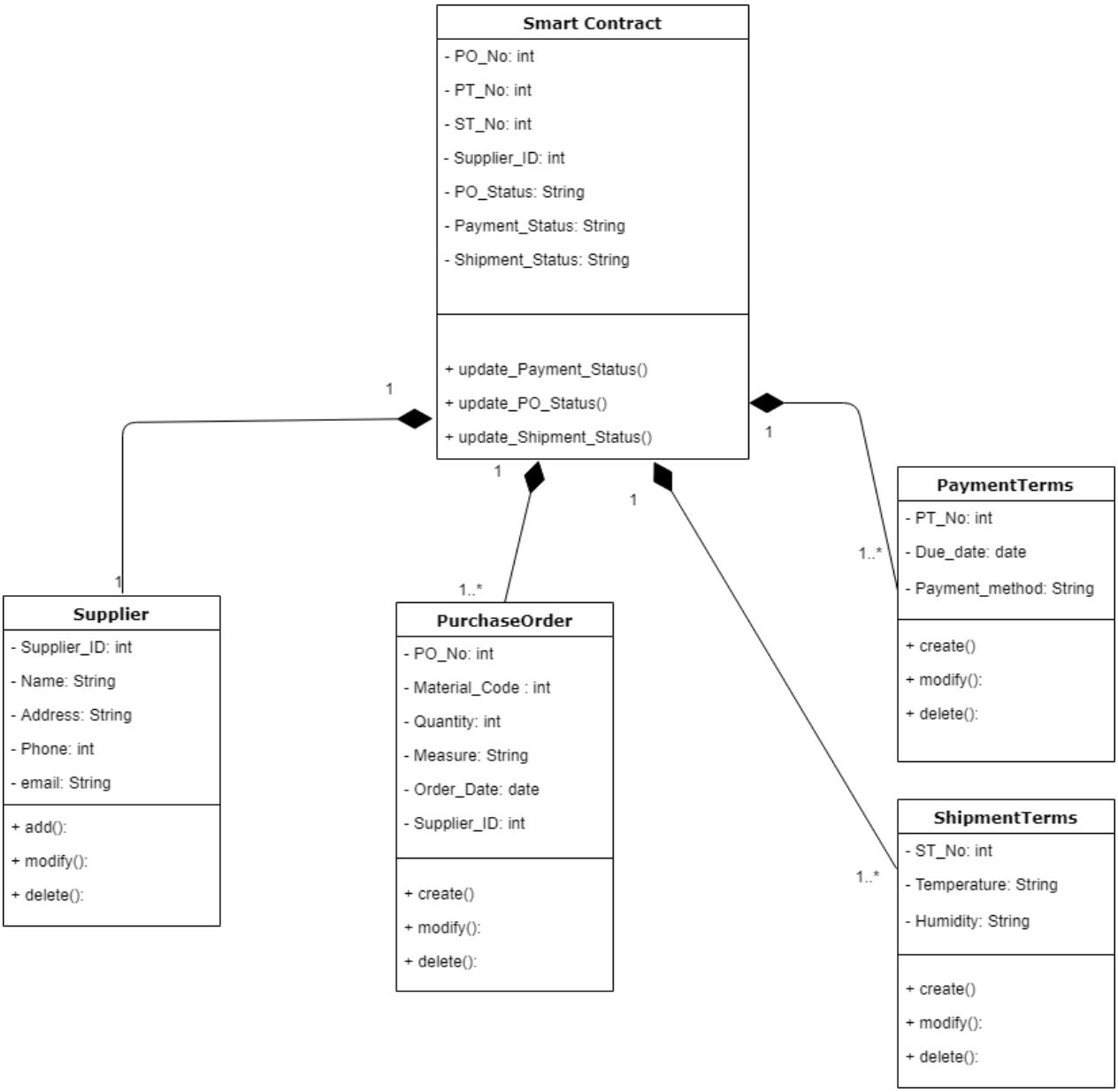

Figure 18: Smart contracts class diagram

Smart contract consists of all the information regarding supplier, purchase order, payment terms and shipment terms. There can be only one supplier for one contract but there can be many purchase order, payment term and shipment term can be defined. Shipment terms are crucial since the rules will be defined on them, buyer will be notified in case there will be a violation of these rules during the shipment.

Below process flow represents the creation of a smart contract by procurement department. When the production department reaches minimum stock level, a material requisition form (MRF) is created based on the material resource planning. As this is an internal process, the MRF can be recorded into local ERP to be sent to procurement for purchase order creation.

Based on the MRF, procurement specialist will search for the best supplier and create the smart contract to interact with the supplier through blockchain.

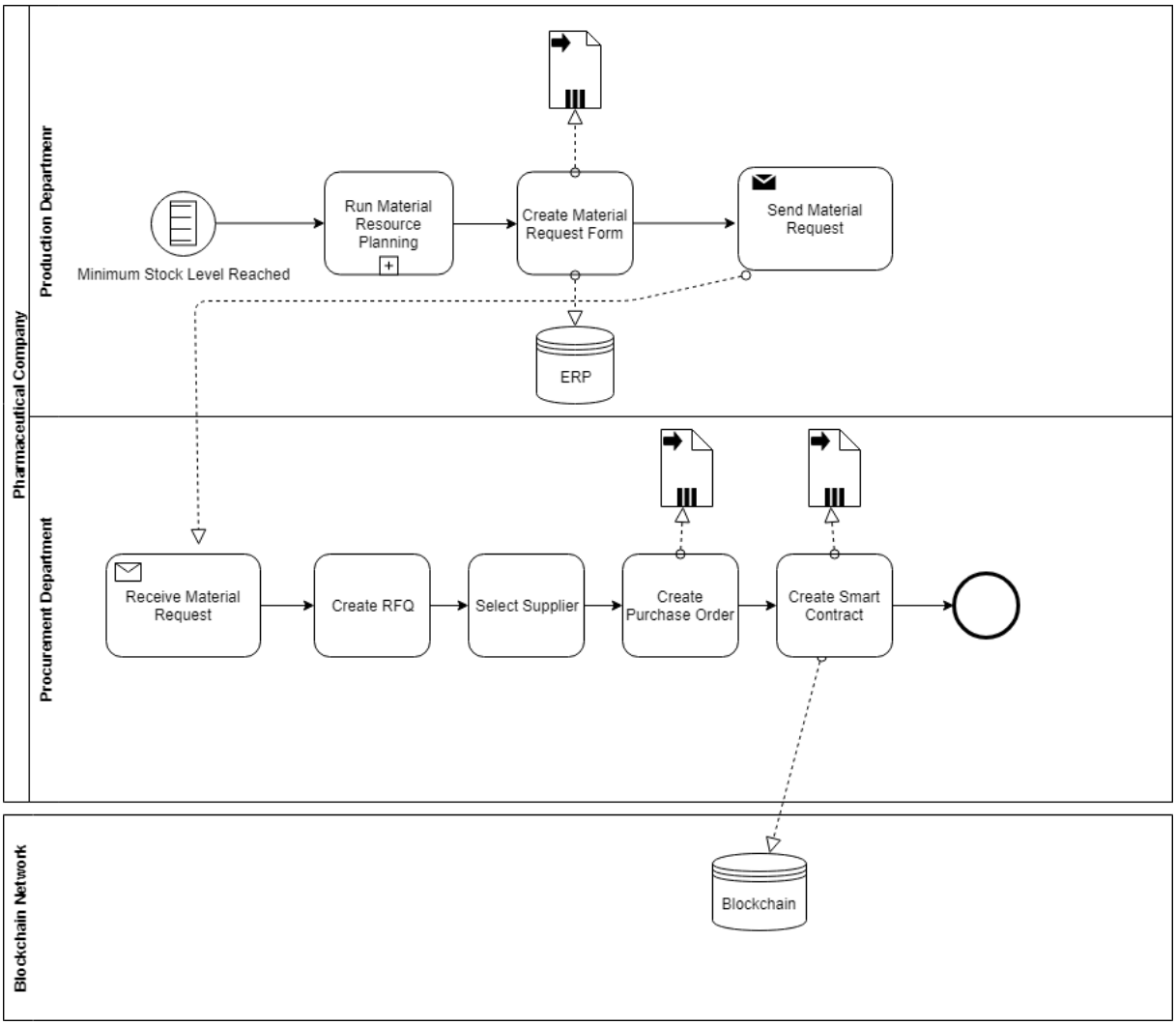

Figure 19: Smart contracts creation process flow

4.3. Shipment and Warehousing

Due to high regulatory requirements, a seamless and transparent supply chain is very important for pharmaceutical companies. However, they face complex challenges as multiple parties are involved including supplier, second, the tier supplier, the wholesaler, the pharmacy and the hospital. These parties use different and often separate IT systems which makes the exchange of data difficult. Transport conditions of drugs such as temperature humidity, luminosity or vibration cannot be accessed in real time and can be subject to manipulation. Compliance with FDA and EU regulations is costly and time-consuming.

This can be solved by integrating IOT together with blockchain for tracking products when they are shipped or stored in warehouse. A smart contract can be setup as previously mentioned with certain transit conditions for the drugs to be transported like temperature,

vibration, humidity and luminosity which must be kept between certain levels. IOT sensors can be installed either in the warehouses or within the transportation vehicles to track and record data to individual batch IDs or drugs via blockchain and provide information to stakeholder of the supply chain about all the conditions of drugs through shared ledger technology. The IOT sensors together with blockchain can establish the integrity of the data. Tracking the condition of medical products through the start point till the end would not be possible with different IT infrastructures and database which belongs to each partner involved in the supply chain from the manufacturer to logistic companies and wholesalers.

Following business process flow created to show supply chain operations when there are multiple partners involved and product must be handled by different logistic companies. Once the manufacturer sends shipment through first logistic company, condition of the products is continuously sent to blockchain via IOT devices to ensure if they are shipped according to suitable conditions like temperature and humidity. The wholesaler is noticed in case there is a violation and a claim can be raised according to contractual agreement. If not, conditions are sent to blockchain while the products are kept in the warehouse. When the wholesaler sends the shipment to the hospital via second logistics company, the process is the same as the first one and hospital is getting notified if it is required.

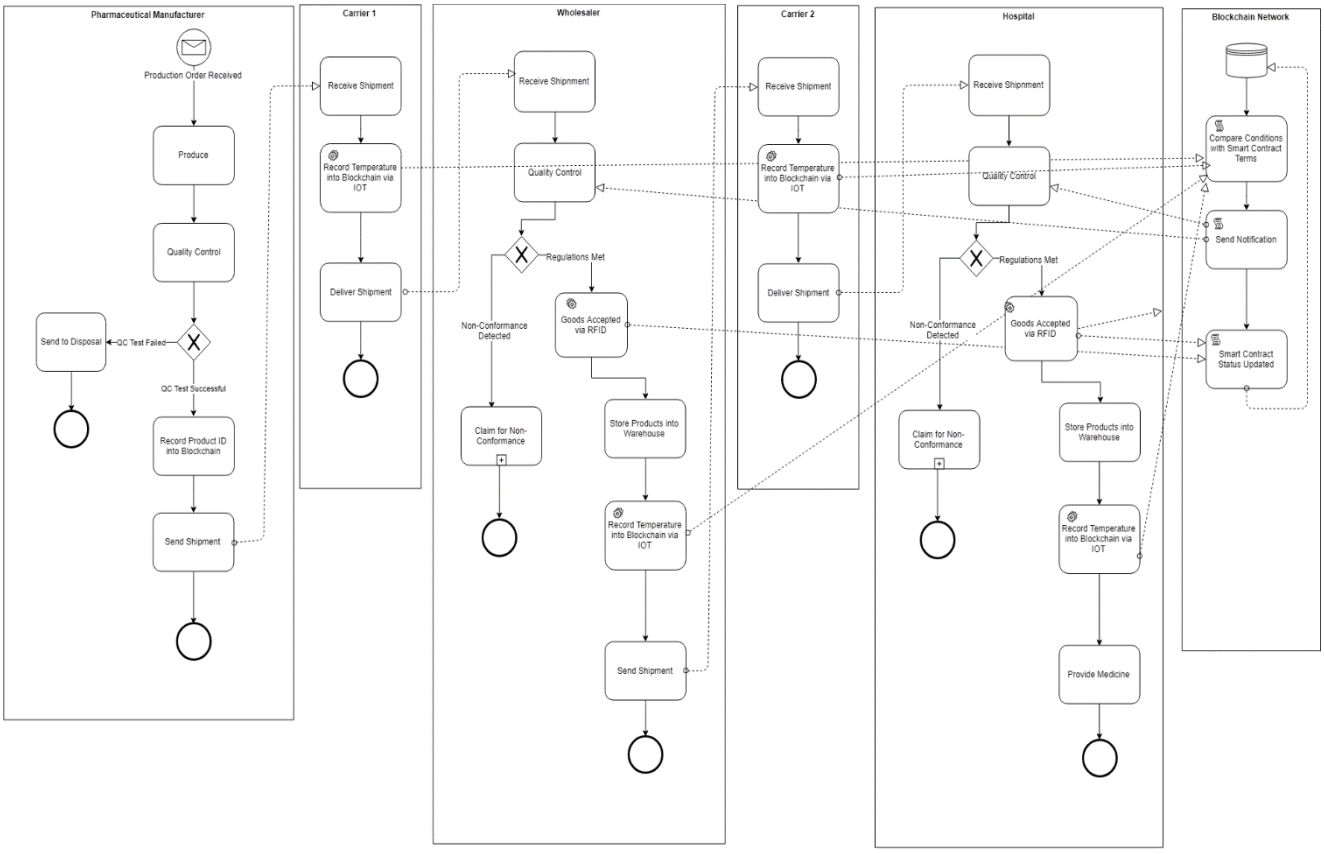

Figure 20: Process for monitoring shipment and warehousing via IOT and blockchain

As a result, all supply chain data is transparent and immutable which enables to detect violations of regulations or contracts in real time and make the quality and safety of drugs transparent and dramatically lowering the time and effort required for supply chain and compliance management.

4.4 Payment

Hofmann et. al. (2017) explain that payments in pharmaceutical supply chain can be done between buyer and supplier through cryptocurrencies due to the ease of payment in blockchain as everything is verified automatically. The transaction fees are low comparing to the commissions for the payments through banks. All the payments are transparent thus the fraudulent actions can be prevented. Some of the companies are already accepting cryptocurrency like Amazon.

There is a strong potential for the cryptocurrency when combined with smart contracts to improve existing payment services especially in global real time payments. Cryptocurrencies are the key to the complex digital cash problem that solved how to maintain integrity and consensus across independent and potentially malicious actors. Cryptocurrencies are fundamentally the financial opportunity offered to anyone willing to keep the network secure. Implementing digital payments in to supply chain infrastructure with blockchain will remove the need for each organization to keep their ledger and improve efficiency.

This section analyses the five cryptocurrencies with high market capitalization from coinmarketcap (2019) to determine the most suitable one for business to business transactions. Analysis are done based on three categories; Transactions per second (tps), transaction confirmation time (tct) and volatility.

Low tps duration results in underperforming and slower transaction processing throughput and higher latencies. According to Litke et. al. (2019), Bitcoin (BTC) TPS is from 3 to 7 seconds, Ethereum (ETH) is 15 to 20 seconds same as Tether (USDT), Ripple (XRP) is 1500 seconds and Bitcoin Cash (BCH) is 60 seconds.

Transaction confirmation time on the other hand indicates bad performance when the duration is high. Bitcoin (BTC) tct is 25 minutes, ETH is 2 minutes, XRP is 4 seconds, BCH is 60 minutes, USDT and is 15 to 30 seconds.

Volatility is one of the strongest indicators to determine the best cryptocurrency to serve business to business transactions. High volatility represents serious barriers for companies since the price is not stable.

Following charts are created based on the raw data retrieved from coinmetrics (2019) to show the volatility of each cryptocurrency over time and the data is demonstrated in Appendix.

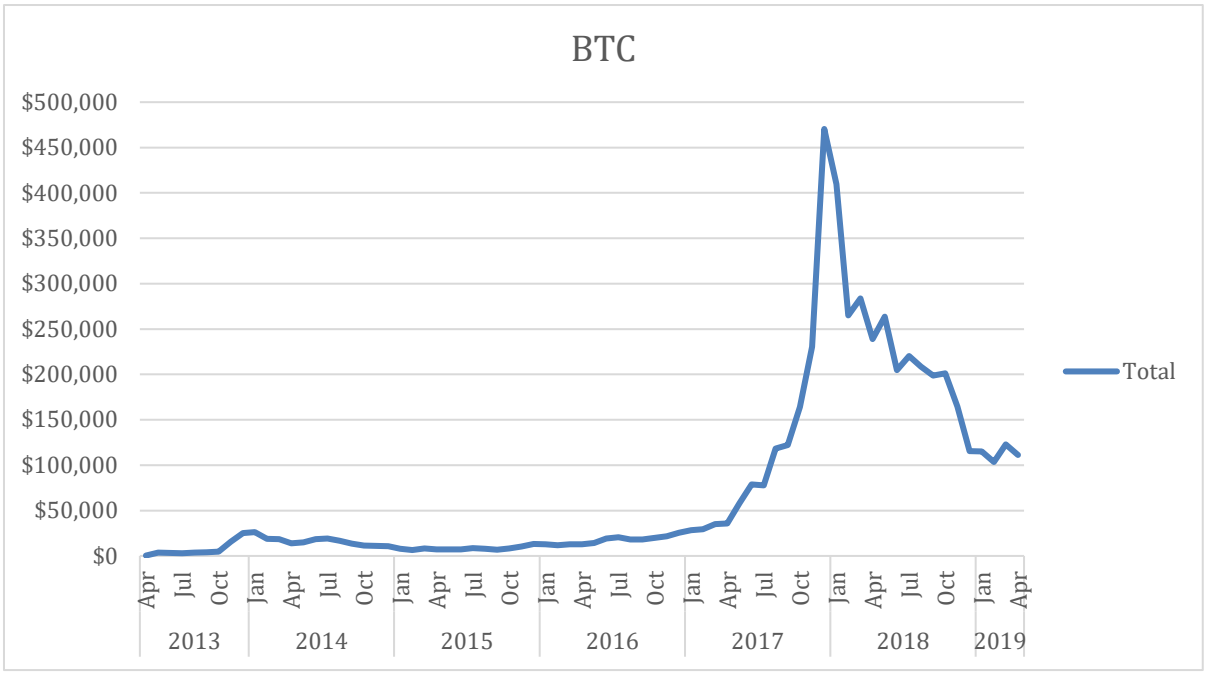

Figure 21: Bitcoin Volatility

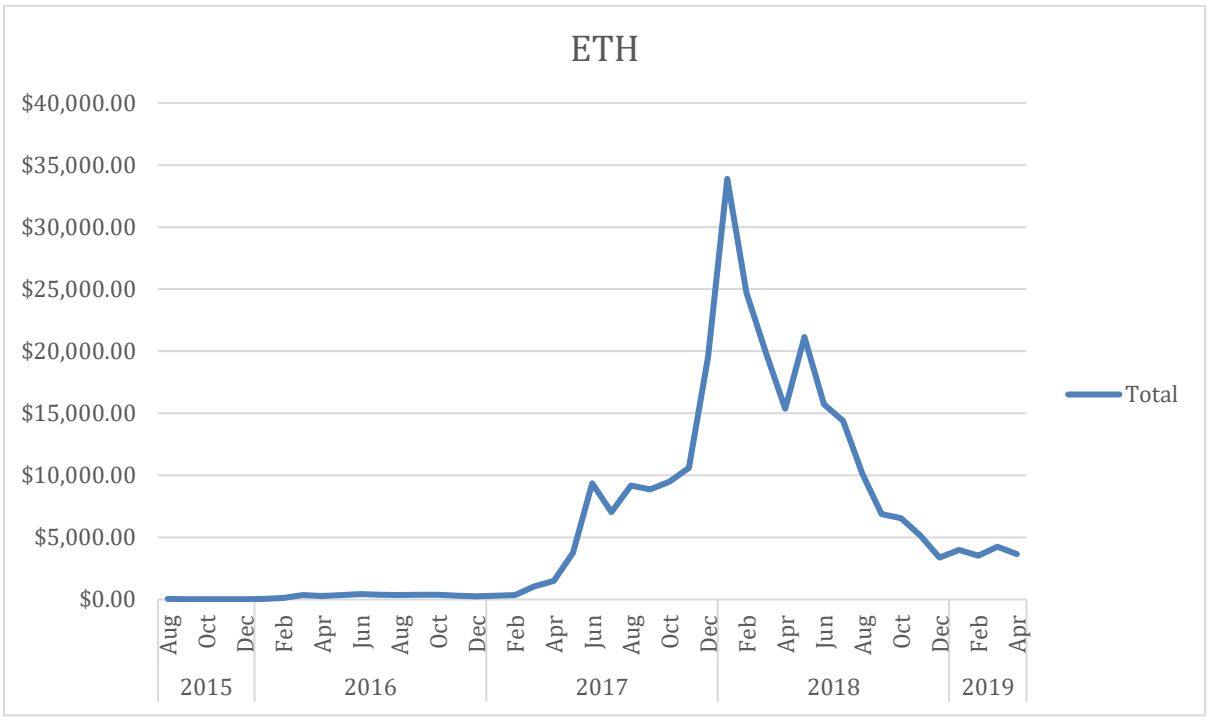

Figure 22: Ethereum Volatility

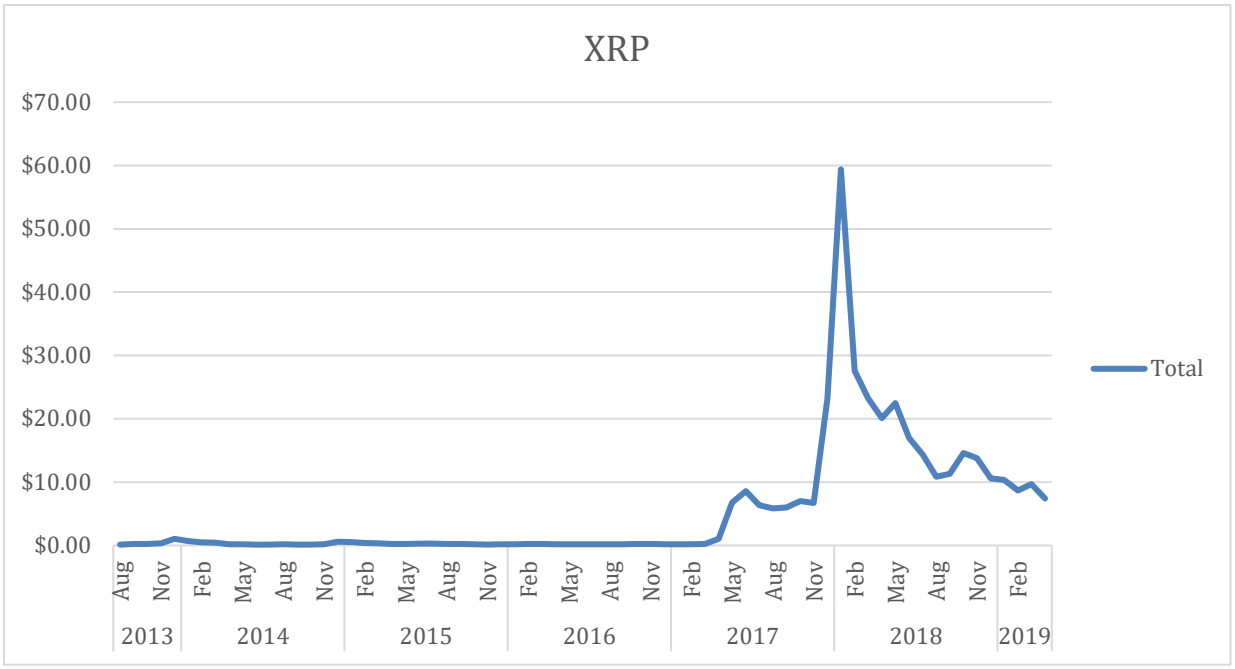

Figure 23: Ripple Volatility

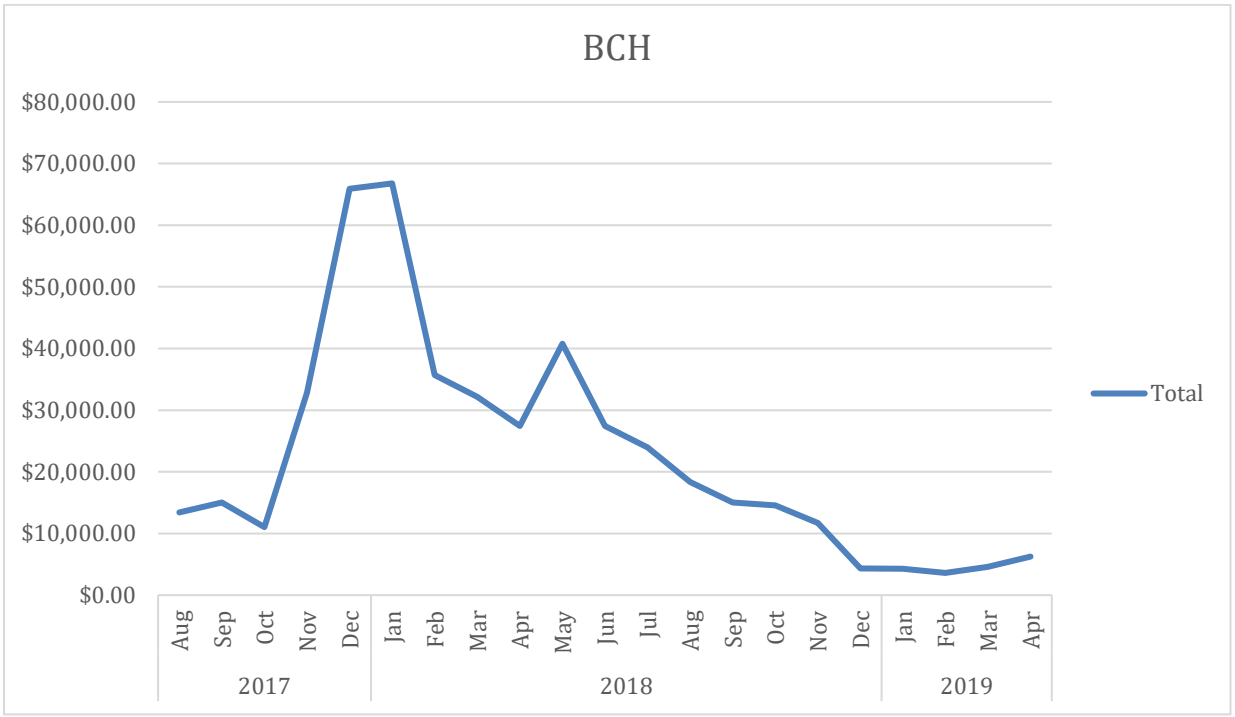

Figure 24: Bitcoin Cash Volatility

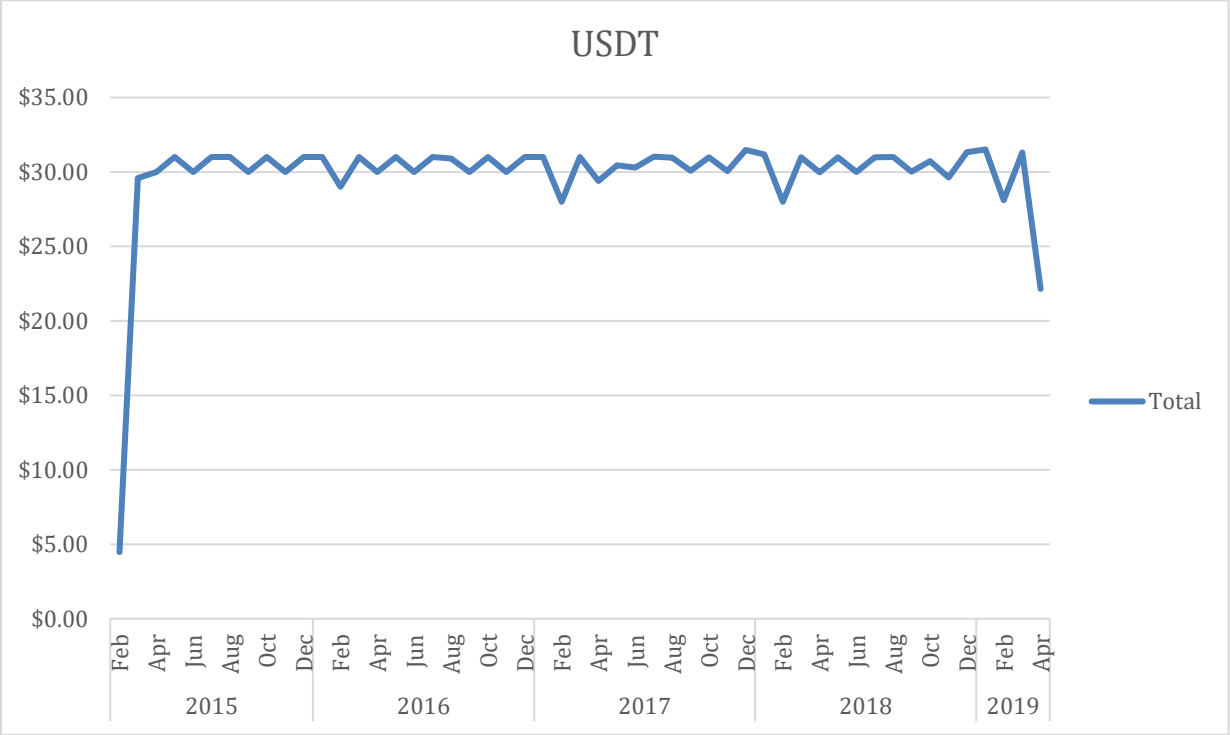

Figure 25: Tether Volatility

It is clearly seen that four out of five cryptocurrency has high volatility whereas Tether (USDT) is the most stable coin without any drastic price changes.

Table 1: Cryptocurrency comparison table

Cryptocurrency	Transactions per Second (TPS)	Transaction Confirmation Time (TCT)	Volatility
Bitcoin (BTC)	Low	High	High
Ethereum (ETH)	Moderate	Low	High
Ripple (XRP)	High	High	High
Bitcoin Cash (BCH)	Moderate	High	High
Tether (USDT)	Moderate	Low	Low

According to comparison table above, Tether performs moderate speed on TPS, low duration on TCT with low volatility makes a strong indicator that it can be considered as a digital payment method.

5. Conclusion

The purpose of this research was to analyze and highlight potential and proven applications of blockchain and distributed ledger technology in pharmaceutical shipping logistics and design a new concept of supply chain management in pharmaceutical industry by using blockchain technology. The steps to achieve this goal were:

- To discover blockchain technology and to gain knowledge on blockchain technicalities,
- To understand the pharmaceutical supply chain business processes,
- To identify the important concepts of blockchain technology and to clarify the findings to be used in pharmaceutical supply chain industry.
- To integrate important findings and blockchain specifications into pharmaceutical supply chain business processes and to design a new concept of supply chain management.

During the early stages of the research, it was found out that blockchain has a lot of potential usage area in business which are still under investigation. Pharmaceutical supply chain is one of the best use cases for blockchain to solve problems occurring during supply chain operations. Blockchain technology can be used to cure these vulnerabilities by fulfilling demand efficiently, driving customer value, improving responsiveness and contributing to financial success.

Pharmaceutical supply chain is constantly growing along with globalization. This global network with established worldwide operations brings the requirement of outsourcing and that the supply chain can be composed of many steps across vendors which may be in different locations around the world. These multiple different parties have lack of transparency because each one of them contains and controls a certain part of data pertaining to what they add into the supply chain. It is getting harder to keep control over the complex processes. This lack of control affects business negatively and causes a lot of vulnerabilities in pharmaceutical supply chains today. Counterfeit drug problem is one of the biggest vulnerabilities. Blockchain can help efficient and effective data exchange between all the parties involved in the supply chain starting from manufacturing through wholesalers, distributors, logistic companies to hospitals, pharmacies and patients. The information through this chain will be from a single source of truth, reliable and secure to prevent counterfeit drugs.

The European Commission and the United States of America put strict rules and regulations for pharmaceutical supply chain to control drug safety. This includes shipping and storing medical products under specific conditions. Meeting regulatory requirements in pharmaceutical industry is a big challenge and if not compensated, they cause a lot of casualties and economic losses. The information flow with blockchain and IOT enables to track information at item level by each product instead of transaction level (purchase order, sales order, invoice) till its source, thus, the certain conditions of medicines can be monitored during the entire supply chain flow.

Smart contracts can be used in procurement stage and cryptocurrency can be used as a payment method to digitalize and to ensure both parties comply with the contract rules and run their operations without any doubt.

Taking all into account, a complete supply chain flow of pharmaceutical industry is optimized and illustrated in business process modeling, starting from production by recording and tracking products into blockchain at item level. Storage and transport conditions are monitored during shipment and warehousing, and procurement process is done by smart contracts and finance management is expedited by Tether as the most suitable cryptocurrency.

Rerefences

Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): definitions, challenges and recent research directions. International Journal of Computer Applications, 975, 8887.

Amegashie-Viglo, S., & Nikoi, J. A. K. (2014). Supply Chain Management of the Pharmaceutical Industry for Quality Health Care Delivery: Consumer Perception of Ernest Chemists Limited as a Pharmaceutical Service Provider in Ghana. Journal of Information Engineering and Applications, 4(8).

Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9(10), 533.

Barr, A., (2016). Emerging risks : A strategic management guide. Gower Publishing Limited

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., ... & Zanella-Béguelin, S. (2016, October). Formal verification of smart contracts: Short paper. In Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security(pp. 91-96). ACM.

Blanchard, D. (2010). Supply chain management best practices (Vol. 45). John Wiley & Sons.

Chopra, S., & P., Meindl (2005). Supply Chain Management Planning, Strategy and Operations. Pearson Education, Third edition.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

Cmolik, A. (2012). Threats and Opportunities for European Pharmaceutical Wholesalers in a Changing Healthcare Environment. Diplomica Verlag.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Apress.

European Commission (2013, November 5) Guidelines on Good Distribution Practice of medicinal products for human use (Text with EEA relevance) (2013/C 343/01)

Gates, M. (2017). Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. Wise Fox Publishing.

Global Brand Counterfeiting Report (2018) Retrived from

https://www.researchandmarkets.com/reports/4438394/global-brand-counterfeiting-report-2018

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. SIAM Journal on computing, 18(1), 186-208.

Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography(pp. 437-455). Springer, Berlin, Heidelberg.

Hofmann, E., Strewe, U. M., & Bosia, N. (2017). Supply chain finance and blockchain technology: the case of reverse securitisation. Springer.

Hughes, E. (1993). A Cypherpunk's manifesto. URL (accessed 3 August 2004): http://www. activism. net/cypherpunk/manifesto. html.

Iansiti, M., & Lakhani, K. (2017). R.(2017). The truth about blockchain. Harvard Business Review. Harvard University. Retrieved, 27(9).

Jayashree Dubey, J., & Kumar, S., (2007). Supply Chain Management. New Century Publications, Second edition.

Kshetri, N. (2017). Can blockchain strengthen the internet of things?. IT professional, 19(4), 68-72.

Litke, A., Anagnostopoulos, D., & Varvarigou, T. (2019). Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. Logistics, 3(1), 5.

Manners-Bell, J. (2017). Supply chain risk management: understanding emerging threats to global supply chains. Kogan Page Publishers.

Mediledger Project 2017 Progress Report (2018), Chronicled.

Modum (2017) Whitepaper V. 1.0.

Mukhopadhyay, M. (2018). Ethereum smart contract development. Birmingham: Packt Publishing.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Stallings, W. (2005). Cryptography and network security: principles and practice (4th ed). Prentice Hall.

Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

Panetta, K. (2019). Top 10 Strategic Technology Trends for 2019. (n.d.).
Retrieved from
https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/

Penard, W., & van Werkhoven, T. (2008). On the secure hash algorithm family. Cryptography in Context, 1-18.

Presenter, F.M. (year, month). Title of paper or poster. Paper or poster session presented at the meeting of Organization Name, Location.

Quayle, M. (Ed.). (2006). Purchasing and Supply Chain Management: Strategies and Realities: Strategies and Realities. IGI Global.

Raskin, M. (2017). The law and legality of smart contracts.

Rees, H. (2011). Supply chain management in the drug industry: delivering patient value for pharmaceuticals and biologics. John Wiley & Sons.

Rometty, G., (2017, January 9) Retrieved from
https: //www.ibm.com/ibm/ginni/01_09_2017.html

Rooyen. J., V., (2017, May 23). Blockchains for supply chains – part II. Retrieved from
https://resolvesp.com/blockchains-supply-chains-part-ii/

Schmitz, A. (2019, February 11). What is SAP Leonardo? Retrieved from https://news.sap.com/2017/07/what-is-sap-leonardo-2/

SANOFI (2017, May) The Fight Against Counterfeit Medicines. Retrieved from https://mediaroom.sanofi.com/-/media/Project/One-Sanofi-Web/Websites/Global/Sanofi-COM/mediaroom/pdf/2017/DP_Sanofi_counterfeit_EN.pdf

Sayah, D., Wittkamp, N., & Stoffels, J. (2018, August) Blockchain Applications in Transport & Logistics – Deep Dive on Shipping presentation of McKinsey & Company.

Schöner, M. M., Kourouklis, D., Sandner, P., Gonzalez, E., & Förster, J. (2017). Blockchain technology in the pharmaceutical industry. Frankfurt, Germany: Frankfurt School Blockchain Center.

Syncfab (2018, August 3) Decentralized Manufacturing V15.

United Stated Food and Drug Administration (2013, November 27) ‘‘Drug Quality and

Security Act''.

WHO. (2018, January 31). Substandard and falsified medical products. Retrieved from https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products

WHO (2017) Global Surveillance and Monitoring System for substandard and falsified medical products. Retrieved from https://www.who.int/medicines/regulation/ssffc/publications/gsms-report-sf/en/

World Economic Forum (2013) Building Resilience in Supply Chains , WEF/Accenture, Geneva

Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2017). A distributed ledger for supply chain physical distribution visibility. Information, 8(4), 137.

Wüst, K., & Gervais, A. (2018, June). Do you need a Blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45-54). IEEE.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain technology overview (No. NIST Internal or Interagency Report (NISTIR) 8202 (Draft)). National Institute of Standards and Technology.

Appendix

Data below retrieved from coinmetrics to show currency prices over time.

Years	date	Sum of BTC price(USD)
2013	Apr	413.74
	May	3729.06
	Jun	3265.7
	Jul	2799.65
	Aug	3504.3
	Sep	3905.42
	Oct	4836.98
	Nov	15615.18
	Dec	25206.66
2014	Jan	26092.77
	Feb	18783.5
	Mar	18469.24
	Apr	13849.47
	May	14910.72
	Jun	18456.67
	Jul	19212.98
	Aug	16730.32
	Sep	13443.02
	Oct	11338.2
	Nov	10945.52
	Dec	10635.32
2015	Jan	7805.8
	Feb	6518.99
	Mar	8347.63
	Apr	7071.24
	May	7352.04
	Jun	7108.24
	Jul	8644.59
	Aug	7842.62
	Sep	7004.62
	Oct	8131.48
	Nov	10405.99
	Dec	13101.16
2016	Jan	12796.98
	Feb	11666.85
	Mar	12935.12
	Apr	13004.62
	May	14236.36
	Jun	19156.34
	Jul	20552.31
	Aug	18018.4

	Sep	18138.44
	Oct	19861.78
	Nov	21752.23
	Dec	25454.36
2017	Jan	28355.12
	Feb	29557.36
	Mar	35129.59
	Apr	35929.41
	May	57838.21
	Jun	78917.2
	Jul	77785.61
	Aug	118414.19
	Sep	122322.03
	Oct	164032.47
	Nov	230572.38
	Dec	470431.8
2018	Jan	409574.3
	Feb	264942.8
	Mar	283854.34
	Apr	238908.55
	May	263662.46
	Jun	204877.74
	Jul	220145.46
	Aug	208437.83
	Sep	198684.64
	Oct	201314.51
	Nov	164448.45
	Dec	115520.68
2019	Jan	115000.89
	Feb	103521
	Mar	122999.93
	Apr	111372.9

Years	date	Sum of ETH price(USD)
2015	Aug	34.518212
	Sep	30.311641
	Oct	20.32117
	Nov	27.995069
	Dec	27.417914
2016	Jan	44.93359
	Feb	127.96
	Mar	342.34
	Apr	271.02
	May	347.39
	Jun	431.91
	Jul	368.67

	Aug	344.8
	Sep	372.62
	Oct	376.69
	Nov	301.67
	Dec	243.52
2017	Jan	313.63
	Feb	341.44
	Mar	1046.11
	Apr	1481.62
	May	3746.08
	Jun	9344.19
	Jul	7044.22
	Aug	9172.7
	Sep	8876.18
	Oct	9491.03
	Nov	10601.07
	Dec	19548.11
2018	Jan	33886.1
	Feb	24710.78
	Mar	19864.4
	Apr	15364.45
	May	21143.43
	Jun	15737.76
	Jul	14385.48
	Aug	10139.15
	Sep	6878.71
	Oct	6542.75
	Nov	5156.85
	Dec	3360.27
2019	Jan	4000.74
	Feb	3531.15
	Mar	4253.26
	Apr	3655.92

Years	**date**	**Sum of XRP price(USD)**
2013	Aug	0.144131
	Sep	0.249306
	Oct	0.253546
	Nov	0.35741
	Dec	1.015607
2014	Jan	0.691684
	Feb	0.476325
	Mar	0.422898
	Apr	0.204298

	May	0.170383
	Jun	0.123755
	Jul	0.146162
	Aug	0.159373
	Sep	0.144931
	Oct	0.151092
	Nov	0.201647
	Dec	0.602378
2015	Jan	0.559212
	Feb	0.387994
	Mar	0.320746
	Apr	0.246315
	May	0.225177
	Jun	0.279726
	Jul	0.27575
	Aug	0.24937
	Sep	0.222118
	Oct	0.157116
	Nov	0.133936
	Dec	0.196084
2016	Jan	0.178121
	Feb	0.227319
	Mar	0.2507
	Apr	0.206435
	May	0.190134
	Jun	0.186625
	Jul	0.200141
	Aug	0.187679
	Sep	0.20237
	Oct	0.256051
	Nov	0.232951
	Dec	0.204045
2017	Jan	0.20268
	Feb	0.171375
	Mar	0.228371
	Apr	1.037162
	May	6.735033
	Jun	8.558161
	Jul	6.327514
	Aug	5.820667
	Sep	6.006062
	Oct	6.988858
	Nov	6.712209
	Dec	23.246156
2018	Jan	59.39
	Feb	27.59685

	Mar	23.211904
	Apr	20.120198
	May	22.452915
	Jun	16.976948
	Jul	14.369928
	Aug	10.823036
	Sep	11.310174
	Oct	14.579171
	Nov	13.75867
	Dec	10.575129
2019	Jan	10.364897
	Feb	8.681844
	Mar	9.701428
	Apr	7.403796

Years	date	Sum of BCH price(USD)
2017	Aug	13408.06
	Sep	15013.49
	Oct	11026.97
	Nov	32841.38
	Dec	65894.92
2018	Jan	66786.16
	Feb	35710.89
	Mar	32161.84
	Apr	27456.32
	May	40796.23
	Jun	27444.15
	Jul	23958.99
	Aug	18368.6
	Sep	15007.95
	Oct	14557.74
	Nov	11720.24
	Dec	4315.44
2019	Jan	4288.32
	Feb	3597.26
	Mar	4564.06
	Apr	6259.13

Years	date	Sum of USDT price(USD)
2015	Feb	4.4770774
	Mar	29.5860031
	Apr	30
	May	31
	Jun	30
	Jul	31
	Aug	31

	Sep	30
	Oct	31
	Nov	30
	Dec	30.999663
2016	Jan	30.999977
	Feb	28.999812
	Mar	30.999585
	Apr	29.999846
	May	31
	Jun	29.999949
	Jul	30.999987
	Aug	30.895858
	Sep	29.999898
	Oct	30.999995
	Nov	29.999997
	Dec	31
2017	Jan	31
	Feb	27.999609
	Mar	30.999613
	Apr	29.387502
	May	30.448919
	Jun	30.292745
	Jul	31.036315
	Aug	30.964073
	Sep	30.075803
	Oct	30.977564
	Nov	30.060641
	Dec	31.46976
2018	Jan	31.183745
	Feb	27.995243
	Mar	30.977903
	Apr	29.963083
	May	30.99253
	Jun	29.997994
	Jul	30.987384
	Aug	31.01475
	Sep	30.025568
	Oct	30.728957
	Nov	29.629947
	Dec	31.337009
2019	Jan	31.51
	Feb	28.097933
	Mar	31.297396
	Apr	22.14