

Digital Supply Chain Management Ecosystem Powered by Blockchain Technology

by

Syed Rifat Ahsan
18321014

Yusra Mehrin
18241013

Ismat Sifat Yousuf
16101148

Zunaira Khan
16101230

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
December 2019

© 2019. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis submitted is our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Syed Rifat Ahsan
18341014

Yousra Mehrin
18241013

Ismat Sifat Yousuf
16101148

Zunaira Khan
16101230

Approval

The thesis titled “Digital Supply Chain Management Ecosystem Powered By Blockchain Technology” submitted by

1. Syed Rifat Ahsan (Student ID: 18341014)
2. Yousra Mehrin (Student ID: 18241013)
3. Ismat Sifat Yousuf (Student ID: 16101148)
4. Zunaira Khan (Student ID: 16101230)

Of Fall, 2019 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on December 31, 2019.

Examining Committee:

Supervisor:
(Member)

Mahbubul Alam Majumdar
Professor and Chairperson
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Mahbubul Alam Majumdar
Professor and Chairperson
Department of Computer Science and Engineering
Brac University

Abstract

Most of the leading companies of the world are investing heavily in a computerized system to maintain their supply chain management. From collecting manufacturing equipment all the way to final delivery, products are being tracked by supply chain management software. Supply chain institutions also use their own separate software to maintain confidentiality. Despite this huge investment in digitizing the supply chain system, complete visibility of a product at any given time is not fully achieved. Quality issues, information mismatch, slow cash flow is still hampering the whole supply chain management and financing ecosystem. Companies involved in a supply chain maintain their own databases and the same information might get altered in different data storage or might as well contain redundant or missing information. This situation can create conflicts between parties involved in the supply chain. Thus protecting authentic information throughout the supply chain management still holds a huge challenge along with maintaining the quality of products. Knowing all the information in real-time such as location, ownership status, product status etc. within the involved parties is still not fully attained by the existing systems. As all parties of a supply chain system have their own standalone software, real-time communication amongst this software developed in different platforms using different technologies is not relatively feasible. By taking advantage of this situation, other illegal parties can inject counterfeit products in the supply chain. This can be a significant threat not only to the company's revenue but also to its public image. In this paper, we propose a thoughtful framework to implement a unique decentralized ecosystem powered by the new emerging innovative technology called blockchain for the whole supply chain system.

Keywords: Blockchain, supply chain, smart contract, authentication, transactions

Dedication

We would like to dedicate this thesis to our loving parents and teachers.

Acknowledgement

We would like to acknowledge and appreciate our sincerest gratitude towards our respected supervisor and mentor Mahbubul Alam Majumdar for his time and assistance towards the successful completion of this thesis as well as for giving us the opportunity to work on this topic.

We would also like to express our heartfelt gratitude towards Ms. Aleya R Iqbal, Head of Information Technology of IPDC Finance Limited in Gulshan for allowing us to visit their corporate office and for introducing us to their ongoing blockchain integration in supply chain.

Last but not the least we would like to thank our beloved parents for their constant support and appreciation.

Table of Contents

Declaration	i
Approval	ii
Abstract	iii
Dedication	iv
Acknowledgment	v
Table of Contents	vi
List of Figures	viii
Nomenclature	ix
1 Introduction	1
1.1 Motivation	1
1.2 Thesis Overview	2
1.3 Thesis Orientation	2
2 Literature Review	3
3 Background Analysis	7
3.1 Blockchain Basics	7
3.2 How Blockchain Can Revolutionize Supply Chain	7
3.3 Traditional Supply Chain	10
3.3.1 Inadequate Traceability And Visibility	11
3.3.2 Trust Issues Of Stakeholders	11
3.3.3 Fewer Transparency Options	11
3.3.4 Safety Issues	11
3.3.5 Absence Of Collaborative Forecasting	11
3.3.6 Keeping Up With Customer Demands	12
3.4 The Potential Of Blockchain Technology Integrated In Supply Chain Management	12
3.4.1 Trustless System	12
3.4.2 Immutable	12
3.4.3 Traceable	12
3.4.4 Secured	13
3.4.5 Efficient And Robust	13

3.5	Smart Contract	13
4	Proposed Model	15
4.1	Experimental Setup	15
4.2	Network	15
4.3	Public and Private Keys	16
4.4	Transaction Process	21
4.5	Mining	22
4.6	Real-time Tracking	25
5	Analysis Of Implementation	28
5.1	Network Setup	28
5.2	Smart Contract Development	33
5.3	Web3 Implementation	41
6	Conclusion	46
6.1	Conclusion	46
6.2	Future Scope Of Work	46
	Bibliography	46

List of Figures

2.1	Flowchart of initialization [6]	4
2.2	TradeLens’s automated workflow [14].	6
3.1	Blockchain Framework in a supply chain ecosystem [6]	8
3.2	Working structure of blockchain [18]	9
4.1	A simple structure of the supply chain of a smartphone.	16
4.2	Work flow of the experimental implementation.	17
4.3	Symmetric Cryptography [36].	18
4.4	Public Private key pair for authentication.	19
4.5	Asymmetric Cryptography Visualization [37].	20
4.6	Asymmetric Cryptography for securing transaction data	21
4.7	Transaction Process Illustration	22
4.8	Bitcoin Energy Consumption Index chart [38]	23
4.9	Automated Mining Process	24
4.10	Different Companies using different management softwares	25
4.11	A blockchain-based seamless tracking system	26
4.12	Authentication process and adding of new blocks	27
5.1	Ganache CLI Server (Blockchain)	29
5.2	Ganache CLI server port, wallet, and gas limit	30
5.3	The connection between smart contract and local blockchain server (Ganache CLI Remix)	31
5.4	Web3.js Package for Interacting with the blockchain	32
5.5	All Web3 packages are installed.	33
5.6	Enrollment Algorithm of Involved Parties	34
5.7	Asset/ Product smart contract solidity codes	35
5.8	Transaction Process Algorithm	37
5.9	Asset Creation Process in Solidity Language	38
5.10	Posting Transaction in Solidity Language	39
5.11	Transaction Receiving Algorithm	40
5.12	Automated Mining Algorithm.	41
5.13	Migration.sol contract to initialize the deployment	42
5.14	Testing Smart Contract	43
5.15	Deployment of the product_Asset Contract	44

Nomenclature

The list describes several symbols & abbreviation that will be later used within the body of the document

BC Blockchain

BCT Blockchain Technology

EDI Electronic Data Exchange

IBM International Business Machines

KP Kimberley Process

OEM Original Equipment Manufacturer

RFID Radio Frequency Identification

SCM Supply Chain Management

SC Supply Chain

XML Extensible Markup Language

Chapter 1

Introduction

Supply chains are vast ecosystems which play a predominant factor in business growth. With the rapid diversification of e-commerce and scalability of modern business, global supply chains are becoming all the more complex and challenging. In this study we dive into the world of blockchain-enabled supply chain ecosystem that drives the wave of technological innovation set to expand and empower complex supply chain solutions.

1.1 Motivation

Our primary motivation was to research and utilize Blockchain Technology (BCT) to enhance Supply Chain Management (SCM). We explored several research papers, journals, articles and finally decided to work on the Blockchain (BC) optimization on SCM to elevate business growth. SCM is a very complex and vital part of any business structure. From the raw material to the end product, a lot of parties are involved in the process namely suppliers, buyers, stakeholders, financial institutions, etc. The traditional supply chain system offers several problems that are hindering business development. Extensive paperwork slows down the movement of a product in the supply chain. Lack of trust between the involved parties create issues in business deals and consumes considerable amount of time. Information mismatching is also a big issue as different parties use different technologies to manage SCM. If we can bring the whole SCM under a single secured system like Blockchain, many problems will be solved and the door for multiple opportunities will be unlocked. The merging of business and technology fostering the transformation of the whole scenario is powered by blockchain, a revolutionizing innovation which showcases the need for shifting away from the obligation to have a centrally dependent trusted authority in a massively distributed network of a supply chain.

After analyzing various research approaches, we found that integrating BC technology in SCM requires a properly designed software. A lot of attention should be paid in order to build a blockchain-based management system. Network type, mining, security, confidentiality, accessibility, etc have to be addressed and handled carefully while implementing the system. In this paper, we have tried to design SCM incorporating BC while keeping all those significant constraints in mind.

1.2 Thesis Overview

This paper highlights on the applications of blockchain towards transforming the supply chain management ecosystem. After the advent of blockchain technology unveiled by Satoshi Nakamoto in 2008, the staggering potential of blockchain innovation unlocked the possibilities of security solution and shifted the trust towards technology rather than people. One of the main purposes of this paper was about the dynamic application of blockchain technology in supply chain management providing transparent interactions between producers, retailers, distributors, transporters, suppliers, and consumers within supply chain and how it enhances trust among the stakeholders.

1.3 Thesis Orientation

The illustrated chapters of this paper are organized in the following orientation process. Chapter 2 presents a brief review of previous works and applications of blockchain in supply chain mechanism. Chapter 3 demonstrates a thorough analysis of the background of the paper as well as case studies. Experimental setup, flowcharts and simulations are introduced in chapter 4. Then, chapter 5 provides the implementation analysis in detail along with algorithms and relevant data. Finally, chapter 6 concludes the paper along with some insights of future scope of work and summarizes and subsequently provides the references.

Chapter 2

Literature Review

As an emerging technology Blockchain has established itself strongly. Bitcoin was the first popular implementation of blockchain technology back in 2008 [1]. In 2019, Samsung [2] and other big companies are moving towards blockchain based solution for secured storage, asset transaction, financing, management, etc. Supply Chain is a vital sector which is being revolutionized by blockchain. Numerous researches have been done on managing supply chain more efficiently and effectively.

Walmart is using blockchain to track and keep record of the food inventory [3]. They along with IBM have created a system on Linux Foundation's Hyperledger Fabric. From now on every vegetable supplier needs to adopt to this new technology in order to enhance food safety as well as internal accountability. For the first time in Bangladesh, IPDC Finance Limited has introduced the concept of a digitized integrated program called "IPDC-Orjon" [4]. Orjon is an extensive supply chain finance ecosystem program designed to collaborate the stakeholders of any small or micro-organization. They are using blockchain to increase the traceability of loans and improve transparency.

Korpela et al [5] described how the integration of a digital supply chain (DSC) is done in blockchain, its requirements and technicalities. DSC collaboration is a process to digitalize the multi-partner system where the leading companies work as a hub that encompasses other involved supplied companies. They came up with the idea of Cloud integration that will offer a cost-effective business procedure and enhance the opportunity for DSC.

Queiroz et al [6] discussed the opportunities of blockchain in Supply Chain Management (SCM) and challenges that are in SCM as the blockchain technology integrates with SCM. This study intends to highlight what the recent blockchain applications in SCM are, the main

disruptions and challenges in SCM as a consequence of blockchain adoption and what the future of blockchains holds in SCM.

Apte et al [7] explains the extent at which the blockchain may actually have an impact to revolutionise the existing supply chain management system. The editorial talks about the pros and cons, ranging from the security and transparency to the actual goods that can be considered for transactions. As much as blockchain simplifies the process by replacing the physical authentication steps, it can also provide a pathway for miners to conduct illegal transactions (in verifying contracts, not gaining access to the contents). However, it is only limited to private blockchains.

Manupati et al [8] sheds light on the fact that sustainable supply chain can reduce carbon emission and will be low cost. Their proposed model is to resolve the different production allocation problems of a Multi Echelon Supply Chain (MESC) under carbon taxation policy by Blockchain. They considered the lead time under emission rate restraints as stated in a carbon taxation policy as well as the production, supply, stock, distribution and control decisions in a production allocation-based MESC problem. This scenario is named as a Mixed Integer Nonlinear Programming (MINLP) model. The flowchart of initialization in their proposed model is presented in Figure 2.1.

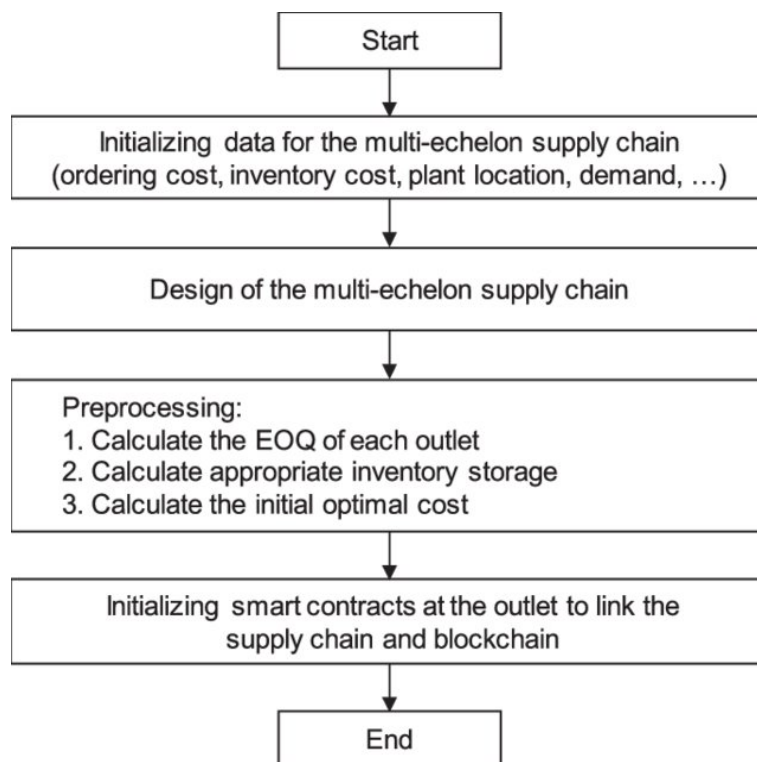


Fig. 2.1 Flowchart of initialization [6]

Dobrovnik et al [9] in their model proposed that the blockchain framework in a supply chain goes through various (mainly four) stages of transformation making it usable despite the assets having no third-party confirmation or to verify the transfer of ownership. These are- single-use, localization, substitution and transformation. The idea has been derived from another existing model by Ianiti and Lakhani [10]. It can be applied to digitise paperwork across various industries ranging from vehicles, food, pharmaceuticals to luxury goods such as diamonds. Initially, a ‘proof of concept’ is used to create a database that would include managing and recording across a network. This would develop to solve specific problems regarding each item handling in the supply chain. IoT may be used to transform the existing framework but is till date unable to support such a large number of devices and data security.

Tian [11] has presented a blockchain technology using Radio Frequency Identification (RFID) to ensure the agri-food supply chain sustainability, by addressing food safety and its manufacturing/production concerns. It functions on the basis of traceability and sharing of authenticated data, over farms, warehouses, markets and plants. It will be accessible for governments and regulators to check on the safe consumption of food. The system has been divided into two parts- (I) for fresh fruits and vegetables and (II) meat. RFID has been extensively described to be useful for identification, monitoring combined with GPS for tracking of goods’ vehicles.

Christidis et al [12] discussed the impact and easiness of smart contracts being deployed throughout a decentralized blockchain technology. The transactions between several parties are still able to be procured by a manufacturer that has long left the network without any user interactions. The “auditable trail of information” is shared within a single database which can be automated using IoT. However, some drawbacks include that any third party can recognize transactions patterns and can identify their hash, subsequently the identity of the participant as well.

El Maouchi et al [13] proposed a system for a supply chain that is totally decentralized, transparent and focused on traceability, namely ‘T R A D E’. The system is structured to have multiple stakeholders encompassing the supply chain and using blockchain to gain maximum traceability. As per the design, customers can access and get all the necessary information to verify their required products. Verification also helps to keep track of the auditability and trustworthiness of the suppliers’ end. These records can be later used as the accountability of both parties. The transaction authenticity is ensured by a digital signature of a private key holder who decides the validity of the transaction.

Litke et al [14] discussed how blockchain can come in handy in case of managing the supply chain industry. It talked about how blockchain will be scalable, transparent, efficient,

secure, trackable and reliable altogether. Furthermore, it shed light on the tradeoff among consensus code, throughput and validation time. The future challenges that still remain to be solved are also discussed in their article. We have used this model to implement our project.

Kim et al [15] presented a model where they linked ontologies to describe food provenance, traceability and knowledge provenance. Mainly, they focus on ontologies and why blockchain should be benefited by these. In this paper, they consider a traceability ontology to translate it to smart contracts to be used as a sample. Furthermore, they executed a provenance trace by imposing few traceability restraints on the Ethereum Blockchain platform.

IBM and Maersk has introduced “TradeLens” which is a block chain based solution for shipping [16]. Tradelens [17] is offering a framework for all the parties involved in shipping to share documents while security is ensured. They are emphasizing on structured document over traditional scanned or pdf documents for better processing and analyzing. Figure 2.2 shows their automated workflow.

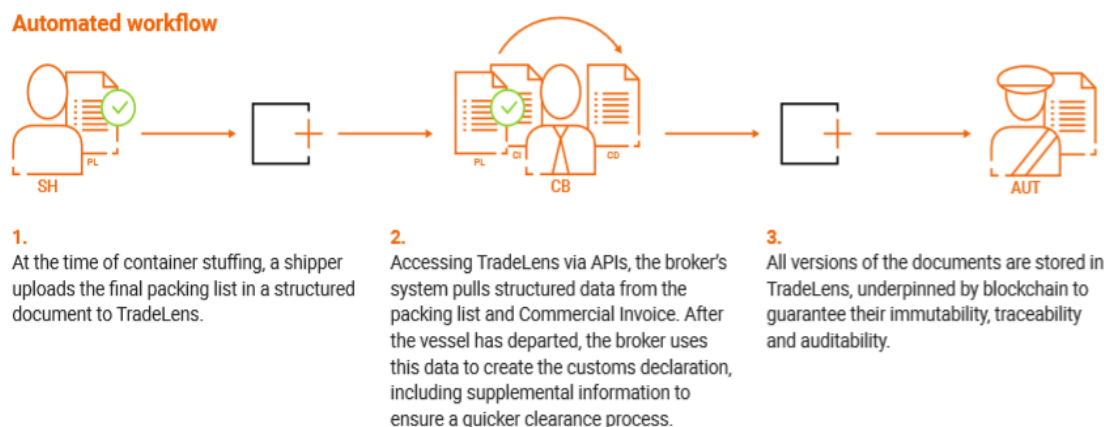


Fig. 2.2 TradeLens's automated workflow [14].

Chapter 3

Background Analysis

In this section we dwell into why blockchain technology can be a plausible fit for global supply chain collaborative management as well as look out for contingencies whether or not this innovation can really live up to its capacity and prowess.

3.1 Blockchain Basics

Blockchain is made up of blocks of information connected with a “chain” (a public ledger). The three pillars of blockchain are: i) Transparency ii) Decentralization iii) Immutability. A block is a collection of real-time data [18]. This information can be of a transaction, people who are participating in the transaction, state of the goods, the actual value of the good in the market when it was being delivered and many more. Data can be added and never get deleted. Immutability is ensured because one can add data but he cannot modify it later on. Blockchain uses different types of cryptography [19]. Among them, the most known is ‘Public Key cryptography’. It allows a public ledger to be viewed by anyone with a public key. However, using a private key, only the people who are involved in the transaction can enter the blockchain and add more data to it. Private keys are kept a secret, also known as a secret key. The Figure 3.1 shows the basic structure of blockchain framework and how the blocks are associated.

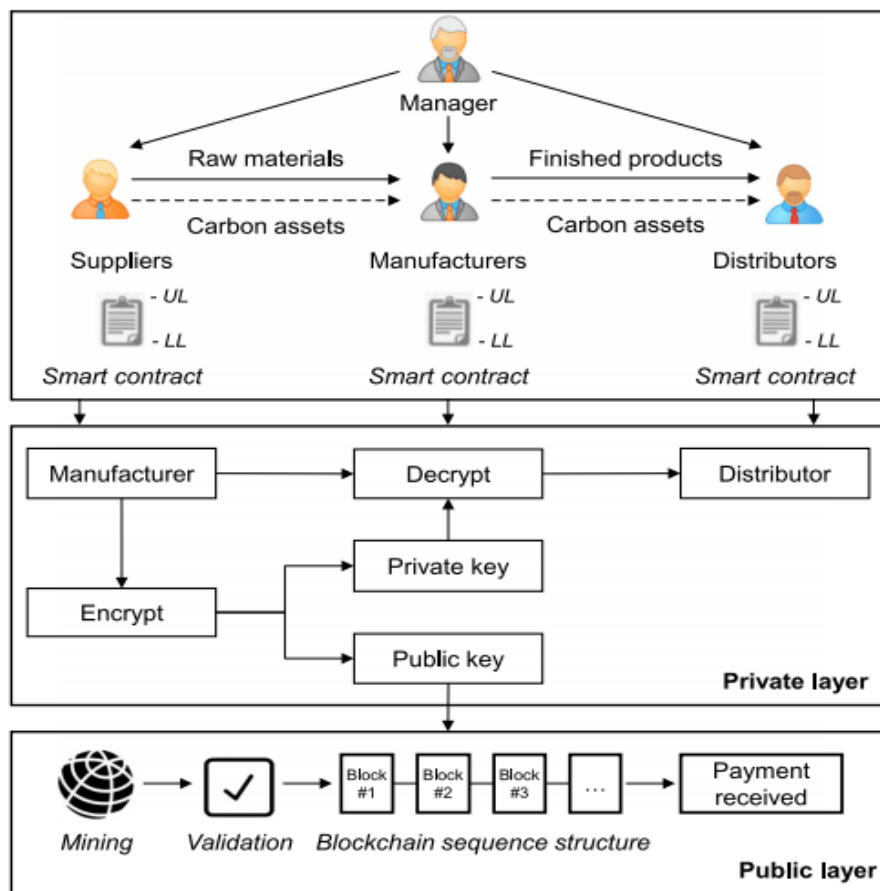


Fig. 3.1 Blockchain Framework in a supply chain ecosystem [6]

3.2 How Blockchain Can Revolutionize Supply Chain

Even though this technology has been out for a while, blockchain is still a fairly fresh and an evolving concept and it is supposed to revolutionize a lot of industries apart from just the supply chains. The more extensive applications of blockchain as much as it appears in bitcoin and other cryptocurrencies have already fuelled interests and despite that other implementations of blockchain [20] such as in supply chain are remarkably exceptional as well. In order to maintain a holistic management, supply chain facilitates the whole process starting from manufacturing a product or service to its distribution process, all the events regarding the supply chain are digitally recorded in the blockchain. We can see the product location status, how long it will take to reach, all the information is stored in an immutable digital record thus making the whole process evenly convenient. Individual control of altering information is not an option. Hence it is a secured, transparent and authorized peer-to-peer network system that can influence the supply chain sector multifold.

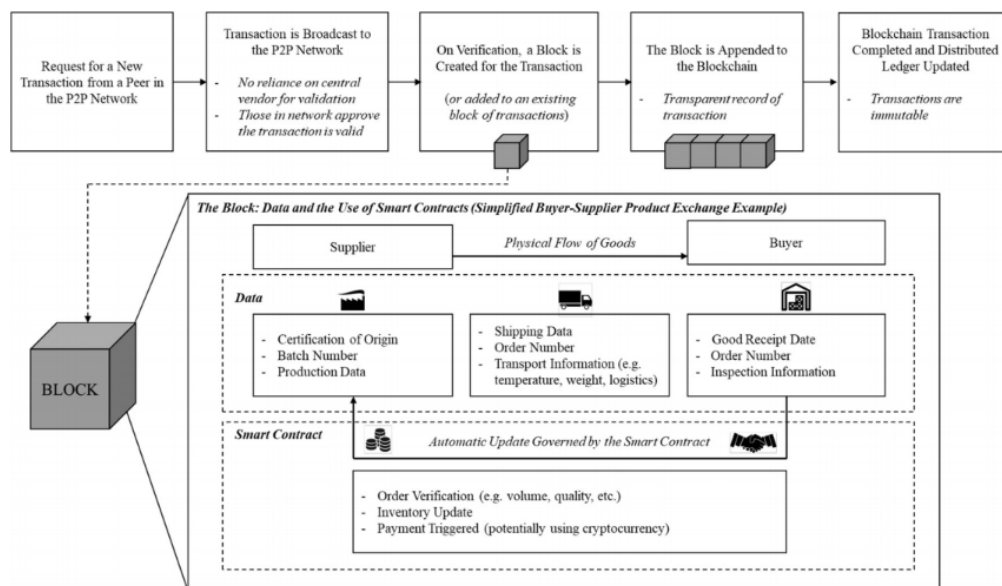


Fig. 3.2 Working structure of blockchain [18]

It is important to identify the business requirements and benefits on the supply chain in order to maximize the application of blockchain in a fruitful way. Minor issues can turn out to have large-scale impacts in the supply chain. For example, a product might get damaged during shipping. Hence customer satisfaction is degraded along with delayed revenues and waste of time. Here blockchain comes to the rescue as it records all the transactional information and progress of a product from procurement to the final delivery thus tracking

issues can be solved at an earlier stage and likewise technical obstacles can be solved easily. Moreover, one of the key features of blockchain is that it provides consensus, that is, all the entities on the supply chain have the exact same version of the ledger making the chances of dispute rare.

Diamonds and other rare elements undergo the mining process by receiving funding from war-zoned activities and are sold to different locations in order to keep the raw materials hidden. Thus, child labor practice in the mining process along with the fabrication of ‘blood diamonds remain as key problems in the supply chain management [21]. Kimberley Process (KP) is a collaboration with administrations, civil societies, and industries in reducing the flow of counterfeit diamonds, that is rough diamonds that are used to finance wars against governments worldwide where India acts as the Chair and the Russian Federation acts as the Vice Chair [22]. 81 participating countries in this process provides a system of warranties of the stone’s origin and thus they trade diamonds inside the group, making up to 99 percent of the total diamond trade volume globally [23]. Everledger, an IBM-based ledger is a blockchain-based solution to improve efficiency of supply chain management which provides each bottle a unique digital identity with an RFID tag in terms of ownership and storage history information and other sales platforms are able to link the bottle to its digital identity for verification purposes [24].

3.3 Traditional Supply Chain

Supply chain management process is an integration of a lot of sub processes that involve raw materials, products, information, capital, suppliers, vendors, customers etc. Hence the complexity rate involving the whole process is higher per se. Multiple companies or at least some departments interact and collaborate for trading on a global scale within a given supply chain and thus the associated costs of managing the inventory, processes and failure detection are substantially higher. Traditional SCM compared to blockchain-based Supply Chain Management (SCM) deals with full distributed process without a central entity coupled with a huge pile of paperwork whereas a blockchain powered SCM maintains a decentralized distributed ledger where each authorized participant can participate, update and read the current SCM state [25]. Hence traditional supply chains are pretty complex and has to confront a plethora of uncertainties. Traditional SCM is driven by planning, monitoring, execution, communication, estimation and prediction of future demand based on the past and current demand and the involved stakeholders to respond to any changes, delays or errors from time to time [25]. Moreover, building a competitive infrastructure, managing invoices

and scheduling, synchronizing supply with demand and measuring performance globally becomes a challenging enough task. Also, the ever-evolving customer requirements along with the barriers and challenges that come in the way play a significant role in making the traditional supply chain profoundly complex.

At about 30 years ago companies used systems like Electronic Data Interchange (EDI) and XML messaging system to communicate across system, having said that these messaging systems might often get out of sync or perhaps information might get mismatched or may have the inventory twice in one location creating conflicts [26]. In the recent times, supply chains are no longer traditional networks of OEMs and suppliers rather vast ecosystems where a single company has multiple manufacturers with many product variants moving through multiple parties, all trying to collaborate in the process [26].

Some vital issues that the traditional supply chain propagates are: . . .

3.3.1 Inadequate Traceability And Visibility

For supply chain, traceability and visibility are one of the most crucial factors to address within supply chain with regard to customer service along with business operational activities [27].

3.3.2 Trust Issues Of Stakeholders

There will be no presence of an effective supply chain network without a solid foundation of trust within the concerned parties within the network. Primarily the stakeholders have to rely on third party intermediaries to support verification and trust which eventually increases the operational [27] costs as well as decrease overall efficiency.

3.3.3 Fewer Transparency Options

“Transparency” - the term itself is vital in the supply chain network which refers to the overall shared access of information about the supply chain cycle within the network. If for some reason information is lost or altered when data is transferred among the relevant parties that means there is an acute shortage of transparency [27] in that network. Traditional supply chain holds huge paperwork documentation which may often fail to ensure and maintain transparency.

3.3.4 Safety Issues

Customer claims to know how the products they are purchasing are made via what process, place of production, raw material production, operations, dealer's information etc. to ensure product quality and if any internal fault occurs in the process. This factor builds up the question of safety of the products within the supply chain since there exists a huge information gap between suppliers and customers in traditional supply chains

3.3.5 Absence Of Collaborative Forecasting

Collaborative forecasting is beneficial as all members of the supply chain can contribute towards the development of the best forecasting process. Collaborative forecasting reduces a company's dependency on the historical records and all the functionalities are operated together collaboratively in one supply chain using a single plan [28].

3.3.6 Keeping Up With Customer Demands

It is also difficult for traditional supply chain stakeholders to stay updated with the ever-changing user demands and applying those required changes into the current supply chain management process. For such issues in supply chain along with the soaring competition in the market, most of the firms have started showing their preference towards introducing Blockchain [29] technology in the supply chain ecosystem.

3.4 The Potential Of Blockchain Technology Integrated In Supply Chain Management

3.4.1 Trustless System

Trust is a very pivotal component in any sector and blockchain redefines trust in supply chain management fundamentally. One of the foremost potential of applying blockchain in supply chains is tracking all the actions that take place, the time of the action as well as the location of each action [23] and every participant within the supply chain can track orders, shipments, progress, deliveries etc. starting from evaluating the performance of each action to monitoring product quality. Apart from that, blockchain based platform also tracks digital assets [14] such as certifications, licenses, warrants, copyrights, serial numbers etc.

Therefore, Blockchain doesn't require any third-party involvement in fact it replaces the third-party association and its significantly a trustless system that benefits the supply chain management.

3.4.2 Immutable

Blockchain is a decentralized ledger innovation which does not rely on any single entity for storage purpose. Information gets updated automatically every time a new transaction is carried out in the connected nodes of a blockchain. The multiple copies of the ledger hold the absolute "truth" about all the transaction record [30] which can never be altered, i.e. it is irreversible. For any attempt of fraudulent activities there needs to have tampering in all of the copies of ledger and the chances of achieving that is quite negligible considering the scalability of the blockchain network. This mechanism of blockchain makes the supply chain highly immutable.

3.4.3 Traceable

One of the principle characteristics of blockchain in a supply chain is ensuring traceability with maximum level of reliability by providing real-time access and status. Hence all the transactions in the network are traceable via timestamp [31] to authenticate the fact that source of the product is genuine and there is no counterfeit material added. Timestamp is a distinctive feature of every block in a blockchain based network.

3.4.4 Secured

Every transaction that is recorded on a block spread over multiple copies of the ledger [32] and they are encrypted meaning that records cannot be modified without modifying the succeeding blocks. That means there is no single point of failure for any infiltration since there is no central location of ledger and thus reduces the risks of a centralized platform. Hence, this makes the supply chain immensely secured.

3.4.5 Efficient And Robust

Blockchain technology aims at reducing complexity and making data sharing more precise and efficient since it creates efficient payment system between banks thus eliminating the need for separate institution management. Smart contracts are able to generate a one-layer

invoice payment system where “Smart invoices” [33] could potentially generate payments automatically for robust processing. Blockchain enables faster e-invoice receipt and replaces paper-based documentation reducing the number of operations along with fewer errors and thus reducing the overall workload.

3.5 Smart Contract

To put simply, smart contract in general terms is a preprogrammed conditional agreement stored inside the blockchain that is all the business rules and terms governed by the contract are embedded in the blockchain and then implemented with transactions. This is like a “digital contract” which automatically executes itself when conditions that are inserted in the blockchain are satisfied. Invented by Nick Szabo in the year 1994, smart contracts are simply computer protocols which doesn't require any third-party involvement just like blockchain.

Let's have a look at a simply elucidated case scenario. Customers forward the cryptocurrency in the smart contract and if the supply chain is fully funded then the contract automatically transfers the currency to the supplier. Likewise if the supply chain network fails to reach their goals for some issues, the payment automatically goes back to the customers. Since smart contract is distributed and immutable just like blockchain, there is no central authorization of currency and it is entirely tamper-proof. Banks can make use of smart contracts for the sake of issuing loans. Smart contracts will also be favourable for delivery companies in order to maintain “payment on delivery” process.

Smart contracts work as a substitute of the conventional procedures where certain conditions are supposed to be met in order to transfer assets and in many cases require lawyers to create contracts and banks to provide Escrow services [34]. Although Ethereum platform has its own version of cryptocurrency known as ethers, it allows anyone to create their own cryptocurrencies [34] as well as pay for smart contracts.

A smart contract is composed of three major mechanisms: the contractual agreements between the parties, the governance of preconditions necessary for the contractual obligations to be carried out, and the actual execution of the contract [35]. Smart contracts contributes to cost reduction and higher efficiency for all parties involved.

Chapter 4

Proposed Model

In the proposed mechanism, under a private blockchain, each of the involved parties of supply chain management will join as a node. So, the entire supply chain will come under a single system like a tree ensuring transparency, security as well as traceability. For example, the following Figure 4.1 shows a supply chain structure of smartphones. All the suppliers, distributors, manufacturers, etc will come under a single blockchain based network. Depending on the type of supply chain the need for the company involvement may vary. For instance, in a smartphone supply chain a customer can be involved in the network for authentication purposes. On the other hand, a supply chain of the chemical industry may not involve the customers in the blockchain network. So, there are many variables to play with while designing a system although the core structure is the same. Here, we have attempted to highlight the code parts of a generalized implementation for managing a supply chain using blockchain.

4.1 Experimental Setup

For implementation procedure, we have chosen the Ethereum platform. Web3 JS [36], the Ethereum JavaScript API to establish a connection between application and blockchain to execute the logic of smart contracts for manipulating data. Ganache [37] provides us with a local blockchain server with ten accounts to experiment with Ethereum. For writing the smart contract we have used Remix [38] online ide for easy observation and manipulation of the smart contract. Figure 4.2 portrays how the entire setup works together collaboratively.

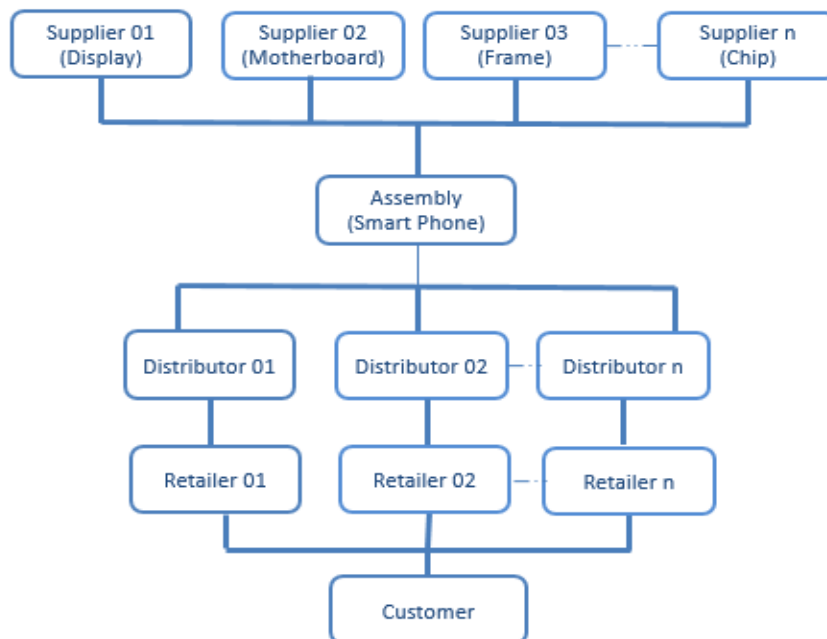


Fig. 4.1 A simple structure of the supply chain of a smartphone.

4.2 Network

To begin with, An Ethereum [39] Private Blockchain Network will be issued by the main company or companies depending on the type of SC. After that, the other participants like suppliers, distributors, retailers, financiers, etc. will join the network with proper verification process by the host of the network. As a result, any outside party will not be allowed to participate in the network and thus ensuring the privacy of the SCM. Then, each participant or blockchain node will be given a pair of public and private keys to access and engage within the network. Public and private keys will work like Bitcoin Blockchain [40]. A public key is widely distributed in the network which holds the identity of a node whereas a private key is a secret password which is required to get access to a node's personal account. After the account is created, participants will be able to make transactions, track the progress in real-time and enjoy other features. Each of the components of the system will be described in the upcoming sections.

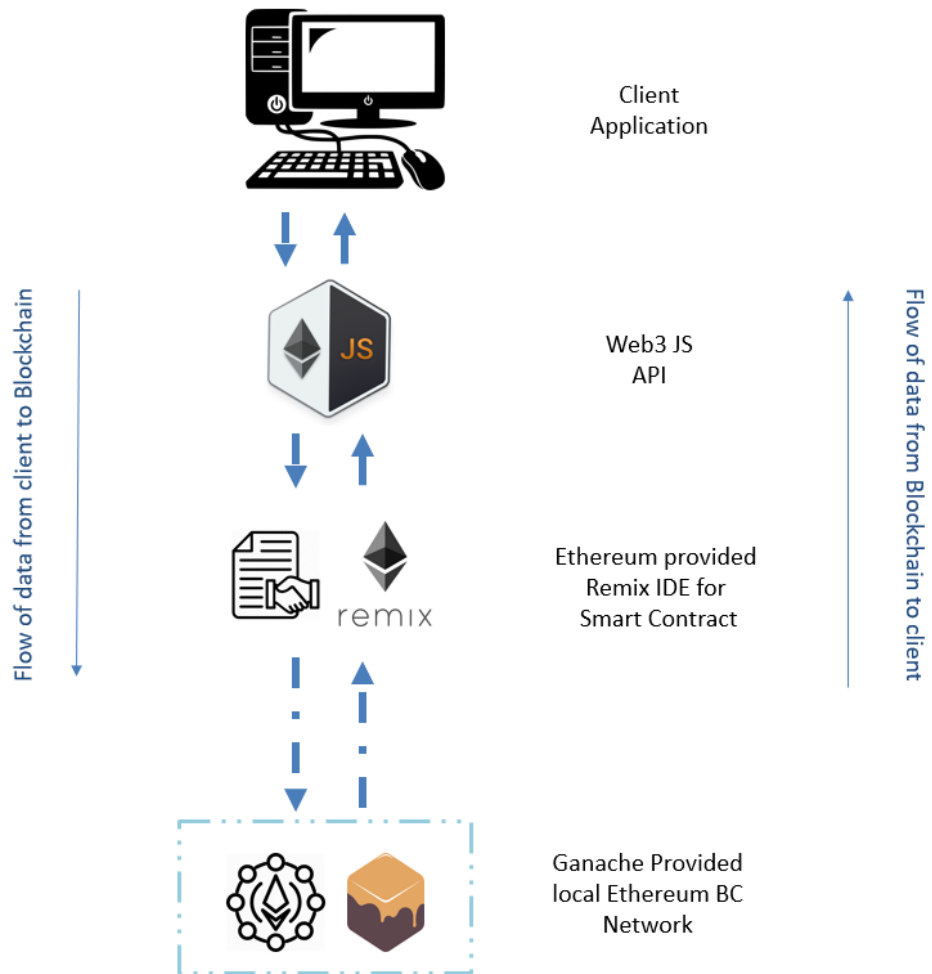


Fig. 4.2 Work flow of the experimental implementation.

4.3 Public and Private Keys

Public and private keys are implemented using asymmetric cryptography. It provides a way to digitally sign transactions to ensure authenticity. If compared with typical symmetric cryptography, it will be understood how and why it is more reliable. Firstly, in symmetric cryptography [41], a piece of information is encoded which can be decoded as well using a key as shown in Figure 4.3. In order to send the information, the receiver will have to have the key to decode it. But, sending the key over the network has a security threat.

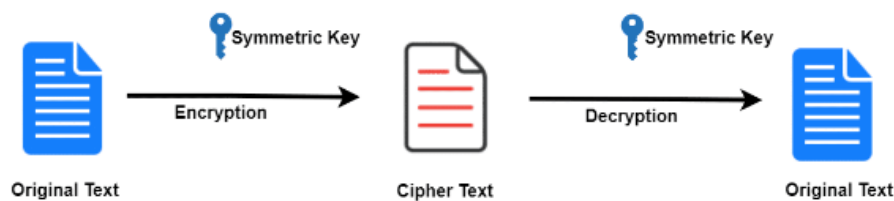


Fig. 4.3 Symmetric Cryptography [36].

On the other hand, in asymmetric cryptography [42], a piece of encoded information can be decoded by both the public key as well as the private key. We can compare the public key as a username which is known globally and the private key as a password which should not be shared by the user. The way in which authentication process works is that the private key can be hashed to public key but doing it the other way is not possible as shown in Figure 4.4.

Additionally, this key pair can help us to send transactions to specific nodes therefore assuring that others will not be able to discover the information. The way it works is that if a piece of information or data is hashed by the private key, it can be opened by the public key and vice versa as portrayed in Figure 4.5.

This process is used to give a digital signature [5] which is there to help other nodes verify whether the sender and the writer of the information is the same entity. Hence, any transaction can be verified by any nodes as the public address will be visible to everyone. But we can use this technique to send transactions to one or more nodes and only they will be able to verify and decode the information. From the flowchart of Figure 4.6, a clear idea about

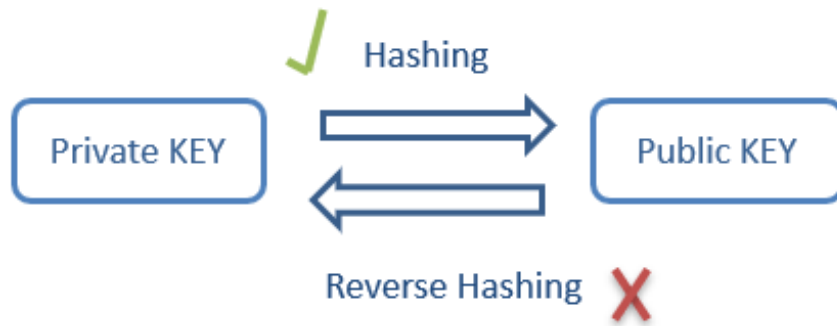


Fig. 4.4 Public Private key pair for authentication.

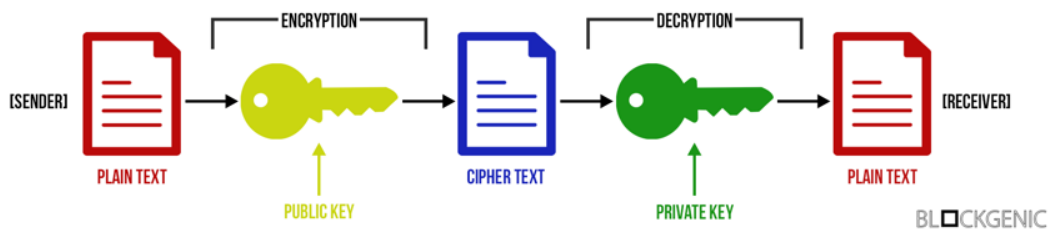


Fig. 4.5 Asymmetric Cryptography Visualization [37].

the process can be evaluated. To illustrate, Company A will encode the transaction with its private address which can be decoded by its public address. Then, Company A will again encode it with Company B's public address which again can be decoded by Company B's private address. On the other side, company B will receive the transaction and will decode it with its private address at first and then will again decode it with company A's public address to get the original data.

4.4 Transaction Process

In the third step, we have demonstrated an easy, fast and reliable way to make transactions. Each transaction will contain information about the product, deal, signatures, etc. to validate authenticity. To eliminate the costing process, no third party will be appointed to validate the transaction. Signatures of the involved parties on the transaction will validate it automatically. The signature can be given by using the private key which will appear as your public key in the network. After both the sender and receiver agrees and signatures digitally, the transaction will be sent for mining in order to get added in a block and then in the blockchain. Furthermore, the visibility of the transaction's information can be controlled by making a "visibility list" while throwing the transaction. The sender can make a list of public addresses to whom the transaction will be visible. This will ensure security, as every participant should not be allowed to see what is in a transaction with which they are not related. Figure 4.7 illustrates the algorithm of transaction.

4.5 Mining

In a typical public blockchain mining is the most time and resource-consuming task. As it is a public network anyone can make a transaction whereas in a private blockchain network like SCM, all the participants involved are verified. Moreover, the transactions are also verified by the participant's digital signature. As a result, we can implement a simple and automated mining process rather than a complicated one like in bitcoin [43] where miners compete against one another to mine a block spending a huge computational power [Figure 4.8].

On the other hand, in businesses and in a private blockchain network we do not need to spend that much time and effort on the mining process. Rather an automated mining system can be used that saves both cost and time, the two most important factors in business. From

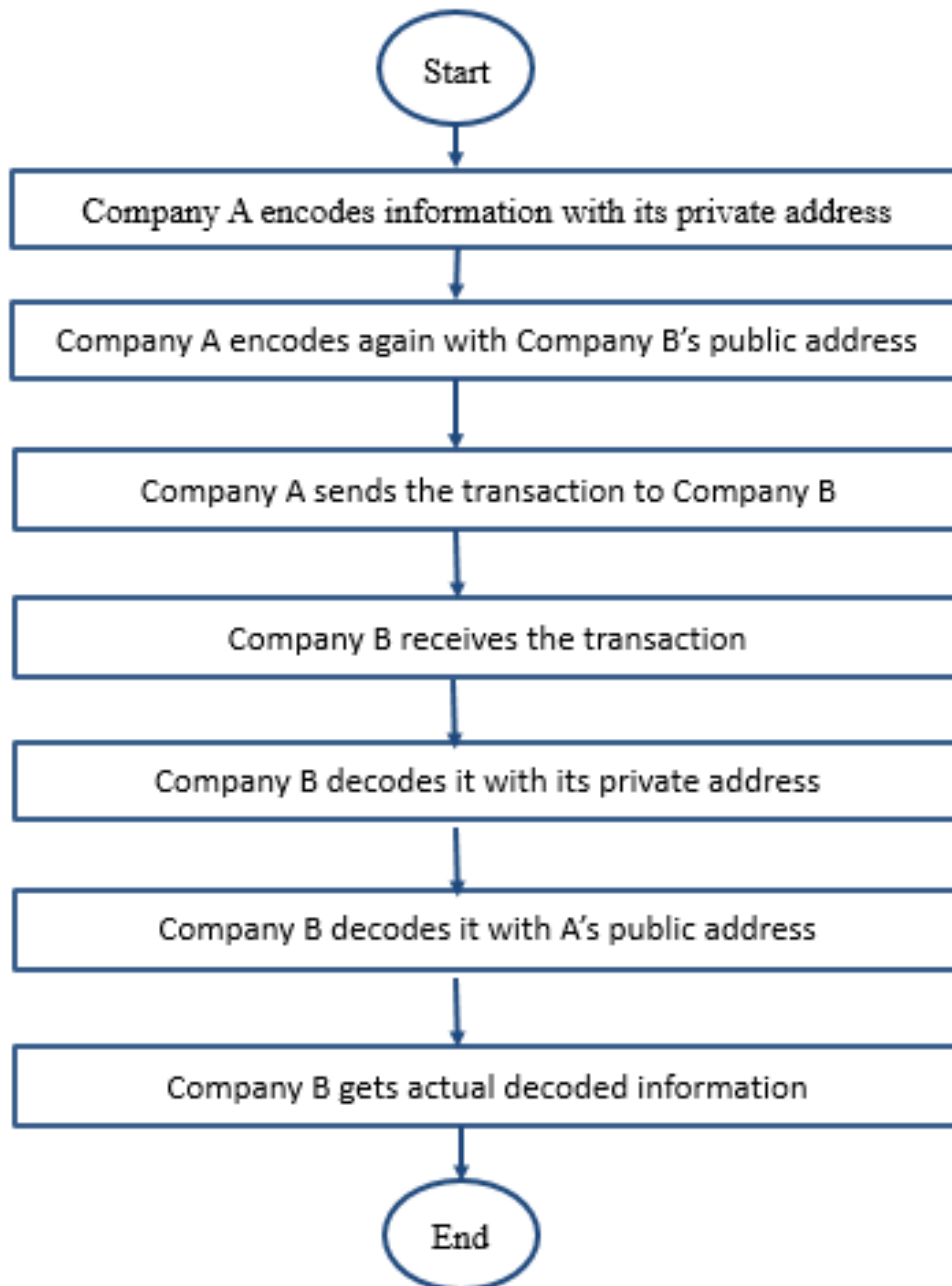


Fig. 4.6 Asymmetric Cryptography for securing transaction data

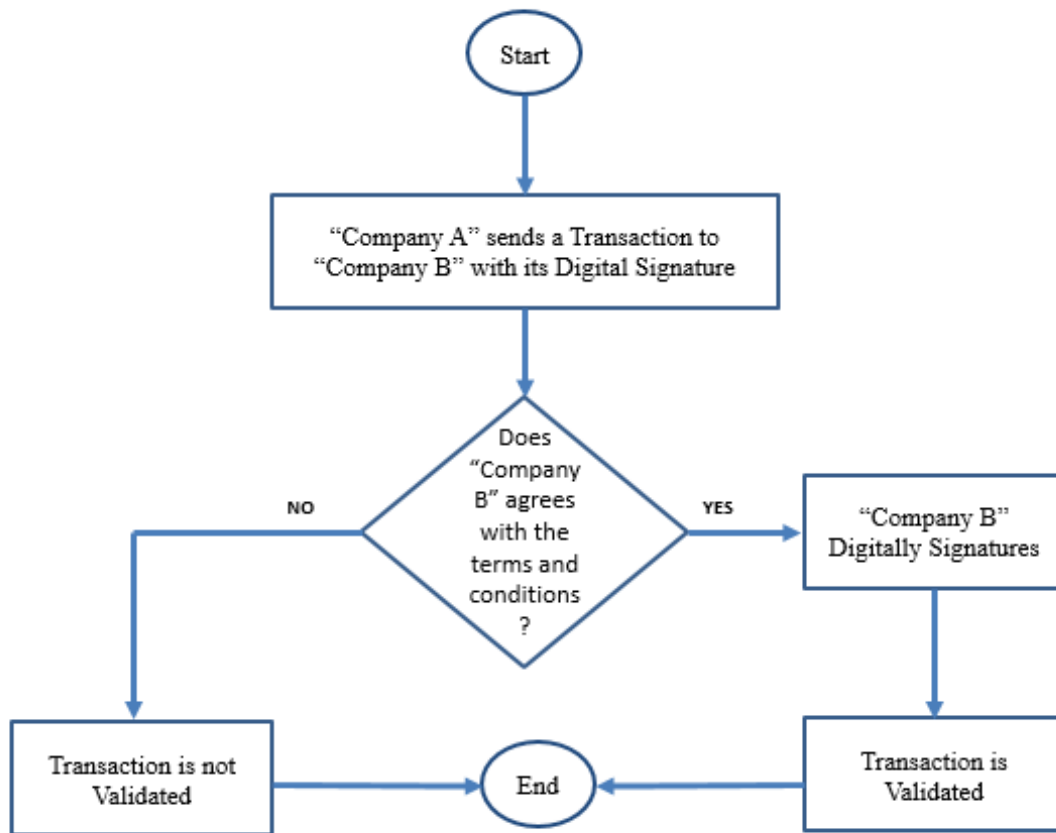


Fig. 4.7 Transaction Process Illustration

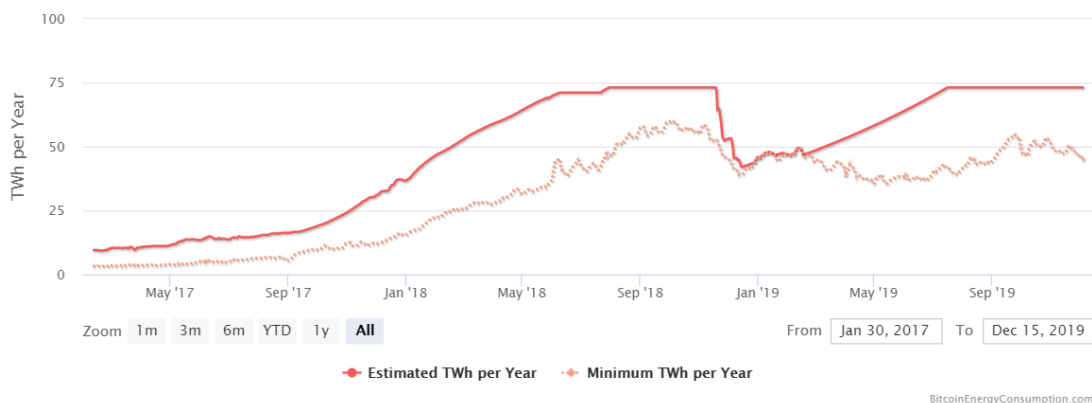


Fig. 4.8 Bitcoin Energy Consumption Index chart [38]

the flowchart in Figure 4.9, an idea about the automated mining process for the system can be found.

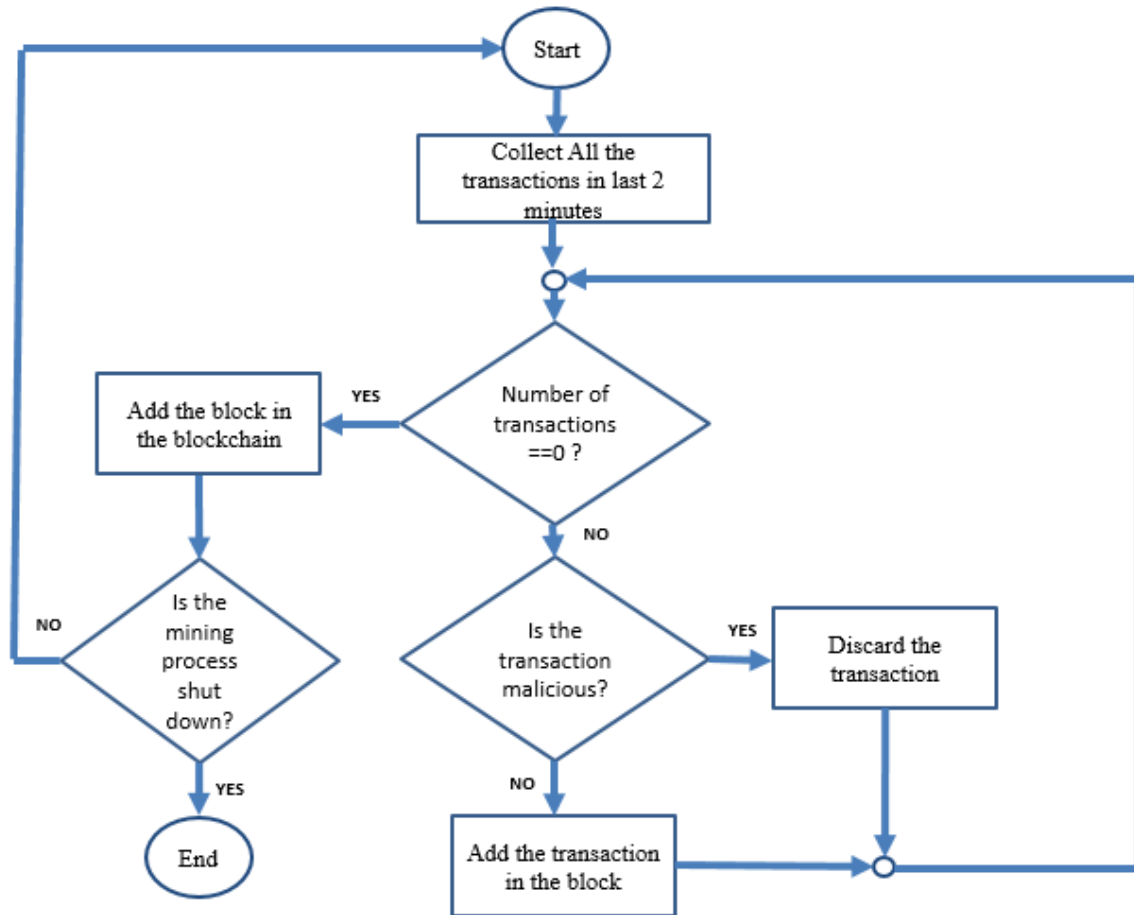


Fig. 4.9 Automated Mining Process

Firstly, the program will collect all the transactions in a certain period of time. Then it will check all the transactions one by one and will detect and discard the malicious ones (if any). All the valid transactions will get added to a block. Lastly, the block will be added to the blockchain and the process will continue to run until it is shut down.

4.6 Real-time Tracking

Another astonishing feature that is enabled by the blockchain is real-time asset tracking. In the traditional tracking system companies store data on their independent centralized database. For instance, company A uses a supply chain software developed in the JAVA

programming language whereas company B's software is developed in Python. They might use different databases as well and intercommunication between companies may be difficult. Even though in traditional system real-time tracking is possible but the experience is not solely seamless.

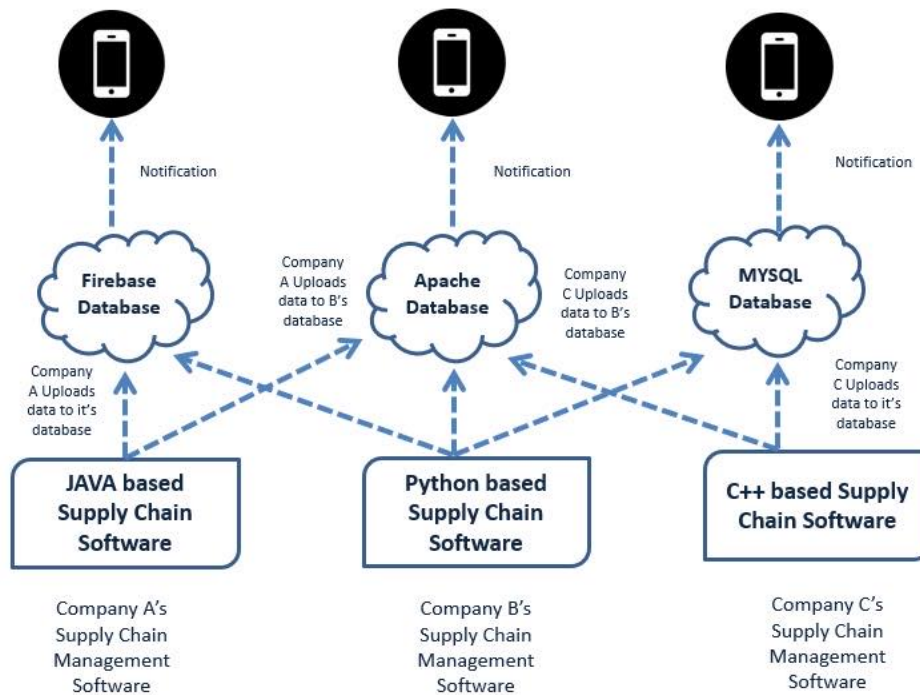


Fig. 4.10 Different Companies using different management softwares

From Figure 4.10, it can be observed how syncing information between companies can be difficult and time-consuming. Moreover, information anomalies are most likely to occur due to differences between platforms. Let us assume a situation where company A is a supplier of company B. Company A uploads supply-related data into its server. Company A also has to upload that data into company B's server so that company B can also know about the product. If A makes any mistake and uploads a wrong information, it will be troublesome for company B. Trust issues will arise dramatically resulting in piles of impediment in the supply chain progress.

However a solution to that very problem is displayed in Figure 4.11. In a blockchain-based supply chain management system all the parties use a universal system [Figure 4.12]. They upload all the relevant data into the blockchain for only once implying that it is a single

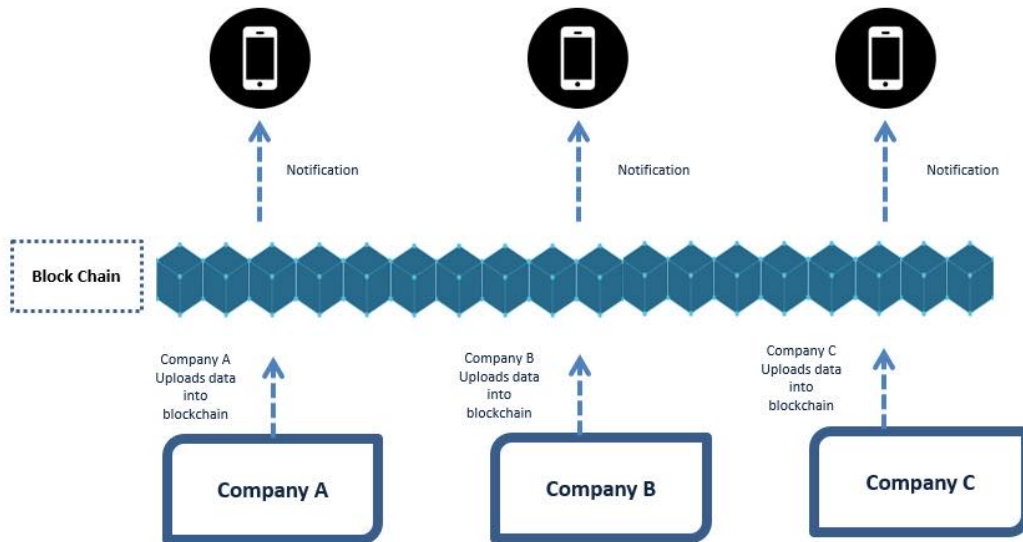


Fig. 4.11 A blockchain-based seamless tracking system

source of truth. As blockchain is tamper-evident and irreversible there is no chance of the data getting modified ever. All the other parties are able to get notifications in real-time without any delays. So, it is safe to say undoubtedly that a blockchain-based approach can save time, solve conflicts and empower a faster-moving and efficient supply chain system.

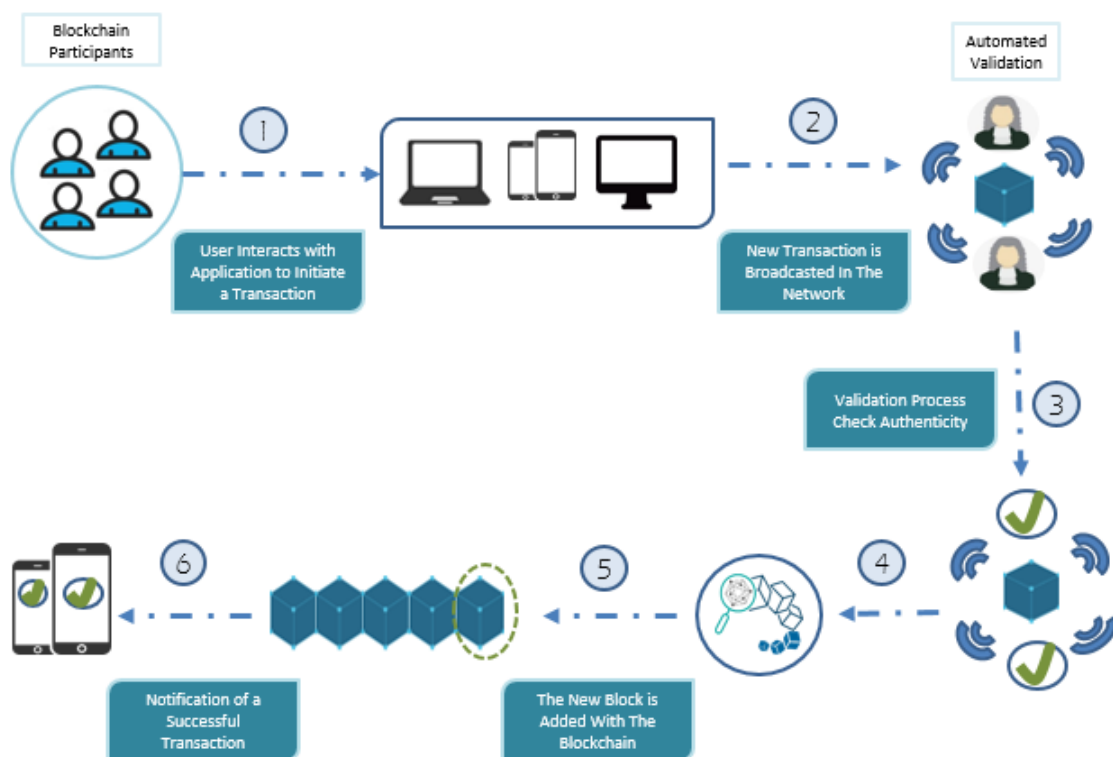


Fig. 4.12 Authentication process and adding of new blocks

Chapter 5

Analysis of Implementation

5.1 Network Setup

In order to implement the proposed model, we need to have a local server for the blockchain. The Ganache will create a local Ethereum blockchain server and will provide us with 10 pairs of public and private addresses. So, we can implement our system without having an actual blockchain server. Though this dummy server has its limitations and we can not have full control over everything. To demonstrate the functions over which we have no control, Python is used to give an idea about the algorithm and process.

From Figure 5.1, we can see the blockchain server has been initiated with 10 accounts. Each account has been given 100 ether to perform the operations. It has to be noticed that these ethers are not real ethers. These are given to test the dummy implementation only.

In Figure 5.2, we can see the wallet we have been given. The wallet will provide us with a way to login to the accounts and manage the transactions. The gas limit is a challenge to write efficient code for smart contracts. For running each transaction a certain amount of gas will be charged. As ethereum is generally a currency based blockchain this gas limit is a very important factor. But in supply chain management we will not have any currency transaction so when we will work on a real blockchain server this concept of gas can be kept aside. The server port is 8545. Through this port, we will connect with the blockchain with the smart contract and with the backend application.

Web3 provider has been used to connect our smart contract with the local Ganache CLI blockchain server. The connection is established via port 8545 which we were given during

```

Command Prompt - ganache-cli
C:\Users\Acer>ganache-cli
Ganache CLI v6.2.5 (ganache-core: 2.3.3)

Available Accounts
=====
(0) 0x2773ba67ad15b3e6f3139ae1de2ed6f05ec2408e (~100 ETH)
(1) 0xfa6cd876f8ffaadedcaaa3802e0ce535ea94bf14b (~100 ETH)
(2) 0xda525790dae119dedf68affe9ea9fd3874f38719 (~100 ETH)
(3) 0x8658c9387e866f10c7f0779ed2c5f6f591c1ca83 (~100 ETH)
(4) 0x9a8bf75c7df2d6a612a99b4b5a39045b383f34 (~100 ETH)
(5) 0x56678dad684d5030e13d467adec4b1fb00f35535 (~100 ETH)
(6) 0xce61aa4f85bf6312861bb48d289410be54889a46 (~100 ETH)
(7) 0x752ab33d33968c7cb092f94fdc03e5ae176308b (~100 ETH)
(8) 0xa588a22f2b05b9d43a9ccf349689ce30558f2f0c (~100 ETH)
(9) 0xa20fe02a0c371e9d29dcb7691d3a9bc7cbfbf89a (~100 ETH)

Private Keys
=====
(0) 0xa3aaf5ef6ffc548f4ab61d8740495342b2f4575b7ea8384c6000a8d7981515d1
(1) 0xfe0bcfdcec5c2726d9e3d1732635ba77b946f931fb73a679975d35855d92374
(2) 0x3d32db2f48d9664a82b70171092f6d7750807d090d47b7f6c59eb3a8d620a451
(3) 0x911a06986c544ebf12e35782d12a1737ecbc3f219f4254be3e6cd4fa81cea2fa
(4) 0xe82b895071b784d88b09f0b6c4f2b5f4fb45de04079b2e8c7c6ae23f5a3f45a3
(5) 0x92e1f244b1fdc5940a01e45986dcfea2baf64dad488ad28f7eaffbf88b3f9efd
(6) 0x959b9eb9fd7b5e5fd9bd3b2146d79a31de06d2c022f33ca4e03efb38a38932b6
(7) 0xd89bbfdbb1576e93c8a37b1a82a18d1a6ecef091b85adf6787d2a143b6658010
(8) 0x655ebd0abf3cb74688bdd280aef6d98f4bc358246de031951571b43038cf6a3a
(9) 0x2819998ab23853e1595463afac4bd37c7c30fa75667172fa64d7350f59c863d8

```

Fig. 5.1 Ganache CLI Server (Blockchain)

```

Command Prompt - ganache-cli
(5) 0x92e1f244b1fdc5940a01e45986dcfea2baf64dad488ad28f7eaffbf88b3f9efd
(6) 0x959b9eb9fd7b5e5fd9bd3b2146d79a31de06d2c022f33ca4e03efb38a38932b6
(7) 0xd89bbfdbb1576e93c8a37b1a82a18d1a6ecef091b85adf6787d2a143b6658010
(8) 0x655ebd0abf3cb74688bdd280aef6d98f4bc358246de031951571b43038cf6a3a
(9) 0x2819998ab23853e1595463afac4bd37c7c30fa75667172fa64d7350f59c863d8

HD Wallet
=====
Mnemonic:      blanket disease chest gorilla sock smoke sweet hundred coffee input ordinary angle
Base HD Path:  m/44'/60'/0'/0/{account_index}

Gas Price
=====
20000000000

Gas Limit
=====
6721975

Listening on 127.0.0.1:8545

```

Fig. 5.2 Ganache CLI server port, wallet, and gas limit

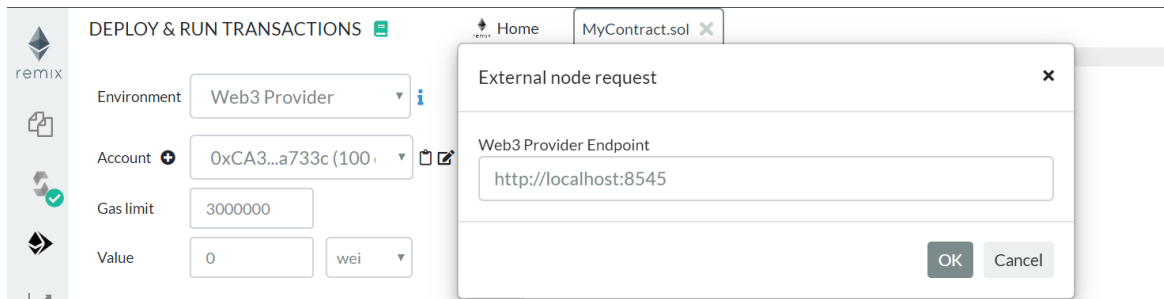


Fig. 5.3 The connection between smart contract and local blockchain server (Ganache CLI Remix)

the establishment of the blockchain network. So from here, this contract has been deployed to our blockchain network.

```

C:\Users\Acer\Final-Thesis>npm install --save ethereum/web3.js

> web3@1.2.3 postinstall C:\Users\Acer\Final-Thesis\node_modules\web3
> lerna bootstrap

lerna notice cli v3.18.4
lerna info Bootstrapping 21 packages
lerna info Installing external dependencies
lerna info Symlinking packages and binaries
lerna info lifecycle web3@1.2.4~postinstall: web3@1.2.4

> web3@1.2.4 postinstall C:\Users\Acer\Final-Thesis\node_modules\web3\packages\web3
> node angular-patch.js

lerna success Bootstrapped 21 packages
npm notice created a lockfile as package-lock.json. You should commit this file.
npm WARN final-thesis@1.0.0 No description
npm WARN final-thesis@1.0.0 No repository field.

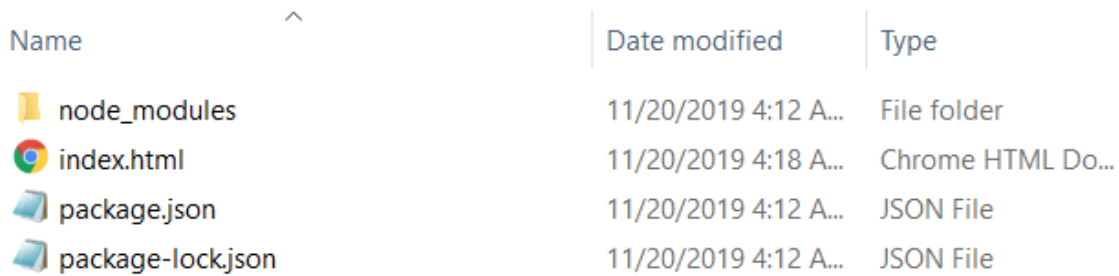
+ web3@1.2.3
added 1 package in 915.729s

```

Fig. 5.4 Web3.js Package for Interacting with the blockchain

Node JS (npm) has provided us with all the necessary packages to implement a backend to interact with our smart contract and local Ganache CLI server. From Figure 5.4, we can see how we have used the npm command to initialize all necessary packages.

In Figure 5.5, we can see the node_module folder which contains all the necessary Web3.js files. After finishing this process we have completed our network and backend setup.

A screenshot of a file explorer window showing a directory listing. The table has three columns: Name, Date modified, and Type. The entries are: node_modules (File folder), index.html (Chrome HTML Do...), package.json (JSON File), and package-lock.json (JSON File).

Name	Date modified	Type
node_modules	11/20/2019 4:12 A...	File folder
index.html	11/20/2019 4:18 A...	Chrome HTML Do...
package.json	11/20/2019 4:12 A...	JSON File
package-lock.json	11/20/2019 4:12 A...	JSON File

Fig. 5.5 All Web3 packages are installed.

5.2 Smart Contract Development

There are many languages to develop a smart contract. Solidity is the most popular language for developing solidity smart contracts. We have used solidity in order to implement our smart contract. Each node will run the smart contract to place the transactions. It can be visualized as the data structure of our implementation. Before proceeding towards blockchain we have to ensure enrollment of a company in the private blockchain network. The pseudo-code is given in Figure 5.6.

As we worked on a dummy blockchain network provided by Ganache CLI, we are confined with 10 given accounts and account registration is not in our hand. When we will get a chance to work with a real blockchain network we will be able to implement this algorithm as per our logic [Figure 5.6]. The logic behind it is pretty simple. Company prefix will ensure the node's identity in the network. Based on the company prefix, access type public address will be created and then as output, we will get private key which must be preserved with utmost secrecy. The participant's private address can be viewed only once from the interactive application. So a participant must preserve his access credentials as the very first task after getting enrolled.

We designed our Assets or products in such a way that after each stage the ownership and other information will get updated. A batch of products is being treated as an asset. As a result, tracking gets easier as in one transaction all the information can be found. Searching blockchain also gets faster and more efficient.

In Figure 5.7, we have created a smart contract to manage the products. First of all, we assigned an "asset_id" to give a unique id to every bunch of products. There are getter

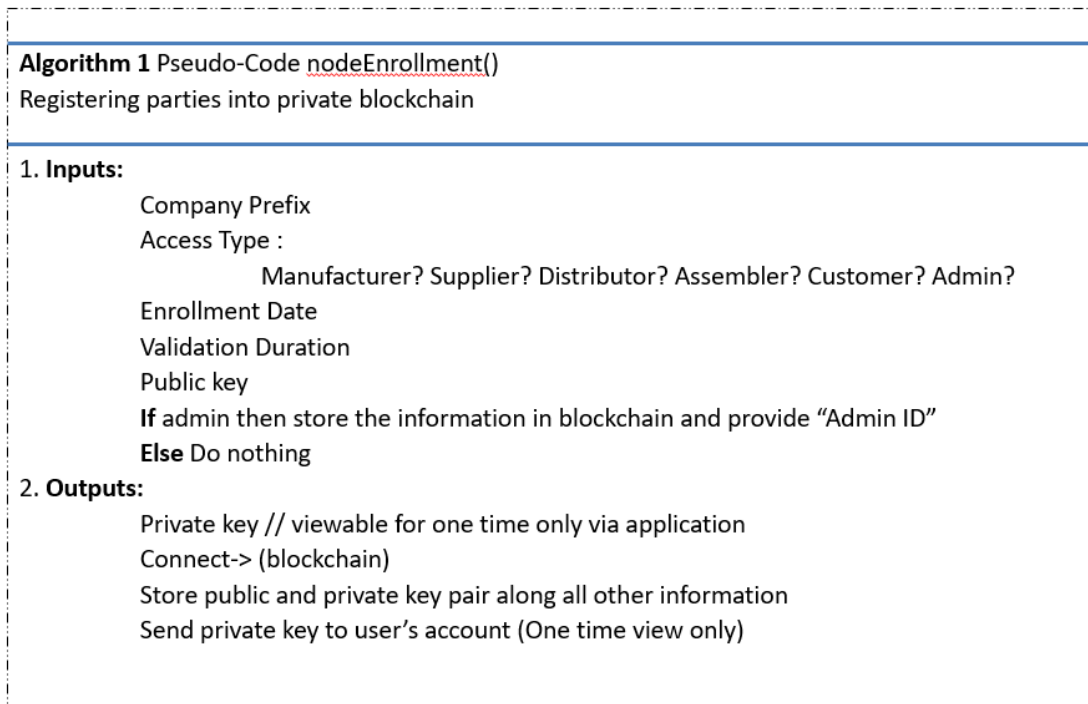


Fig. 5.6 Enrollment Algorithm of Involved Parties

and setter functions for the "asset_id". Then we defined asset struct which contains the attribute an asset must-have. "Asset_status" states about the current state of the asset. The "parentCompany" is the owner company of that product that should have all access regarding the asset.. "isInitialized" indicates if the asset is alive or not and it is a boolean value. "Description" contains all the essential information about the product which can be varied from product to product. Lastly, there is a mapping between "asset_id" and "assetInfo" for creating a list of assets or products.

After enrollment and asset, we implemented the transaction process for moving assets between parties. A transaction needs an asset. Firstly, if the transaction is creating an asset it will assign it with an "asset_id" and initialize all necessary information. If the asset is already being created then some of the information will get updated. Then transaction placer will make a list of public addresses to whom the data will be visible. This step is very important. As a result, we will be able to implement asset tracking while ensuring privacy. With each time an asset moves a new record of this asset is created with updated information. Storing all the information sequentially in the blockchain. Figure 5.8 shows the algorithm of making a transaction.

```
1  pragma solidity >=0.4.0 <0.7.0;
2
3  contract Product_Asset {
4
5      string asset_id;
6
7      function setAssetId(string inputId) public {
8
9          asset_id = inputId;
10
11     }
12
13     function getAssetId() public view returns (string) {
14
15         return asset_id;
16
17     }
18
19     enum Asset_status{shipped, owned, supply, manufacture, dispose}
20
21     struct assetInfo{
22
23         address current_Owner;
24         address recipient;
25         Asset_status assetStatus;
26         uint enrollmentTime;
27         address ParentCompany;
28         string description;
29         bool isInitializez;
30
31     }
32
33     mapping (string => assetInfo) private assetList;
34
```

Fig. 5.7 Asset/ Product smart contract solidity codes

```
Algorithm 2 Pseudo-Code placeTransaction()  
Moving asset among parties of supply chain management  
  
Connect->(blockchain)  
Enter asset_id  
If asset_initialized == False // the asset is newly created  
    setAssetId(id);  
    asset_initialized=True;  
    initializeState(state);  
    initializeOwner(address owner);  
    initializeDestination(address dest);  
    initializedDetails(string Details);  
    initializeEnrollment(string time);  
  
Else // the asset has already been created just update the information  
    changeState(string newState);  
    changeOwnership(address newOwner);  
    updateDetails(string newDetails);  
  
signWithPublicKey(publicKey,privateKey);  
visibilityList(); // list of public addresses of parties who can see the transaction details  
pushTransaction(transactionID); // placing transaction in the blockchain  
  
End();
```

Fig. 5.8 Transaction Process Algorithm

In Figure 5.9, the solidity code of creating an asset is shown. From the algorithm, we have combined all the programs for creating an asset and wrote as one single function. For a better understanding algorithm contains all the steps individually. Through a constructor, we initialize the status. If a user tries to create an asset that is already created he will get an error message. Ultimately all the information are stored and asset gets created successfully.

```
35
36     function initializeState(Asset_status newStatus) public {
37         assetStatus = newStatus;
38     }
39
40
41
42     function assetCreation(string name, string des, string uuid, string owner) {
43     if(assetStore[uuid].initialized) {
44         RejectCreate(msg.sender, id, "Asset already exists.");
45         return;
46     }
47     assetInfo[id] = assetInfo(name, des, owner, true);
48     wallet[msg.sender][id] = true;
49     AssetCreate(msg.sender, id, owner);
50 }
51
```

Fig. 5.9 Asset Creation Process in Solidity Language

Finally, through a method, the transaction is posted in the blockchain through the wallet app which is the front end gateway for the users. We checked if the sender and address exist and then we set all the necessary parameters of the transaction. We have also written a function to retrieve the asset from the id. A user associated with the transactions can only access that transactions only. Thus privacy is ensured. There is also a method to check if the checker is the owner of that particular transaction.

In the third algorithm in Figure 5.11, we have demonstrated the process of receiving a transaction. Public and private key pair is used to implement asymmetric cryptography. Data can be encrypted with the public key and then can be decoded with the private key and vice versa. This process will continue for all the received transactions. After the checking is done the process is ended.

In Figure 5.12, we have described the algorithm of automated mining. Since it is a secured private business blockchain network, the mining process isn't required like a public network. The participating parties are already verified during joining. The software will run this algorithm continuously on the server until it is shut down by the admin. It will collect all the transactions from the transaction pool after a certain time and check for malicious ones. If it detects any malicious transaction it will report to the admin so the admin can check the

```
51
52     function pushTransaction(address to, string id) {
53         if(!assetInfo[id].initialized) {
54             RejectTransfer(msg.sender, to, id, "No asset exists.");
55             return;
56         }
57         if(!wallet[msg.sender][id]) {
58             RejectTransfer(msg.sender, to, id, "Sender is not owner.");
59             return;
60         }
61         wallet[msg.sender][id] = false;
62         wallet[to][id] = true;
63         AssetTransfer(msg.sender, to, id);
64     }
65
66     function getAssetByID(string id) constant returns (string, string, string) {
67         return (assetInfo[id].owner, assetInfo[uuid].des, assetInfo[id].description);
68     }
69
70
71     function isOwnerOf(address owner, string id) constant returns (bool) {
72         if(wallet[owner][id]) {
73             return true;
74         }
75         return false;
76     }
77
```

Fig. 5.10 Posting Transaction in Solidity Language

network's security. If everything goes well it will make a block with the verified transactions and add the block in the blockchain.

5.3 Web3 Implementation

In order to deploy the contract, Web3 JS is the key to make a bridge between our smart contract and blockchain network. Migration.sol contract is the first step to deploy other contracts in the network. Msg id the global variables that store the public addresses and other common information. It can be modified if the modifier is the owner of that account. The owner's public address can be viewed publicly. This can be upgraded with new address [Figure 5.13].

Web3 js comes with a test file. This helps us to test whether a contract is working perfectly in sync with the blockchain given the fact that in a real blockchain network, a smart contract becomes unchangeable when deployed. In Figure 5.13, a piece of code is shown that tests the smart contract that we have developed in Figure 5.7.

In Figure 5.15, we get a view of what happens after deploying the smart contract. Status

```
Algorithm 3 Pseudo-Code receiveTransaction()  
Moving asset among parties of supply chain management  
  
Connect->(blockchain)  
  
While (received transaction !=empty) : //asymmetric cryptography  
    decode the transaction with your private key;  
    decode the transaction with sender's public key;  
    extract transaction's data;  
    if(wantToPushTransaction):  
        pushTransaction();  
    else:  
        do nothing;  
  
endProcess();
```

Fig. 5.11 Transaction Receiving Algorithm

```
Algorithm 4 Pseudo-Code automatedMining()  
Registering Blocks in blockchain  
  
Connect -> (blockchain)  
Collect transactions from transaction pull  
While (mining == 1)  
    While (no. of transaction !=0)  
        if(checkIfMalicious== True)  
            discardTransaction();  
            alertAdmin();  
  
        else  
            addTheTransactionInTheBlock();  
  
    prepareTheBlock()  
    addTheBlockInTheBlockChain()  
  
endProcess();
```

Fig. 5.12 Automated Mining Algorithm.

```
contract Migrations {
    address public owner;
    uint public last_completed_migration;

    modifier restricted() {
        if (msg.sender == owner) _;
    }

    constructor() public {
        owner = msg.sender;
    }

    function setCompleted(uint completed) public restricted {
        last_completed_migration = completed;
    }

    function upgrade(address new_address) public restricted {
        Migrations upgraded = Migrations(new_address);
        upgraded.setCompleted(last_completed_migration);
    }
}
```

Fig. 5.13 Migration.sol contract to initialize the deployment

```
1  var Adoption = artifacts.require("Product_Asset");
2
3  contract("Product_Asset", function(accounts) {
4      it("should assert true", function(done) {
5          var adoption = Adoption.deployed();
6          assert.isTrue(true);
7          done();
8      });
9  });
```

Fig. 5.14 Testing Smart Contract

shows if the deployment was successful or not. Then a transaction has been found. We can also extract the sender's and receiver's public addresses, cost, hash, inputs, value, etc as the contract has been deployed on the blockchain.

```

creation of product_Asset pending...

[vm] from:0xca3...a733c to:product_Asset.(constructor) value:0 wei data:0x608...c0032 logs:0 hash:0xb6a...3a59c

status          0x1 Transaction mined and execution succeed
transaction hash 0xb6ad972d27a24f81bf77176ab04e3f7efcf3858792892ddd49e5833456a3a59c
contract address 0x692a70d2e424a56d2c6c27aa97d1a86395877b3a
from            0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to             product_Asset.(constructor)
gas            3000000 gas
transaction cost 455625 gas
execution cost  302549 gas
hash           0xb6ad972d27a24f81bf77176ab04e3f7efcf3858792892ddd49e5833456a3a59c
input         0x608...c0032
decoded input   {}
decoded output  -
logs           []
value         0 wei

```

Fig. 5.15 Deployment of the product_Asset Contract

Each time we deploy our contract and use the functions to get or set data, a transaction is initiated. All the details associated with the transaction can be found in the Figure 5.13. If the transaction fails there will be a visible red cross instead of the green tick mark. Also, we can listen to the network to understand the data flow.

To conclude our implementation procedure, we would like to point out that we were able to develop the contract successfully by using web3.js. Transactions were also successfully placed. This is just the beginning of our knowledge and learning about blockchain technology within our research area. We have analyzed the system heavily to make it more efficient and business-friendly and developed a smart contract in that regard. Thus it leaves a great opportunity for future work and research scope.

Chapter 6

Conclusion and Future work

6.1 Conclusion

Our objective was to analyze and develop a blockchain based solution for supply chain management. Traditional ways of managing a supply chain is not enough in today's era. Huge paper work, lack of trust, incompatibility, unstructured data (pdf, excel) are hindering the growth of business. So, we have proposed a model which will ensure security, transparency, faster movement of goods, tracking and customer participation for a greater experience. A very important fact to be pointed that, ledgers provided by blockchain helps us to maintain a shared and secured flow of information throughout the supply chain [44]. We have proposed an automated mining system which will reduce cost and save time. Furthermore, the transaction process that has been presented is a magnificent way to ensure transparency and privacy at the very same time. An abstraction of our overall system is shown in Figure 6.1. An easy interaction between users and blockchain will ensure seamless experience. Real time notification of movement of assets or product can be reached to the intended user for real time tracing. In the traditional way where different parties use different software for managing supply chain, this seamless secure experience is impossible to ensure.

6.2 Future scope of work

Implementation of supply chain management by blockchain will open many doors of opportunity. A most valuable fact about this model is that it stores information or data in a

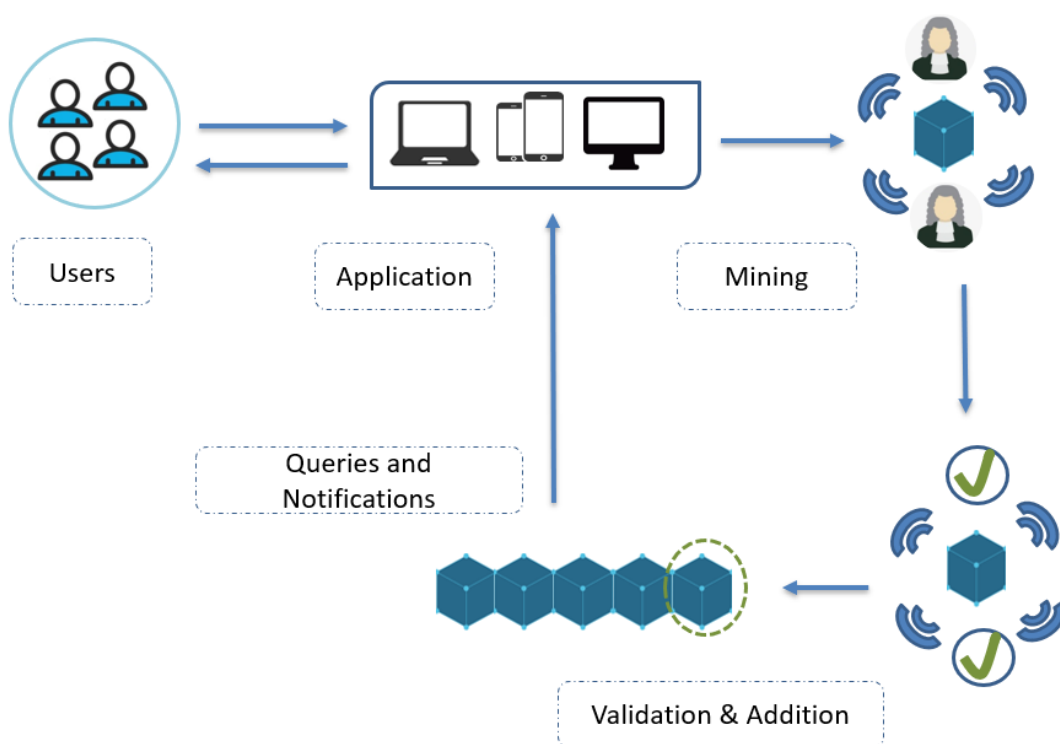


Fig. 6.1 Abstraction of the implementation

structured way. Structured data is one of the most valuable things in today's world. Especially if the data is of supply chain. We can apply machine learning algorithms on this data and find many significant knowledge such as customer behavior pattern, real time demand forecasting, efficient advertising and many more. Blockchain, Artificial intelligence and Big data will completely revolutionize the way business is done. In Figure 6.2 we can get a glimpse of how these technologies [45] work together hand in hand.

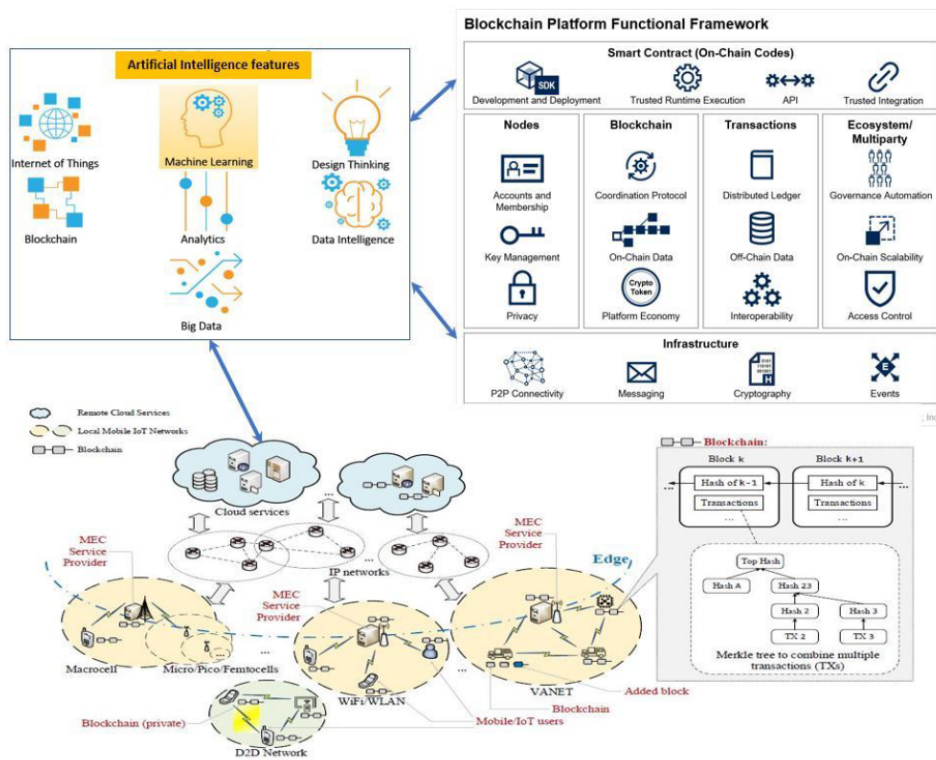


Fig. 6.2 Mobile Edge Computing enabled AI and IoT with Blockchain

Moreover, future scope of work includes the probabilities of analyzing if blockchain technology in different ecosystems can be implemented.

References

- [1] S. Nakamoto *et al.*, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [2] “Blockchain: Enterprise it solution,” 2019. [Online]. Available: <https://www.samsungds.com/global/en/solutions/bns/blockchain/Blockchain.html>
- [3] S. Jagati, “Walmart’s foray into blockchain, how is the technology used?” Sep 2019. [Online]. Available: <https://cointelegraph.com/news/walmarts-foray-into-blockchain-how-is-the-technology-used?fbclid=IwAR00aSaZHRIwa-LXdHRKeNXFgRXSLKyMHtsMD0BLEageqgJFgVMbbHn1CcM>
- [4] S. B. Report, “Ipdcc rolls out blockchain-based supply chain finance platform,” Dec 2019. [Online]. Available: <https://www.thedailystar.net/business/news/ipdc-rolls-out-blockchain-based-supply-chain-finance-platform-1837315>
- [5] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital supply chain transformation toward blockchain integration,” in *proceedings of the 50th Hawaii international conference on system sciences*, 2017.
- [6] M. M. Queiroz, R. Telles, and S. H. Bonilla, “Blockchain and supply chain management integration: A systematic review of the literature,” *Supply Chain Management: An International Journal*, 2019.
- [7] S. Apte and N. Petrovsky, “Will blockchain technology revolutionize excipient supply chain management?” *Journal of Excipients and Food Chemicals*, vol. 7, no. 3, p. 910, 2016.
- [8] V. K. Manupati, T. Schoenherr, M. Ramkumar, S. M. Wagner, S. K. Pabba, and R. Inder Raj Singh, “A blockchain-based approach for a multi-echelon sustainable supply chain,” *International Journal of Production Research*, pp. 1–20, 2019.
- [9] M. Dobrovnik, D. Herold, E. Fürst, and S. Kummer, “Blockchain for and in logistics: What to adopt and where to start,” *Logistics*, vol. 2, no. 3, p. 18, 2018.
- [10] M. Iansiti and K. R. Lakhani, “The truth about blockchain,” *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.
- [11] F. Tian, “An agri-food supply chain traceability system for china based on rfid & blockchain technology,” in *2016 13th international conference on service systems and service management (ICSSSM)*. IEEE, 2016, pp. 1–6.
- [12] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

- [13] M. El Maouchi, O. Ersoy, Z. Erkin *et al.*, “Trade: A transparent, decentralized traceability system for the supply chain,” in *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.
- [14] A. Litke, D. Anagnostopoulos, and T. Varvarigou, “Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment,” *Logistics*, vol. 3, no. 1, p. 5, 2019.
- [15] H. M. Kim and M. Laskowski, “Toward an ontology-driven blockchain design for supply-chain provenance,” *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.
- [16] “Maersk and ibm introduce tradelens blockchain shipping solution, retrieved from newsroom.ibm.com/2018-08-09-maersk-and-ibm-introduce-tradelens-blockchain-shipping-solution,” Aug 2018. [Online]. Available: <https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution>
- [17] “Tradelens solution brief edition two,” *TradeLens Solution Brief Edition Two*, vol. 2, p. 1–11, 2018.
- [18] “What is real-time data? - definition from techopedia.” [Online]. Available: <https://www.techopedia.com/definition/31256/real-time-data>
- [19] D. Massessi, “Blockchain public / private key cryptography in a nutshell,” October 2018. [Online]. Available: <https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c>
- [20] R. Cole, M. Stevenson, and J. Aitken, “Blockchain technology: implications for operations and supply chain management,” *Supply Chain Management: An International Journal*, vol. 24, no. 4, pp. 469–483, 2019.
- [21] M. J. Epstein and K. Yuthas, “Conflict minerals: Managing an emerging supply-chain problem,” *Environmental Quality Management*, vol. 21, no. 2, pp. 13–25, 2011.
- [22] “The kimberley process (kp),” Nov 1970. [Online]. Available: <https://www.kimberleyprocess.com/>
- [23] P. Helo and Y. Hao, “Blockchains in operations and supply chains: A model and reference implementation,” *Computers & Industrial Engineering*, vol. 136, pp. 242–251, 2019.
- [24] N. Kshetri, “1 blockchain’s roles in meeting key supply chain management objectives,” *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.
- [25] K. Wüst and A. Gervais, “Do you need a blockchain?” in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 2018, pp. 45–54.
- [26] P. Brody, “How blockchain is revolutionizing supply chain management,” *Digitalist Magazine*, pp. 1–7, 2017.
- [27] J. Zhang, “Deploying blockchain technology in the supply chain,” in *Blockchain and Distributed Ledger Technology (DLT)*. IntechOpen, 2019.

- [28] M. M. Helms, L. P. Ettkin, and S. Chapman, "Supply chain forecasting—collaborative forecasting supports supply chain management," *Business Process Management Journal*, vol. 6, no. 5, pp. 392–407, 2000.
- [29] C. Bhardwaj, "Blockchain in supply chain: Is it a match made in heaven?" Nov 2019. [Online]. Available: <https://appinventiv.com/blog/blockchain-in-supply-chain/>
- [30] R. O'Byrne, "The supply chain industry looks set to embrace blockchain's potential to improve processes and trace products to their origins." January 2019. [Online]. Available: <https://www.logisticsbureau.com/how-blockchain-can-transform-the-supply-chain/>
- [31] P.-Y. Chang, M.-S. Hwang, and C.-C. Yang, "A blockchain-based traceable certification system," in *International Conference on Security with Intelligent Computing and Big-data Services*. Springer, 2017, pp. 363–369.
- [32] A. Walker, "Blockchain and the supply chain," Oct 2019. [Online]. Available: <https://www.supplychaindigital.com/supply-chain-management/blockchain-and-supply-chain>
- [33] E. Hofmann, U. M. Strewe, and N. Bosia, *Supply chain finance and blockchain technology: the case of reverse securitisation*. Springer, 2017.
- [34] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, no. 6-10, p. 71, 2016.
- [35] C. Sillaber and B. Waihl, "Life cycle of smart contracts in blockchain ecosystems," *Datenschutz und Datensicherheit-DuD*, vol. 41, no. 8, pp. 497–500, 2017.
- [36] W.-M. Lee, "Using the web3. js apis," in *Beginning Ethereum Smart Contracts Programming*. Springer, 2019, pp. 169–198.
- [37] "Ganache: Overview: Documentation," 2019. [Online]. Available: <https://www.trufflesuite.com/docs/ganache/overview>
- [38] "Ethereum ide," 2019. [Online]. Available: <https://remix.ethereum.org/>
- [39] "Ethereum," Dec 2019. [Online]. Available: <https://en.wikipedia.org/wiki/Ethereum>
- [40] C. S. Wright, "Bitcoin: A peer-to-peer electronic cash system," *Available at SSRN 3440802*, 2008.
- [41] R. Libfeld, "What is symmetric key cryptography?: Security wiki," 2019. [Online]. Available: <https://doubleoctopus.com/security-wiki/encryption-and-cryptography/symmetric-key-cryptography>
- [42] Blockgenic, "Asymmetric cryptography in blockchains," Nov 2018. [Online]. Available: <https://hackernoon.com/asymmetric-cryptography-in-blockchains-d1a4c1654a71>
- [43] "Bitcoin energy consumption index," 2019. [Online]. Available: <https://digiconomist.net/bitcoin-energy-consumption>

- [44] R. Khaitan, “Blockchain: One truth across networks for supply chain,” Jul 2017. [Online]. Available: <https://www.ibm.com/blogs/watson-customer-engagement/2017/04/11/blockchain-supply-chain/>
- [45] S. Jangirala, A. K. Das, and A. V. Vasilakos, “Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5g mobile edge computing environment,” *IEEE Transactions on Industrial Informatics*, 2019.