A Project Based Seminar Report

on

"Hyperledger Fabric: A Blockchain Technology"

Submitted to the

Savitribai Phule Pune University

In partial fulfillment for the award of the Degree of

Bachelor of Engineering

in

Information Technology

by

Adarsh Nair

Roll No: T150058596

Class: TE-10

Under the guidance of

Prof. T. A. Rane

Department of Information Technology

Pune Institute of Computer Technology

Sr. No 27, Pune-Satara Road, Dhankawadi, Pune - 411 043

2017-2018

CERTIFICATE

This is to certify that the project based seminar report entitled "**Hyperledger Fabric: A Blockchain Technology**" being submitted by **Adarsh Nair (T150058596 / 3002** & **TE-10)** is a record of bonafide work carried out by him/her under the supervision and guidance of **Prof. T. A. Rane** in partial fulfillment of the requirement for **TE (Information Technology Engineering) – 2015 course** of Savitribai Phule Pune University, Pune in the academic year 2017-2018.

Date: 06/04/2018

Place: Pune

Prof. T.A.Rane
Guide

Dr. B. A. Sonkamble
Head of the Department

Dr. P. T. Kulkarni
Principal

This Project Based Seminar report has been examined by us as per the Savitribai Phule Pune University, Pune requirements at Pune Institute of Computer Technology, Pune – 411043 on

. . . . . .

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

I would like to thank Prof. Tushar Rane for his continuous assistance and support throughout the seminar project. I would also like to thank the staff of the Pune Institute of Computer Technology for creating an atmosphere conducive to learning and progress. I would also like to express my gratitude to my project partners without whom this wouldn't have been possible.

Adarsh Nair.

ABSTRACT

Blockchain Technology has attracted attention as the basis of crypto currencies such as Bitcoin, but its capabilities extend far beyond that, enabling existing technology applications to be vastly improved and new applications never previously practical to be deployed. Hyperledger Fabric (HLF) is a flexible permissioned blockchain platform designed for business applications beyond the basic digital coin addressed by Bitcoin and other existing networks. A key property of HLF is its extensibility, and in particular the support for multiple ordering services for building the Blockchain. Our presentation explains a Perishable Goods Supply Chain Network using Hyperledger Composer.

CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Introduction to Blockchain

Blockchains record a list of transactions in a way that prevents dishonest use, such as tampering or double spending. They allow any computer to keep track of this list by compiling them into a block, which is then encrypted to form a number called a hash. The encryption process is important. It is an algorithm that is easy to calculate but hard to do in reverse (like factorization). The hash value it produces is a unique property of the block, and any tampering with the records would be immediately obvious because this would change the hash. New transactions are next gathered together into a new block and added to the existing hash value. This is then encrypted to create a new hash for the new block. This is added to the next list of transactions when they are encrypted, and so on. The result is a chain of blocks that each contain the hash values of all preceding blocks—hence the term blockchain. Blockchain Technology solves the aforementioned problems as follows:

Due to decentralised nature of blockchain, there is no central authority. So no one single entity can control the records on a blockchain. The blockchain ledger is immutable thus a transaction cannot be reverted or modified. - thus ensuring that it is tamper proof.

1.2 Motivation behind Hyperledger

Bitcoin is a useful way of getting to grips with the blockchain concept. It is also just one (special) example. Blockchain for supply chain uses the same four basic principles. However, there can be significant differences in the way these principles are applied. First, bitcoin uses "mining" as the way to update and extend the ledger. Mining takes large amounts of computer power. It also involves many mining teams over the Internet, each competing to be the one to add the next block to the ledger. Blockchain for business and specifically for supply chain is not obliged to use mining. There are other options for securely updating a business blockchain. Second, the applications for blockchain in supply chain are far more diverse than making or

receiving payments. A large part of this diversity comes from the use of smart contracts.

Hyperledger offers many advancements over traditional blockchain. It does not require mining and solves the 50% attack problem. Using Hyperledger, Business contracts can be codified to allow two or more parties to automate contractual agreements in a trusted way.

1.3 Aim and Objectives

The Distributed Blockchain Application to be constructed eliminates the discrepancies in the records when goods are transported between two parties. It also helps to reduce thefts in the supply chain thus potentially saving the organisation vast amounts of money. It enables trade between to organisations that do not trust each other.The Dapp will have the following functionality:

1) Any Organisation/Individual can register themselves and add their products on the ledger.

2) Ownership can then be transferred from them to the new owner.

3) This grants any user access to the product's ownership history as a proof of authenticity and genuineness.

1.4 Introduction

Business blockchain requirements vary. Some uses require rapid network consensus systems and short block confirmation times before being added to the chain. For others, a slower processing time may be acceptable in exchange for lower levels of required trust. Scalability, confidentiality, compliance, workflow complexity, and even security requirements differ drastically across industries and uses. Each of these requirements, and many others, represent a potentially unique optimization point for the technology. For these reasons, Hyperledger incubates and promotes a range of business blockchain technologies including distributed ledgers, smart contract engines, client libraries, graphical interfaces, utility libraries, and sample applications. Hyperledger's umbrella strategy encourages the re-use of common building blocks via a modular architectural framework. This enables rapid innovation of distributed ledger technology (DLT), common functional modules, and the interfaces between them. The benefits of this modular approach include extensibility, flexibility, and the ability for any component to be modified independently without affecting the rest of the system.

CHAPTER 2

LITERATURE SURVEY

2.1 Attempts for Digitisation

The first known (to me) attempt at cryptocurrencies occurred in the Netherlands, in the late 1980s, which makes it around 25 years ago or 20BBTC. In the middle of the night, the petrol stations in the remoter areas were being raided for cash, and the operators were unhappy putting guards at risk there. But the petrol stations had to stay open overnight so that the trucks could refuel.Someone had the bright idea of putting money onto the new-fangled smartcards that were then being trialed, and so electronic cash was born. Drivers of trucks were given these cards instead of cash, and the stations were now safer from robbery. At the same time the dominant retailer, Albert Heijn, was pushing the banks to invent some way to allow shoppers to pay directly from their bank accounts, which became eventually to be known as POS or point-of-sale.

2.2 Digital Cash

Even before this, David Chaum, an American cryptographer, had been investigating what it would take to create electronic cash. His views on money and privacy led him to believe that in order to do safe commerce, we would need a token money that would emulate physical coins and paper notes: specifically, the privacy feature of being able to safely pay someone hand-to-hand, and have that transaction complete safely and privately.

As far back as 1983 or 25BBTC, David Chaum invented the blinding formula, which is an extension of the RSA algorithm still used in the web's encryption. This enables a person to pass a number across to another person, and that number to be modified by the receiver. When the receiver deposits her coin, as Chaum called it, into the bank, it bears the original signature of the mint, but it is not the same number as that which the mint signed. Chaum's invention allowed the coin to be modified untraceably without breaking the signature of the mint, hence the mint or bank was 'blind' to the transaction.

When working in the late 1980s at CWI, a hotbed of cryptography and mathematics research

in Amsterdam, he started DigiCash and proceeded to build his Internet money invention.

The invention of blinded cash was extraordinary and it caused an unprecedented wave of press attention. Unfortunately, David Chaum and his company made some missteps, and fell foul of the central bank (De Nederlandsche Bank or DNB). The private compromise that they agreed to was that Digicash's e-cash product would only be sold to banks. This accommodation then led the company on a merry dance attempting to field a viable digital cash through many banks, ending up eventually in bankruptcy in 1998. The amount of attention in the press brought very exciting deals to the table, with Microsoft, Deutsche Bank and others, but David Chaum was unable to use them to get to the next level.

2.3 Second Wave - Web Based Money

A particular simple instance of this scenario is depicted in Figure 2.2. Here, Alice wishes to send a single confidential message P to Bob. The plaintext message P is an input to Alice. When Alice processes this input, it produces a ciphertext output C. Both Bob and Eve receive C, process it, and attempt to recover P. The representation of what they compute is shown by PBob and PEve, respectively. Alice and Bob have an advantage over Eve: they share a secret key K. We treat K as an additional input to Alice and Bob. One fresh key K per plaintext P is assumed, but, at least at this abstract level, there is no imposition that K and P have the same length.

2.4 The Regulatory Bust

E-gold ran into trouble for its libertarian ideal of allowing anyone to have an account. In theory this is a fine concept, but the steady stream of ponzis, HYIPs, 'games' and other scams attracted the attention of the Feds.

In 2005, e-gold's Florida offices were raided and that was the end of the currency as an effective force. The Feds also proceeded to mop up any of the competitors and exchange operations they could lay their hands on, ensuring the end of the second great wave of new monies.In retrospect, 9/11 marked a huge shift in focus. Beforehand, the USA was fairly liberal about alternative monies, seeing them as potential business, innovation for the future. After 9/11 the view switched dramatically, albeit slowly; all cryptocurrencies were assumed to be hotbeds of terrorists and drugs dealers, and therefore valid targets for total control. It's probably fair to speculate that e-gold didn't react so well to the shift. Meanwhile, over in Europe, they were going the other way. It had become abundantly clear that the attempt to shut down cryptocurrencies was too successful, Internet business preferred to base itself in the USA, and there had never been any evidence of the bad things they were scared of. Successive generations of the eMoney law were enacted to open up the field, but being Europeans they never really under-

stood what a startup was, and the slightly less-high barriers remained deal killers.Which brings us forward to 2008, and the first public posting of the Bitcoin paper by Satoshi Nakamoto.

CHAPTER 3

METHODOLOGY AND ALGORITHMS

3.1 Introduction to Hyperledger Fabric

Hyperledger Fabric is a platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability. It is designed to support pluggable implementations of different components and accommodate the complexity and intricacies that exist across the economic ecosystem. Hyperledger Fabric delivers a uniquely elastic and extensible architecture, distinguishing it from alternative blockchain solutions. Planning for the future of enterprise blockchain requires building on top of a fully vetted, open-source architecture; Hyperledger Fabric is the starting point.

The Linux Foundation founded Hyperledger in 2015 to advance cross-industry blockchain technologies. Rather than declaring a single blockchain standard, it encourages a collaborative approach to developing blockchain technologies via a community process, with intellectual property rights that encourage open development and the adoption of key standards over time. Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions.

Where Hyperledger Fabric breaks from some other blockchain systems is that it is **private** and **permissioned**. Rather than an open permissionless system that allows unknown identities to participate in the network (requiring protocols like Proof of Work to validate transactions and secure the network), the members of a Hyperledger Fabric network enroll through a trusted **Membership Service Provider (MSP)**. Hyperledger Fabric also offers several pluggable options. Ledger data can be stored in multiple formats, consensus mechanisms can be swapped in and out, and different MSPs are supported. Hyperledger Fabric also offers the ability to create **channels**, allowing a group of participants to create a separate ledger of transactions. This is

an especially important option for networks where some participants might be competitors and not want every transaction they make - a special price they're offering to some participants and not others, for example - known to every participant. If two participants form a channel, then those participants – and no others – have copies of the ledger for that channel.

3.1.1 Shared Ledger

Hyperledger Fabric has a ledger subsystem comprising two components: the **world state** and the **transaction log**. Each participant has a copy of the ledger to every Hyperledger Fabric network they belong to. The world state component describes the state of the ledger at a given point in time. It's the database of the ledger. The transaction log component records all transactions which have resulted in the current value of the world state; it's the update history for the world state. The ledger, then, is a combination of the world state database and the transaction log history. The ledger has a replaceable data store for the world state. By default, this is a LevelDB key-value store database. The transaction log does not need to be pluggable. It simply records the before and after values of the ledger database being used by the blockchain network.

3.1.2 Smart Contracts

Hyperledger Fabric smart contracts are written in chaincode and are invoked by an application external to the blockchain when that application needs to interact with the ledger. In most cases, chaincode interacts only with the database component of the ledger, the world state (querying it, for example), and not the transaction log.

3.1.3 Privacy

Depending on the needs of a network, participants in a Business-to-Business (B2B) network might be extremely sensitive about how much information they share. For other networks, privacy will not be a top concern.Hyperledger Fabric supports networks where privacy (using channels) is a key operational requirement as well as networks that are comparatively open.

3.1.4 Consensus

Transactions must be written to the ledger in the order in which they occur, even though they might be between different sets of participants within the network. For this to happen, the order of transactions must be established and a method for rejecting bad transactions that have been inserted into the ledger in error (or maliciously) must be put into place. This is a thoroughly researched area of computer science, and there are many ways to achieve it, each with different trade-offs. For example, PBFT (Practical Byzantine Fault Tolerance) can provide a mechanism for file replicas to communicate with each other to keep each copy consistent, even in the event of corruption. Alternatively, in Bitcoin, ordering happens through a process called mining where competing computers race to solve a cryptographic puzzle which defines the order that all processes subsequently build upon. Hyperledger Fabric has been designed to allow network starters to choose a consensus mechanism that best represents the relationships that exist between participants. As with privacy, there is a spectrum of needs; from networks that are highly structured in their relationships to those that are more peer-to-peer.

3.2 Components

3.2.1 Membership Service Providers (MSP)

To Membership Service Provider (MSP) is a component that aims to offer an abstraction of a membership operation architecture. In particular, MSP abstracts away all cryptographic mechanisms and protocols behind issuing and validating certificates, and user authentication. An MSP may define their own notion of identity, and the rules by which those identities are governed (identity validation) and authenticated (signature generation and verification). A Hyperledger Fabric blockchain network can be governed by one or more MSPs. This provides modularity of membership operations, and interoperability across different membership standards and architectures.

3.2.2 Fabric CA

The Hyperledger Fabric CA is a Certificate Authority (CA) for Hyperledger Fabric.It provides features such as: 1) registration of identities, or connects to LDAP as the user registry. 2)

issuance of Enrollment Certificates (ECerts). 3) certificate renewal and revocation

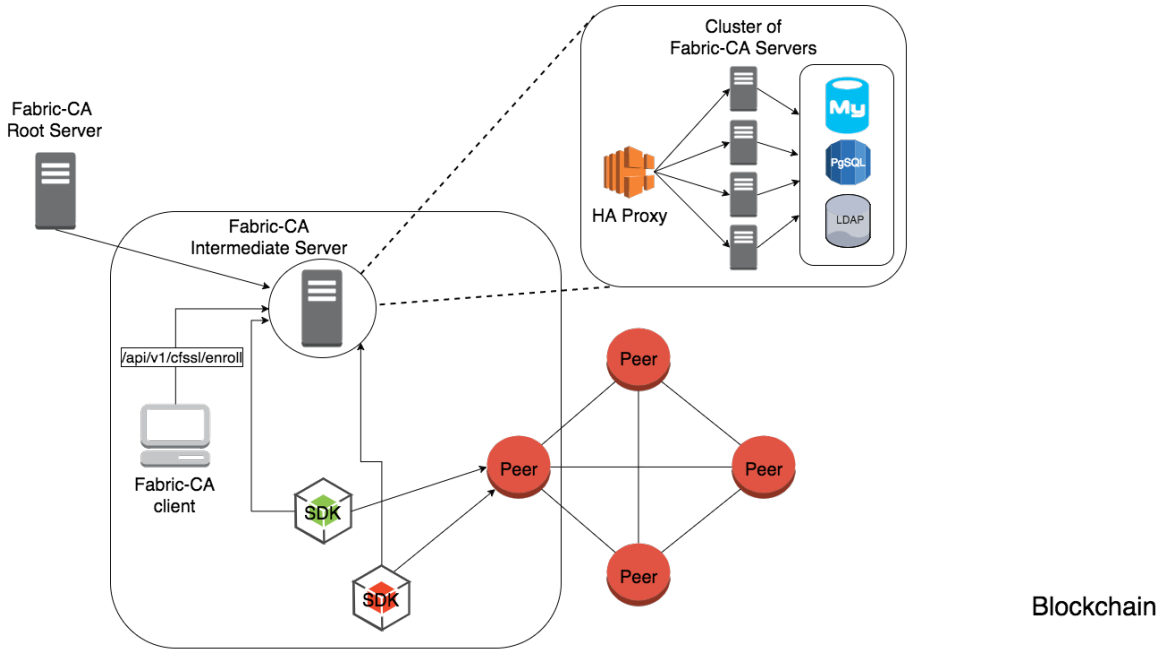

Figure 3.1: Working of Fabric CA

3.2.3 Ordering Service Nodes (Orderers)

The orderers form the ordering service, i.e., a communication fabric that provides delivery guarantees. The ordering service can be implemented in different ways: ranging from a centralized service (used e.g., in development and testing) to distributed protocols that target different network and node fault models. Ordering service provides a shared communication channel to clients and peers, offering a broadcast service for messages containing transactions. Clients connect to the channel and may broadcast messages on the channel which are then delivered to all peers. The channel supports atomic delivery of all messages, that is, message communication with total-order delivery and (implementation specific) reliability. In other words, the channel outputs the same messages to all connected peers and outputs them to all peers in the same logical order. This atomic communication guarantee is also called total-order broadcast, atomic broadcast, or consensus in the context of distributed systems. The communicated messages are the candidate transactions for inclusion in the blockchain state.

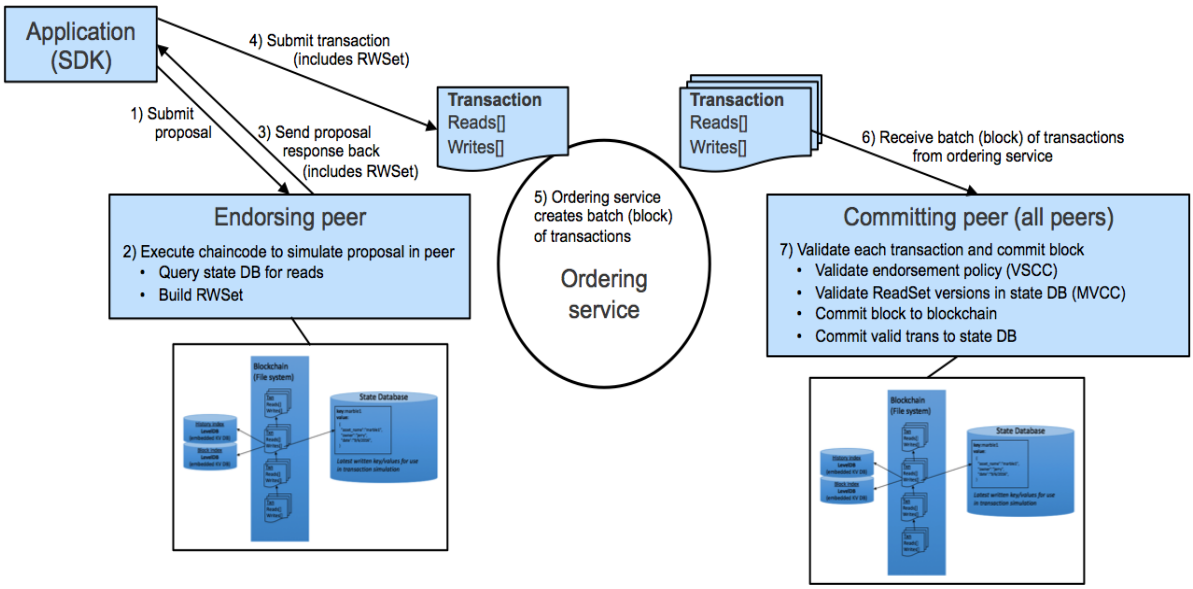

Figure 3.2: Ordering Services in Fabric

3.2.4 Peer

Peer receives ordered ledger state updates in the form of blocks from the orderer and maintains the state of the ledger. Peers can additionally take up a role of an endorsing peer.

3.2.5 Organization

Organizations logically separates members (peers) and they may or may not share the MSPs. It is recommended to have one MSP per organization and we follow that recommendation.

CHAPTER 4

ADVANTAGES AND DISADVANTAGES

4.1 Challenges

4.1.1 Ecosystem still in progress

The first telephone was useless until the second one arrived. In time the phone spread all over the world and now we can't do without it. The situation is similar for blockchain and companies that want to do business with specific partners. Those partners will need to buy into blockchain as well. For example, Tomcar mentioned above only uses bitcoin payments for about 2% of the parts it buys. However, niche uses of blockchain are on the rise. It may be just a matter of time until businesses "join the dots" for widespread acceptance.

4.1.2 Currency Volatility

Bitcoin is an easy way to start using blockchain. The problem is that bitcoin exchange rates with other currencies can change rapidly. Payment terms must be short enough or flexible enough to be able to cash in bitcoin and recover the value expected. Bitcoin and other cryptocurrencies (Ether for example for the Ethereum platform) are also volatile in another sense. If you lose the digital key (passcode) to your cryptocurrency reserve, there is no other way of getting it back.

4.1.3 Technology and knowhow

Blockchain programming takes a mix of software skills. It also helps to understand economies and businesses, especially your business. You may have to train staff or hire new people with these skills. You could also outsource your blockchain development to a third party. The best choice for you will depend on your current situation and future aspirations.

4.1.4 Mindset

Blockchain was started by people who wanted to decentralise applications and operations. They wanted to make dependency on centralised entities like banks optional instead of obligatory. This is a new way of thinking. Don't be surprised if it takes you or your colleagues a little time to shed your mental shackles and get into the swing of the blockchain movement.

CHAPTER 5

APPLICATIONS

5.1 Applications

5.1.1 B2B Payments

Though Cryptocurrencies(Blockchains biggest application) are garnering a lot of attention these days, an institutional level of acceptance is still missing. The system would get a major push if banks are willing to accept and hold cryptocurrencies as deposits and exchange it for fiat currencies.

5.1.2 International Payments

Typically, if one wants to transfer money to a person or an institution in another country, they use a bank/money exchange based wire transfer. This process of wire transfer takes two business days because it has to go through domestic Automated Clearing House (ACH) of both nations involved in the transfer. Additionally, international wire transfers have huge minimum costs (approx US $ 45–50) to initiate the transfer. Using Blockchain, this transaction would be done in less than 10 minutes with transaction fees of around 15–50 US cents.

5.1.3 Banking Access in Remote Areas

In a country like Zimbabwe and Afghanistan, where all people may not have access to banks or the banking infrastructure itself is not robust due to uncertainties, currency fluctuations and mistrust; Blockchain is useful as a stable form of currency, which would not lose its entire value overnight.

5.1.4 Trade Finance

According to Investopedia, a 'Letter of Credit' refers to a document issued by the bank guaranteeing a seller about the accuracy of time and value from the buyer. If a buyer is unable to make payments, the bank will cover the full or remaining amount of the purchase. This is a widely tool due to difference in laws and economy of multiple regions and countries involved, where the possibility of valid and timely payments are not guaranteed.

The typical process of issuing 'letter of credit' is very time-consuming and paper-based. This slow process creates liquidity issues for businesses as the time consuming nature of processing makes sellers wait for the payment till the buyer receives goods. Using Blockchain, this can be done in few hours.

There are various initiatives taken to implement this. R3, a global banking consortium for Blockchain, is building prototypes to support trade finance on this technology. Barclays has partnered with the Israeli Fin-tech Wave to guarantee a letter of credit for export of $ 100,000 worth of agricultural products. Such solutions could solve issues in hours which would have otherwise taken days to complete.

5.1.5 Smart Contracts

A Smart contract is nothing but a piece of code stored on all computers of the blockchain network. It defines a set of conditions to which all parties using the contract mutually agree upon. Once the required conditions are met, certain actions are executed and all members of the

network get to the same result by executing this action. This enables smart contracts to execute contractual obligations without any human intervention. The integration of Smart contracts, a big application of blockchain, with payment gateways, would automate a major process.

There are multiple ways in which Smart contracts can be used. For instance, in case of insurance claims, all contracts(claims) can be recorded on a blockchain, thus eliminating multiple claims being registered by one user. Concurrently, the user is also not scammed out of a claim by the company stating that they have already issued a payout.

5.1.6 Supply Chain Tracking

Most of the companies in the world have ERP and supply chain management software yet, there is a limited visibility and details about the whereabouts of product at any given moment. Blockchain can ease the tracking of items across the global supply chain.

The product can be tracked at every stage creating the record of the location, who handled it and when. It can also record details like temperature, internal pressure at each point to help retailers be assured of product safety. This could possibly solve the problem of lost or damaged products in the shipment and increase accountability at each point. Due to an accurate, specific and immutable nature, retailers can resolve issues easily.

Wal-Mart is experimenting with blockchain to address food safety by tracking the place of food items and faster identification of the source of an issue if any product is causing health problems to customers.

CHAPTER 6

ENHANCEMENTS

- Right now, blockchain is used primarily for Bitcoin, which integrates digital flows of money and information via peer-to-peer personal computer networks. According to IT consultancy firm Gartner, blockchain is currently at the peak of the so-called Hype Cycle for emerging technologies. Several companies have recently announced their intentions to use this technology to integrate flows of goods and information within their supply chains. Container shipping company Maersk Line will implement this technology next year to improve the speed and efficiency of insuring cargo. Philips plans to purchase scare materials and then track them throughout the entire life cycle using blockchain. And IBM has announced a collaborative food-industry project with Unilever, Nestlé, Dole and Walmart to set up a blockchain in which product data will be added for all transactions, making it quicker and easier to see where products have come from and what has happened to them.

- Blockchain can transform supply chains, industries and ecosystems. Interestingly, even organisations like banks, who would seem to be losing out, can see opportunities to use blockchain to streamline their own business. In-depth transformation of supply chains will not happen overnight. However, supply chains can already start using blockchain for small portions of their operations. Smart contracts can help eliminate costly delays and waste currently due to manual handling of paperwork. From there, the door is then open to smarter, faster, more secure supply chain from one end to the other.

CHAPTER 7

CONCLUSION

The Hyperledger Fabric is a permissioned blockchain platform aimed at business use. It is open-source and based on standards, runs user-defined smart contracts, supports strong security and identity features, and uses a modular architecture with pluggable consensus protocols. In theory, blockchain can at last integrate – and hence synchronize – the flows of goods, information and money.This would significantly reduce the bullwhip effect while also eliminating cash-flow problems in the chain. However, achieving this utopia will require openness, collaboration and trust from all chain partners. Based on the evolution of other technological developments in recent decades, once it has peaked as a hype blockchain is destined to fall into a deep abyss of disillusion. But with utopia in sight blockchain could achieve a real breakthrough for supply chain management.

CHAPTER 8

REFERENCES

[1] Iuon-Chang Lin and Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges," International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017. (DOI: 10.6633/IJNS.201709.19(5).01)

[2] Linux Foundation, Hyperledger Architecture, Volume 1 Whitepaper. Retrieved from https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf

[3] Satoshi Nakamoto, “metzdowd.com” , “Bitcoin: A Peer-to-Peer Electronic Cash System” .

[4] Sarah Underwood , “Blockchain Beyond Bitcoin” , DOI:10.1145/2994581 Nov, 2016

[5] Marko Vukolic . "Rethinking Permissioned Blockchains". IBM Research - Zurich. DOI: http://dx.doi.org/10.1145/3055518.3055526