University of Zurich[UZH]

A Survey on Blockchain and IoT Based Implementations for Supply Chain Management

Tanbir Mann
Zurich, Switzerland
Student ID: 16-744-807

Supervisor: Sina Rafati
Date of Submission: September 7, 2018

University of Zurich
Department of Informatics (IFI)
Binzmï¿½hlestrasse 14, CH-8050 Zï¿½rich, Switzerland

ifi

IS REPORT – Communication Systems Group, Prof. Dr. Burkhard Stiller

Independent Study Report
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmï¿½hlestrasse 14, CH-8050 Zï¿½rich, Switzerland
URL: http://www.csg.uzh.ch/

Abstract

In recent times food safety peaked upswings of academic and commercial concerns. In the area of supply chain, a lot of rising technologies along with the rapid growth of internet of things (IoT) have been applied in traceability systems. Yet, majority of such technologies are monitored centrally which has vulnerabilities regarding trust, fraud, corruption, data integrity, and false information. Whereas today's new technology BlockChain (BC), a decentralized information technology brings a whole new approach in communication systems world. As the technology is in its early phase, it has some built-in deficiencies, in which scalability is most elementary one. In this paper we will study all the related work that has been implemented in order to find a feasible solution for supply chain management (SCM) by leveraging BC and IoT technologies together. Furthermore we will study the relative measures playing crucial role in order to append such technologies in supply chain systems e.g., choosing a suitable architecture, efficient consensus mechanism, cryptographic algorithms, throughput maintenance, and dealing with privacy, security and scalability challenges. After studying the measures and work in this field, one would be able to consider every aspect which may turn out to be critical for an ideal system in SCM.

Contents

Chapter 1

Introduction and Motivation

Demand for transparency is increasing, surprisingly we know little about most of the products we use in our day to day life [1]. Products travel frequently through huge network of stakeholders before reaching the end consumer which includes retailers, distributors, transporters, storage facilities, and suppliers that participate in design, production, delivery, and sales etc., still in almost all the cases these journeys remain an unobserved attribute of our possession.

Consumers as well the government's demands for more transparency from brands, manufacturers, and producers throughout in the supply chain is increasing. Governments tend to provide more transparency in goods and their manufacturing details. "The 2016 Food Revolution Study, which surveyed 1,522 consumers to discover how they make food choices, shop and what they expect from brands in terms of product information, reveals that brands that to meet customer expectations for product information and deliver that information instantly develop a new dynamic of convenience, trust, and long-term value" [31]. This leads to an increase demand to producers in order to provide complete information about the product and its origin.

For human beings the food and its life cycle has always been important and with the passing time, food choices have become more crucial. With increasing demand in the twenty first century, many production process of foods have encountered enormous changes, the usage of Enterprise Resource Planning (ERP) systems has revolutionized the whole supply chain management systems [30].

Nowadays, we are blessed with most enthralling and amazing technologies from the field of computer science. Internet of Things (IoT) is one of the most significant disruptive technologies of this century expanding at a fast pace. IoT provides a platform for devices e.g., smartphones, sensors, and wearables to connect to each other devices via Internet to share data. The devices in IoT can be controlled remotely to perform the desired functionality. The information sharing among the devices then takes place through the network which employs the standard protocols of communication. But this technology comes with various security and privacy challenges due to its massive size [2]. The deficiency of fundamental security safeguards in many of the first generation IoT devices has aggravated the privacy concerns related to IoT products. Many secure network protocol

like IPsec and TLS are used to provide authentication and privacy, but these methods are computationally expensive which limits their versatility with resource-limited IoT devices [9]. In order to have control over the access of sensitive information , a distributed capability based access control method is proposed in [10], but this method also compromises the user privacy due to its excessive delays and overheads. Hence, there is a need to have for an approach to share privacy-aware IoT data without tempering user privacy.

Blockchain technology has attracted huge attention from the researchers of Computer Science in the past decade. Blockchain (BC) was introduced in 2008, as a platform for secure, anonymous transactions, using a decentralized network of computers or devices. It's first application was cryptocurrency Bitcoin, which assures anonymity, by allowing users to transfer tokens over a peer-to-peer (P2P) network without any need of centralized authority [5]. Blockchain maintain a distributed ledger in the form of transactions and these transactions are shared among all the nodes in the network. New transactions are embedded in the network, once they are verified and confirmed by the all relative nodes in the system, thus abolishing the need for central authority. BC has many features which includes distributed structure, immutability and security and privacy [3]. Blockchain also provides solution to most of the security and privacy challenges faced by IoT [4], specifically data authentication, Integrity, authorization and privacy. BC provides a trusted platform to its user to share their data/information without bothering about the tampering of the data or unauthorized access.

From the past decades, the consumers trust in the food industry is fading after many food safety risk scandals e.g., mad cow disease and genetically modified food in China [6] and âhorsemeat scandalâ in 2013 in Europe [7]. These scandals can leave a deep impact on development of countries economy and can incurs a great threat to the stability of the society. As an outcome, consumers are more concerned about the safety and quality of food, which has drawn quite an attention from academic and industrial areas. In response to such issues many IoT technologies were used such as RFID and wireless sensors based network in supply chain for traceability and visibility. As the IoT technology is governed by centralised based systems which develops the issues of trust and integrity of data and valuable information can be tempered by bribing the administration. To deal with such issues it is required to come up with the solutions where the data can be transferred without any centralised control keeping the key security, privacy, confidentiality issues in mind. Whereas, Blockchain provides solutions to such issues but we cannot implement BC technology directly with IoT as it has key scalability and high resource consumption issues [8], which ultimately rises the need for a lightweight blockchain which can be used for IoT considering the key scalability issues.

Therefore, combining BC and IoT together could be an efficient solution for traceability in supply chain management. By making use of IoT devices such as sensors for information gathering and using BC for storing the gathered information securely without worrying about data integrity. There are many related work in this field that has showed some immense results in tracing the products lifecycle at each phase of its life (starting from producer to its end consumer). These works are described in following section.

The main goal of this paper is to investigate and compare the most efficient proposed BCs, especially the approaches that has been integrated with IoT to increase the transparency

of supply chain management (SCM) systems. Result of such a comparative analysis will lead to proposing an ideally and feasibly best BC IoT based approach with the goal of enabling an automated and transparent supply chain management and monitoring system.

Chapter 2

Related Work

In the literature there are very few instances of application of blockchain with IoT for supply chain management systems. One application of blockchain based distributed cloud/fog platform for IoT Supply Chain Management (SCM) is proposed in [11], the researchers aims to provide high quality of products and processes with use of advanced, state-of-the art ICT technologies and thus contribute to provide SCM far better than the current standard certification methods. The end goal is to provide better performing value chains by proposing new food-on-demand business model, based on Quality of Experience (QoE) food metrics, bridging the gap between subjective experience and objective metrics based on quality standards. The research focused on the key steps of the food chain, addressing the emergent needs of various stakeholders involved in the project. The system is applied on a typical food product - 'grape' as a case study. This study is implemented on real world smart environment by making the use of sensors in overall food supply chain system to collect data and integrate it in a cloud infrastructure.

In [12] author has represented AgriBlockIoT which is fully decentralized blockchain based traceability solution for SCM to integrate IoT devices producing and consuming digital data along the chain. They defined a use case from-farm-to-fork using AgriblockIoT, then this use case is implemented to achieve traceability using two different blockchain i.e,. Ethereum and Hyperledger Sawtooth. The proposed system guarantees transparency and traceability of the products by directly getting all the relevant data from the IoT devices along the entire supply chain and then storing it to the latent blockchain directly.

The author in [13], analyzed and scrutinized the possible requirements and functionalities of supply chain integration. They implemented common solutions, technology and standards for integrating business processes within a large supply chain. The study aimed to establish how Business-to-business Digital Supply Chain (DSC) integration can be hastened and how blockchain technology support that integration. The analysis showed that many-to-many integration models like private cloud (ERP/Hub companies) and public cloud (Intermediate/blockchain and ERP/SME) are most effective integration models. Blockchain offered data security and cost effective transmission of transactions in peer-to-peer network which simplifies business-to-business (B2B) integration and micro level IoT integration. The study funds blockchain ledger , security and smart contract platforms and software connectors proposes apparatus to compose a cost effective extensible

DSC network. Trade finance is used for occasionally providing financing services to DSC network and BC which later on came out to be suitable solution for such integration.

In [14], the author investigated the pros and cons of using RFID and blockchain technology in building the agri-food supply chain traceability system and demonstrated the building process of SCM system. They inaugurated an agri-food supply chain traceability system based on RFID and blockchain together with Wireless Sensing Network (WSN), Government Satellite Network (GSN), Geographic Information System (GIS) and computer data processing technology for helping Chinese agri-food markets to strengthen the food quality and its safety. The system encloses the entire processes involved from data collection, information management of every link in the chain which registers the monitoring, tracking and traceability management from producer to end consumer and effectively guarantees the quality and safety of the products.

The author in [15] , presents a methodology to allow traceability along the processes to provide end user with sufficient knowledge of the product. This methodology is used by integrating Blockchain technology in the food supply chain and implemented its application in the organic coffee industry in the Colombian market. The author named his work a Cold chain which assures the sterile safety of the products with respect to the ClodChain throughout the entire processes involved from storage to producer, transport, distributor and the end consumer. For quality assurance, they took the compliance certification attests that unprocessed food or agricultural product complies with certain attribute concerning the product packaging or origin and as an outcome the authors methodology turned out perfectly suitable for integration of blockchain in food supply chain industry.

The work in [16] represents a Use-case of Blockchain in the Pharma Supply-Chain, they presented modum.io as the startup company that used IoT (Internet of Things) sensor devices using blockchain technology for data immutability and publically accessible temperature records reducing the operational cost in pharmaceutical supply-chain. The sensor devices examines the temperature of each package of medicine during the shipment for comprehensive affirmation of GDP regulations. Smart contracts were used to assess the temperature information against the product attributes. In the study Ethereum blockchain is used for temperature data verification along with Ethereum Virtual Machine (EVM) which verifies data through smart contracts. As an outcome, the study took offline features (store data internally until it can be uploaded) and higher decoupling of Ethereum blockchain into consideration so that temperature reports can be given at later times as well.

The work in [17] also represents the use case of BC to solve agricultural food supply chain problem of traceability putting forward the application of BC in information security of food supply chain in Chinese market. They compared traditional supply chain system with their implemented system. PEST, an analytical model which evaluated the macro-environment location of the industry , is used to analyze and reveal the application of BC in food supply chain. PEST comprises of four factors Political , Economic , Society and Technical. Based on these factors the study concluded that blockchain is a well suited technology for the governments to maintain traceability and security and can help manufacturers to record the transactions with full authenticity.

In [18] a real-time traceability system is fvamed based on HACCP (Hazard Analysis and Critical Control Point), BC and IoT, for food supply chain. This system serves as platform for accessing information across all the supply chain members with transparency, immutability, security, reliability, and neutrality. They also addressed the scalability of blockchain technology when handling huge data within a business environment. BigchainDB is introduced which keeps three key characteristics of the blockchain (decentralized control, immutability, creation and movement of digital assets) and three characteristics of distributed databases (high throughput, low latency and high capacity). RFID technology is used as a unique digital cryptography identifier for connecting physical items to their virtual identity in the system. The data in the system is stored in BigchainDB which can be accessed by any user, it also has some set of rules in it written in coded language to monitor data sharing and interaction of the users with the system. The system improves the transparency and safety of supply chain building consumers confidence in the food industry.

In [19], the author proposed a tiered Lightweight Scalable Blockchain (LSB) escalated for IoT requirements. They examined LSB in a smart home setting with decentralized overlay network. The smart home setting is managed centrally by Local Block Manger (LBM) which establishes shared keys for communication and perform the processing of each incoming and outgoing requests. Whereas Overlay network is completely decentralized where high resource devices collectively govern a public BC ensuring end-to-end privacy and security. This overlay is organized in the form of 4 tiered clusters (including smart homes, mobile devices, service provider (SP) servers and cloud storage) and each cluster maintains its Cluster Head (CH), this collection of cluster heads is responsible for managing the public BC. LSB also incorporates few optimizations which includes a lightweight consensus along with distributed trust and throughput management. LSB has an IoT compatible (in terms of resource consumption) consensus algorithm which removes the need for solving any puzzle in order to append a block in the blockchain. Distributed trust algorithm steadily decreases the processing time as OBMs develop trust in each other. The outcome of the study proved LSB as a robust approach against certain security attacks. Comprehensive simulation results showed that the LSB decreases packet overhead and delay enhancing the scalability of BC in comparison with relevant baseline models. On a general note, LSB ensures high level security and privacy to its users while enforcing marginal overhead.

In [20], the author gives an overview on the use of Blockchain for the IoT, the study provide insights to how to come up with suitable blockchain with respect to the specific needs of IoT so that a compatible Blockchain-based IoT can be developed. It provides the basics of the blockchain (functionalities, blockchain types, and need for BC) and its relevant BIoT applications along with its impact on traditional cloud-centered IoT applications. It gives us thorough knowledge of current challenges for BIoT applications (privacy, security, energy efficiency, throughput and latency , blockchain size, bandwidth and infrastructure) and other relevant issues like Adoption rate, usability , versioning and forks and mining boycott etc,. Recommendations to future BIoT researchers provided to tackle issues that have to be considered before deployment of any BIoT applications. The study review examined state-of-art of BC technology and proposed several schemes for BIoT applications in the field of healthcare, logistics , smart cities or energy management.

In [21], the author address the secure data transmission through Blockchain technology, [22] introduces the use of cloud and fog as hosting platform for blockchain, after analysing the performance of cloud and fog they concluded that the network latency is the dominant factor for implementing such platforms with BC, hence the fog outperformed the cloud. Therefore, there are also several works that talks about blockchain based security solutions for IoT [23]. As blockchain provides anonymous transaction over per-to-peer network using decentralized distributed ledger, the study [24] removes the trust of central authority for validating the transactions with cryptographic proofs. They represented a proof-of-concept method for field devices to store and share data using a distributed ledger which is built on the IOTA tangle. Whereas in [25], Edge computing is incorporated to handle data storage along with certificateless cryptography. The main aim of the study was to eliminate traditional centralized approaches by leveraging blockchain miners to implement transaction verifications with the cooperation of certificateless cryptography.

The comparison of all the above related work is done in the underlined section, certain measures are compared to find out an appropriate combination of BC with IoT in SCM system.

Chapter 3

Relative Measures

3.1 Architecture

The major concern to be considered when we think of an architecture for SCM using BC and IoT technologies is its adaptiveness to the amount of traffic that may be generated by the IoT applications and support for different IoT devices which perhaps required for data collection in SCM. In [18], a food supply chain model with HACCP is used which control for various hazard for supply chain such as safety risk associated with processing environment, field practices, site equipment, and warehouse management. The model is based on blockchain and IoT dividing the chain into 5 links Production, Processing, Warehousing, Distribution, Retail. BigchainDB is used which holds the key benefits of distributed DBs and blockchain for data storage and management. RFID, WSN , GPS were used to collect and transfer data. The data in the system is open to any user, whereas the system is governed by set of rules defining users interaction with the system and sharing the data among users held in the form of smart contracts.

A Real-world smart environment is used In [11]. The architecture of the SCM comprises of 5 modules i.e., Farm , Transport and Packaging, Pilots, Fog Node (blockchain based distributed network) and BC based distributed cloud. Pilot module holds instruments for customer social behaviour and satisfaction from the product. All modules exhibits quality measures most importantly Quality of Experience (QoE) based on customers quality perception. Communication among different modules(producers, packaging, transport and distribution) and consumers is done through IoT/Fog/Edge/Cloud. Mobile sensing technologies (sensors) is used to collect and transfer data and are integrated within the cloud infrastructure. Data processing is done in parts at network edge starting from cloud to end point continuum whereas Fog and Mobile Edge Computing (FMEC) is used for addressing latency, limited device processing, storage, bandwidth, and cost. Security and Privacy concerns are also covered with the help of FMEC via BC. Cloud based technologies such as Docker and Kubernetes are used to serve all the needs of the system such as infrastructure required for data gathering and to perform computations.

In [12]AgriBLockIoT a layered architecture is employed based on the BC and IoT to achieve transparency, auditability and immutability to save the data records evidently in

a trust- less environment. Modern edge devices (e.g., gateways, mini-PC) are used as full nodes of the layered blockchain implementation which helps in expanding the resistance, decentralization, security and trust of the whole network. The proposed architecture has 3 main modules:

1. **API** : a REST Application Programming Interface which reveals the potential of AgriBlockIoT to other applications, with a high level of abstraction, the proposed API also grants an easy integration with existing software systems.

2. **Controller** : The controller converts high level functional calls into low-level calls for the blockchain layer, and inverse is also true. Specifically querying and converting the data records stored in the blockchain, into high-level information for the upper layer.

3. **Blockchain**: It is the main component of the system which contain all the business logic. Smart contracts are used to implement these business logics and serves as a barrier to access data from BC.

The system exhibit bottom up approach for defining the high level functionality of the AgriblockIoT. Every participants involved in the setting (e.g., producer, farmer) has to be the registered users of the blockchain and have to update the BC consistently with every passing phase (e.g, production, processing, warehousing). Smart Contracts check the liability of the updated information at every stage and can fire, creating records whenever anomalies are detected [13].

In [13], a Digital Business Ecosystem(DBE) framework is used based on the Zachman Enterprise Architecture. The BC design principles used in DBE framework are Ownership and Security, Network Integrity, Distributed power, Inclusion, Values as Incentives, and Privacy and four functionalities are summarised within DBE framework: 1) Modelling the transaction data; 2) Data processing (done by ledger or smart contract); 3) Peer-to-Peer networks storage 4) Blocks managing by miners. Although the proper architecture and its working is not fully explained but they summarises their study results by stating that blockchain along with smart contracts and software connectors can appear to be a good fit for digital supply chain (DSC) network.

In [19], a Lightweight Scalable Blockchain (LSB) is proposed which consists of two tiers Overlay and Smart home.

1. **Overlay** : The overlay network contain vast number of nodes which are clustered using clustering algorithms. Each cluster choose its cluster head also known as Overlay Block Manager (OBM) which is responsible for managing and process all the incoming and outgoing transactions in the blockchain. Whereas, two types of transactions were used single signature and multisig. The transaction output is set by requester which contains: total number of transactions generated by the requester which have been accepted by the requester, the number of transactions rejected by requestee and the hash of public key (PK) which will be used for its next transaction. The overlay transactions are stored in public BC managed by OBMs.

Whenever OBM receives a transaction , it checks if the requester of the transaction is present in its cluster, then it maintains a key list comprised of requester/requestee PK pair which verifies if the requester is allowed to send transaction to the specific requestee. If it matches than transaction is processed otherwise it is denied.

2. **Smarthome**: It consists of many IoT devices which are managed by local blockchain manager (LBM), LBM centrally manages the local Immutable Ledger (IL) which is similar in structure to blockchain and is responsible for conducting all the local and overlay transactions. It uses generalised Diffie-Hellman key distribution method to generate and distribute shared keys. Each smart home has a local storage repository for storing the data locally. It is assumed that local storage is secure and smart devices are allowed to store data locally (verified by policy header) , LBM then generates a shared key which will be used by the device for its authentication with the local storage.

In [14], Agri-food supply chain traceability system based on RFID and BC is implemented. The agri-food used in this study is of two type: Fruits/Vegetables and Meats. RFID technology is used for the traceability of the food in all the phases starting from data acquisition , circulation in production, warehousing, transportation etc,. Whereas BC is used to for system reliability and authenticity. The building process of such traceability system with BC depends on following links: Production link, Processing link, Warehousing management link, Cold Chain distribution link, Sales link. RFID tags are used to store and transfer the data to the blockchain at each link. For Cold Chain distribution link, vehicle-mounted safety monitoring system is used by setting temperature and humidity sensors in different temperature areas with vehicle-mounted wireless network and computer . This system will allow to transfer the real-time data of agri-food to the BC system. When the temperature and humidity exceed the security standard the vehicle-mounted safety monitoring system immediately raises the alarm. The freshness of the products and transparency of product information can also be guaranteed by RFIDS tags along with BC technology.

The study in [16] is based on the use of BC in pharma supply chain. The modium.io AG is actively involved company which is using blockchain technology for tracking the temperature of the medicines. The Architecture of modium.io AG comprised of 6 components: 1)Ethereum blockchain network: used for temperature verification, data registration in the front end and certification of data is done by smart contract running on Ethereum virtual machine (EVM). 2) Smart contract: used for each new shipment and checks that the temperature required for the shipment is in complains with the GDP requirements programmed in the smart contract. 3) Database: a relational database (postgreSQL) is used to store the raw temperature data and user credentials. 4) Server: it facilitates the communication across the network i.e., among blockchain network and front end users, creating and modifying smart contracts and storing data in database, they used HTTP over JSON. 5) Mobile devices: are used to track and send the records of temperature data to the Server. 6) Sensors: these are thermal sensitive devices having bluetooth technology which is used to send data to the mobile devices.

Concluding the relative architectures used in SCM, a smart setting could be implemented at each phase of supply chain using Overlay and HACCP to gather real time data of

the food items and to control all the information related to the product with the help of various IoT devices.

Architecture Summary				
Related Work	**Systems Used**	**Data Storage**	**IoT Devices**	**Data Transfer**
1	HACCP with BC and IoT	BigChain DB	RFID, WSN, GPS	IoT Devices and Smart Contracts
2	Blockchain-based Distributed Cloud/Fog platform for IoT SCM	Fog and Mobile Edge Computing (FMEC)	RFID and LoraWAN Sensors	IoT/Fog/Edge/ Cloud
3	AgriBlock IoT(API, Controller, Blockchain)	BC(Ethereum / Hyperledger Sawtooth) via Smart Contracts	Sensors, GPS, Smart Tags (QR tags)	Directly to BC by every Actor involved
4	Agri-food Supply Chain traceability system based on RFID and BC	BC	RFID, GPS, WSN	RFID
5	Modium.io AG	Ethereum Blockchain and Relational database (Postgre SQL)	Mobile devices(Smart Phones, Tablets), Sensors	Mobile devices
6	Digital Business Ecosystem (DBE)	-	-	Smart Contracts
7	LSB: Overlay and Smart Home	Smart home's local Storage and BC	Smart Home setting (smart thermostat, laptop, mobile devices etc.,)	LBM and OBM
Proposed Setting	Smart setting at each link of SCM , HACCP for control hazards and Overlay Network	Blockchain or Distributed database like BigChain DB	RFID, GPS , Sensors and Smart tags	Block Managers (BM)

3.2 Consensus Mechanism

Consensus is essential for proper working of a blockchain, it is a mechanism that determines the conditions which need to be accomplished in order to come up with a decision

that an agreement has reached about the validity of the blocks which needs to be appended to the blockchain. Along with traditional consensus approach (PoW), various other consensus mechanisms has been developed such as Proof-of-Stake(PoS), Proof-of-Activity (PoA), Delegated PoS, Practical Byzantine Fault Tolerance(PBFT), Delegated BFT, Sieve etc,. Out of the mentioned mechanisms the most famous and common ones are described below:

1. **PoW**: It is the traditional consensus algorithm which is used in first blockchain (Bitcoin blockchain) , used to confirm transactions and add new blocks to the chain. In this miners (nodes that calculate hash values) compete against each other to complete transaction on the network, the competition is mainly due to the reward system, as the miners who add new blocks to the chain get rewarded 8. Minimum latency of PoW is 10 minutes for solving the cryptographic puzzle which is not a desirable solution for IoT applications [13].

2. **PoS**: This protocol states that a miner can mine or validate the transaction depending on its capacity. It is assumed that the entities that are more involved in the network are less likely to attack the network . Miners in the network have to provide proof consistently that they own specific amount of participation in the network. But this mechanism resulted to be unfair, as the user holding most of the resources in the network was able to rule the whole chain. Later on this problem was solved using different approaches like Peercoin Consensus [8], [20].

3. **PBFT**: It is created to solve the Byzantine General Problem. This algorithm is based on the fact that one third of the nodes in the network are malicious and for each block to be added to the chain, a leader must be selected who will monitor the ordering of transactions. Such selection must be acknowledged by 2/3 of the known nodes in the network [8], [20].

4. **Delegate PoS**: This mechanism is similar to PoS but instead the stakeholders choose delegates for creating new blocks and validating the existing blocks. The performance rate in this algorithm is high due to less nodes are used to reach a consensus [8].

5. **Sieve**: The main goal of this mechanism is to utilize the available computational power of the network which is done by dividing the available power into different sub-committees. These subcommittees run their own consensus internally in order to come up with a common solution [8].

PoS requires less computational power than PoW therefore consumes less energy [20]. Time based consensus algorithm instead of resource consuming (PoW / PoS) is used in LSB [19]. This consensus algorithm ensures that a block generator is selected randomly among the nodes that can only generate certain number of blocks. To ensure that the block generator is selected randomly , each OBM must wait for certain time before the block is generated, removing the possibility of generating duplicate blocks. For example, if an OBM receives a block which is already generated by other OBM, that certain block can be discarded as it already exists in the chain. The newly generated block is broadcasted

to all the overlay nodes to be appended into the BC. The default value for consensus period is 10 minutes as in bitcoin.

The performance of PoW in LSB is low as PoW incurs significant delays increasing the processing time more than 29.22 minutes which is not a best solution for IoT. Also in [20] author proposed that by making the use of private blockchains with controlled user access the threat of Sybil attack is reduced to greater extend and therefore reducing the use of costly mining algorithms and economic incentives. PoS and BFT both outperform PoW in terms of energy consumption. Both are light in comparison with PoW as PoS requires user to show interest in specific service by allocating certain amount of memory or disk [20]. Since we are able to compare only several mechanisms, we can say that PoS/Delegate PoS is a better solution for IoT as it consumes less power and energy.

3.3 Cryptographic Algorithms

Cryptography is a method and study of techniques used for secure communication. Traditionally it is used for secure communication in various fields like military. From the past few decades it has been revolutionized from confidentiality concerns to techniques for electronic commerce, chip based payment cards, password management and digital currencies etc. There are two types of cryptosystems: Symmetric and Asymmetric. In symmetric cryptography , two parties agree on a same secret key which is also know as private key and use this key for encryption and decryption. On the other hand, Asymmetric cryptography also known as Public key encryption use two different keys: public key for encryption and private key for decryption [20].

Public key encryption serves as a main key for providing security and privacy in BC [20], in order to come up with right cryptography scheme several factors like memory requirement, computational load and energy consumption should be considered. RSA and ECDHE are most common public key based cipher suites. RSA has 768-bit and 1024-bit key size which is very small to provide security in IoT networks whereas the minimum size required for security is 2048-bit. On the other hand ECC (Elliptical Curve Cryptography) outperformed RSA in terms of energy consumption and speed [20].

Along with cryptography algorithms, hash functions has to be secure and should not generate collisions. SHA 256 and SHA 256d and Scrypt are the most famous hash functions. In [19], the transactions generated by overlay are secured by asymmetric encryption , digital signatures and cryptographic hash function SHA 256. Therefore work in the above cited papers shows that asymmetric encryption along with cryptographic hash function SHA 256 suits best for blockchain.

3.4 Throughput

Deployment of IoT with BC requires BC network to be capable of handling a large amount of transactions per unit time. Traditionally, Bitcoin's blockchain can handle only upto

7 transactions per second, but the performance of its consensus algorithm Proof-of-work (PoW) has poor scalability which is no longer usefu, specifically for modern cryptocurrency platforms such as Ethereum and for IoT networks [27]. Whereas VISA network (VisaNet) can handle upto 24,000 transactions per second. In terms of throughput, VISA has much more performance capabilities than bitcoin BC [20].

There are many different approaches used to maintain the throughput of blockchain e,g., BigchainDB is used, which holds the main benefits of distributed db and BC. It contain three main characteristics of the BC. Decentralization is achieved by the nodes via voting process which refers to p2p network as in traditional BC. Immutability is achieved by the sequential blocks holding ordered sequence of transactions. Creation and movement of digital assets is done through asset-issuance and asset- transfer permissions or key of the asset. This phenomenon reduces various risks like data tampering and single point of failure. The throughput is increased by increasing the number of nodes [18].

A distributed throughput management (DTM) mechanism is used to monitor the utilization (α) of the network for LSB. This mechanism helps to make the adjustments accordingly to minimum and maximum utilization required for the specific network by running an algorithm to ensure that α remains in an acceptable range. The utilization is computed as the ratio of number of transactions generated to the number of transactions that are added to the block in each consensus period. The calculations are done through an equation as shown in equation (3.1) [19]. This equation suggests that there are only two ways to adjust α, either by changing the consensus period or by changing the number of block mangers (M). If α exceeds α(max) then new value of consensus period is computed, DTM checks if the consensus period can be reduced if no, calculations to find the number of M required are done according to the equation, same procedure is followed if α is below α (min) in order to maintain the throughput of the system. But this phenomenon is only helpful to improve the throughput in the networks like LSB which could be helpful in accordance with the proposed setting.

$$\alpha = \frac{N \star R \star Consensus - period}{T\_max \star M} \tag{3.1}$$

3.5 Latency

Latency is defined as the the amount of time it takes for a transaction to be processed and finally get accepted by the network (and how the confidence of acceptance increases over time). It is well known fact that processing of blocks or appending a new block in the blockchain takes time, and the amount of time it takes for a block to finally join the chain is known as its latency rate. In Bitcoin BC, a P2P Electronic Cash System, follows Poissons distribution with a 10-minute mean time for block creation [20]. It is also important to note that such latency of 10 minutes for processing a transaction cannot suite

IoT due to its massive size and thousands of transactions happening at the same time. The latency rate is even high in bitcoin if it is required to solve big problems like double spend problem, it is possible that the next transaction may have to wait for an hour as five top six blocks are needed to be appended to the chain before the transaction is confirmed. Whereas, for VISA, the latency for block creation requires only few seconds[20].

In [16] , Ethereum blockchain is utilized to verify the temperature of the medicines every 10 minutes whereas in [13], PoW is used for adding new transactions into the system which resulted into latency of 10min. In [12] AgriBlockIoT is implemented on two different BCs (Ethereum and Hyperledger based Sawtooth) and the performance of AgriBlockIoT is compared on both the BCs in terms of latency, Ethereum took 16.55 (sec) and Sawtooth took 0.021 (sec) for processing new transactions into the chain. Sawtooth outperformed Ethereum not only in latency rate but also for CPU load and network transactions.

From the above works it could be considered that instead of applying different consensus mechanisms directly in the system, various approaches like AgriBlockIoT along with suitable BC can be helpful for better performance. Thus, consensus latency highly depends on its consensus algorithm, the more time it takes to process the transaction, longer the block has to wait ultimately increasing the latency. There are many consensus mechanisms such as PoW, PoS, PoA which we will discuss in the coming section and will try to come up with better and more appropriate algorithms for IoT.

3.6 Security

Security can be categorized into 3 parts which should be fulfilled for assuring the security of a system as discussed in [19] [20]:

1. **Confidentiality**: The term confidentiality is implies, protection of sensitive information from an unauthorized access. It can be compromised by the transaction data which can be addressed using various privacy enhancement techniques. The best practice for sustaining confidentiality on an individual level is maintenance of private keys. CONIKS a key management system can be used for maintaining the confidentiality. Certificates also play crucial role in maintaining the security of the system e.g., SSL certificates which can be validated by different frameworks such as google used Merkle hash trees for validating the certificates [20]. In LSB, confidentiality is maintained through Encryption (symmetric and asymmetric) for all the transactions.

2. **Integrity**: It assures that the data is not tempered or removed by any unauthorized third party and if data alteration is done then by some third party than system should be able to delete the changes and retrieve the previous data. As the blockchain is designed in such a way that it is impossible to alter information in the system. This requirement is inbuilt as third-party dependencies are removed [20]. In LSB, each transaction include the hash of all the other fields that are held in the transaction ensuring the integrity of the system [19].

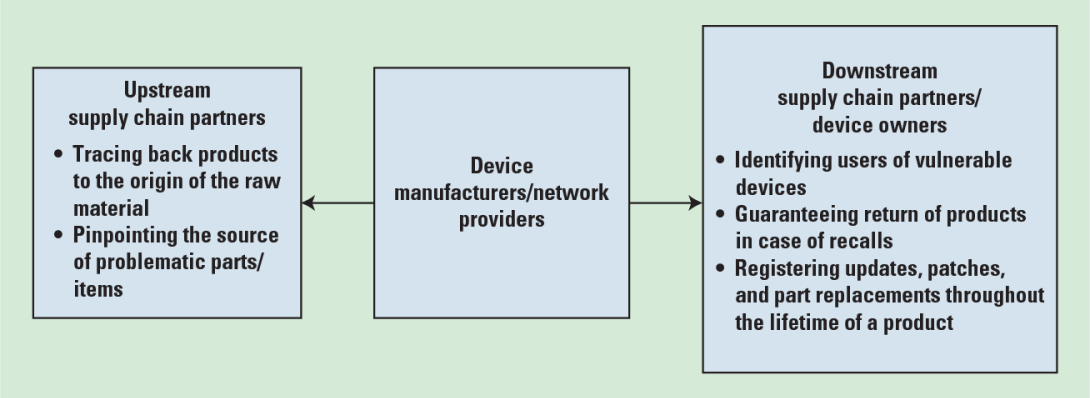

Figure 3.1: Blockchain's role in improving overall security in supply chain networks [29].

3. **Availability**: As the name implies, data should be available whenever needed. In contracts to traditional centralized approach (cloud storage) , when one node fails, the entire system breaks down, whereas Blockchain provides the availability consistently. It is only possible to lose access to data when the system is under 51% attack , which is very rare case [20]. In [19], availability of the data is accomplished through two steps: 1) By making use of LBM for processing all the incoming transactions and control access to smart devices, this helps in guarding the system from malicious requests. 2) OBM transfer the transaction further if and only if the key contained in the transaction matches the list of keys in its keylist ensuring only authorized transaction to move further in the system.

Authentication and Non-repudiation can also be used for ensuring the security [19]. For example in LSB, authentication in smart home is maintained by creating shared key among two communicating devices, LBM is responsible for shared key generation. In Overlay, transactions are chained to genesis transaction and a node is authenticated only if it has private key to the corresponding public key of that specific transaction stored in blockchain whereas Non-repudiation is achieved by transaction generator signing all the overlay transactions.

Whereas in [29], the work illustrated that with blockchain it is possible to achieve immutability at different points of transactions which includes understanding the crucial vulnerabilities in the upstream supply chain as shown in figure 3.1."Blockchain has a capability of easily dealing with crisis situations for example product recall due to security endangeredness" [29].

3.7 Privacy

Privacy is one of the biggest challenges in BC due to its transparent transactions and its even more to maintain privacy in IoT Environments as there is a possibility that IoT devices can reveal private information that could be stored in BC, whose privacy requirements vary from country-to-country [20]. BC is used in IoT for data storage and

access. IoT provides a leverage to a user to access data from any place and blockchain helps in ensuring the privacy of the data and secure access to it. This is done by creating an account in the blockchain where user setup the permissions and require controls for his account [8]. Whereas all the users in the blockchain are identified by their public key or its hash which guarantees no anonymity as the transactions are shared in the entire network of BC. In comparison to traditional approach, where transactions were known by the two communicating parties and a third party who was controlling the transaction centrally (eg., banks, institutes or some government organizations), it is difficult to build such privacy in BC. As BC is an open platform where any user of the network can have access to any information which is available in the same network. In such cases, private blockchains can be used who asks for permissions to have access to data from BC [20].

There are various means to maintain privacy in blockchains, one such approach could be through Smart Contracts e.g., in [18] the privacy of the producer is maintained through digital contracts (Smart contracts) which were stored in the BigchainDB and access is granted to the nodes who can fulfill the contracts requirements. This contract comes into play whenever one user transfer the product to other user (during different phases of the product's life cycle), as both have to sign it for authentication. Public key is used as a User Id and private key is used to authenticate a user to have access to certain data or to interact with the system. The system provides the producers to keep their identities private by passing a digital contract, they can transfer all the important/relevant data which might be useful to the consumer.

Other means to ensure Privacy is via Permissioned blockchain which help to overcome identity certification problem in IoT. It enables identity provider for authorizing identities as well as gives the power to block them for securing and managing multiple IoT nodes. Multi Chains can also be used for deploying private blockchains that guarantees that only the chosen party will monitor the activities. Mixing techniques can also be used to enhance privacy but they are prone to statistical disclosure attack. Zero knowledge proving techniques also enhance the privacy, it is a method that tell the counterparty that user knows some information without actually revealing any information. CryptoNote protocol can also be used as it uses ring signatures and only the legitimate user can have access to the information or the entities which holds the private keys of the transaction [20].

LSB uses anonymity and user control to protect the privacy of the user in the overlay, smart home and the cloud storage by using changeable public keys. In smart home, home owner can have control over the data and can protects its privacy by enforcing his own privacy policies in the LBM. To protect against de-anonymization of devices , overlay uses different credits to store the data of each of its devices which prevents the cloud to identify different devices of the same overlay node [19].

3.8 Scalability

The very first design of cryptocurrencies was not developed for widespread use, it was able to manage the system as the number of transactions were less. But with the passing time,

the system started to expand resulting in more number of transactions than usual which hosted number of issues. One of those issues is scalability. Comparing the transaction time of different BC systems like Ethereum which can have 20 transactions per second with paypall which can manage 193 transactions per second and VISA manages 1667 transactions per second whereas Bitcoin is only capable of implementing 7 transactions per second. Therefore, scalability plays key role for improving the number of transactions [28]. Main scalability problems can be categorized as:

1. Time taken to put a transaction in the block.
2. Time taken to reach a consensus.

Following are the approaches taken by some systems to overcome scalability problems:

1. **Segwit**: It is typically used by Bitcoin, and is a feature of the sidechain which will work in concurrence to the main blockchain. In this system, all the signature data is moved from main chain to side chain and is arranged in a Markel tree form. The Markel tree root along with coinbase transaction was included in the block which increased the overall block size. The signature data, moved to the side chain contains the name of the transaction aka and the hash of the input and output value which makes it bulky in size. In fact, 65% of the data taken up by the transaction is because of its signature which is useful only for the initial verification process and is not required later on at all [28].
2. **Using Proof-of-Stake** : According to [28], usage of PoS will increase the processing speed of the chain as it is easier to monitor who has the most stake than checking the hashing power (as in PoW). It simplifies the implementation of sharding, also miners in PoS can only earn via transaction fees incentivizing them to increase the block in order to get more transactions.
3. **Sharding**: It is used by Ethereum and Zilliqa. This approach has helped Ethereum to solve its biggest problem where ever node has to download and save the whole blockchain whereas through Sharding a transaction can be split up into different shards and is broadcast to the whole network. The nodes works on individual shards side-by-side, reducing the overall time taken to process a transaction and improving the speed of transaction verification. The main challenge in implementing this approach is that it requires a mechanism to know which node implements which shard and it also require PoS to be implemented first in order to simplify the sharding process in the system. Other biggest challenge is that the nodes work on trustless system, meaning node A doesn't trust node B and they should both come to a consensus regardless of that trust. For example, if one particular transaction is broken up into shards and distributed to node A and node B, node A will have to come up with some sort of proof mechanism that they have finished work on their part of the shard [28].
4. **Off- Chain State Channels**: This approach eliminates the need of miners to validate a transaction, being a two-way communication channel among the users,

it enables them to administer the transactions by themselves, which normally takes place on the BC and off the BC. There are three main requirements to be fulfilled in order to run this approach efficiently [28].

(a) A segment of the BC is required to be locked through multi-signatures or via smart contracts, which is agreed upon by set of users.

(b) The interaction among the users is only by signing the transactions without submitting anything to miners.

(c) The entire set of the transaction is then submitted to the BC.

5. **Plasma**: Plasma is a series of contracts that run on top of the root chain in the form of root chain's branches. They contain their own independent data and can issue their own unique tokens which helps them to incentivize the chain validators for proper functioning of the chain and to make sure that the data in the chain is fault-free.It trims unnecessary data from the root chain which run as a series of contracts on top of the root chain. These series of contracts keeps the root chain updated by sending periodical reports. Whenever these branches need to send data to main chain they only send the block header hash keeping the rest content in their own independent data which reduces the load on the main chain. Hence this approach saves the space in the main chain but also increases transaction processing speed. This approach is implemented by Ethereum to solve its scalability issues [28].

In [18], Scalability of the system is addressed by throughput, latency and capacity of the system. Use of BigchainDB helps in increasing the throughput of the system as throughput is positively correlated with the no. of increasing nodes in the system. As the nodes only store subset of the whole data and each bit of data is replicated on certain other nodes, this method also positively correlates with the capacity of the system, as increasing no. of nodes does not change the capacity of the system. Whereas, LSB used distributed trust algorithm to address the scalability of the system, which reduces the number of transactions that are needed to be verified by the OBM based on trust. It uses two notions 1) Direct evidence: If two OBMs have already used a block generated by anyone of them. 2) Indirect evidence: If two OBMs have not shared any Block so far but any Third OBM confirms that the block generated by anyone of them is valid. Each OBM maintain its direct trust association in order to gain respect from other OBMs. If an OBM keeps on initiating false blocks than its trust rating will be decremented by one with each false block, which means more of its transactions are needed to be verified. Ultimately, results the stronger evidence an OBM has obtained in generating new blocks, fewer transactions are needed to be verified [19].

Chapter 4

Conclusions

Blockchain technology is exceeding and expanding over large scale, its applications also has wide range like finance, healthcare, IoT, supply chain and many more. In this paper the applicability of blockchain with IoT for SCM is surveyed which discussed the related work in this direction and architecture of systems using BC & IoT for SCM. Altough BlockChain (BC) is an effective technology for providing traceability, security and privacy in Supply Chain Management (SCM), its application in the IoT context confer several challenges including: complexity, bandwidth and latency overeheads & scalability, to address these challenges light weight BCs could be an appropriate solution. The implementation of such lightweight BCs in SCM depends on the size of the SCM system in terms of its infrastructure, number of stakeholders involved, number of transactions that could take place and how frequently those transactions are needed to be processed. On the other hand, typical structure of a BC is such that it is capable of overcoming various challenges in SCM, specifically traceability and data intergrity.

The result of a comparative analysis in Chapter 3 helps to propose an ideal and feasible blockchain-and-IoT-based approach with the goal of enabling an auto- mated and transparent supply chain management and monitoring system. The Architecture section helps to come up with an appropriate architecture considering various requirements like what systems and IoT devices to use and how to store and transfer data. Decisions related to consensus mechanisms and cryptographic algorithms are demonstrated to provide an appropriate approach for SCM. Further challenges related to throughput management, latency, security and privacy helps to study specific factors that plays a crucial role in proper functioning of the BC system whereas scalability sections provides insights to various approaches used by these systems to overcome their specific scalability problems.

Bibliography

[1] Provenance: Introductio to Blockchains for supply chain transparency,[online] Available: https://www.provenance.org/tracking-tuna-on-the-blockchain, Last Visit: 6 September 2018

[2] M. Weber and M. Boban, "Security Challenges of the Internet of Things," *9th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2006, pp. 638-643.

[3] Abramowicz, Michael, "Cryptocurrency-Based Law," *GWU Law School Public Law Research*, 2015, pp. 2015-9. [online] Available: https://ssrn.com/abstract=2573788 or http://dx.doi.org/10.2139/ssrn.2573788, Last Visit: 6 September 2018.

[4] Minhaj Ahmad Khan, Khaled Salah, "IoT security: Review, Blockchain Solutions, and Open Challenges" *Future Generation Computer Systems*, (Vol. 82), 2018.

[5] Satoshi Nakamoto, "Bitcoin: A peer-to-Peer Electronic Cash" [online] Available: https://bitcoin.org/bitcoin.pdf, Last Visit: 6 September 2018.

[6] Aung, M. Min, & Chang, Y. Seok, "Traceability in a food supply chain: Safety and quality perspectives," *Food control*, 2013, pp. 172-184.

[7] Boyacia, I.H., Temiza, H.T., Uysala, R.S., Veliogluc, H.M., Yadegaria, R.J., Rishkana, M.M. "A novel method for discrimination of beef and horsemeat using Raman spectroscopy," *Food Chemistry*, 2014, pp. 148, 37-41, Available: http://www.labguide.com.tw/user/w016267551/upload/file/beef-horse\%20food\%20chem.pdf, Last Visit: 6 September 2018.

[8] Archana Prashanth Joshi, Meng Han and Yan Wang , " A Survey on Security and Privacy Issues of Blockchain Technology," (Vol.1, No.2) 2018, pp. 121-147, Available: https://www.researchgate.net/profile/Archana_Joshi9/publication/325173502_A_survey_on_security_and_privacy_issues_of_blockchain_technology/links/5b40d165a6fdccbcf9079f73/A-survey-on-security-and-privacy-issues-of-blockchain-technology.pdf, Last Visit: 6 September 2018.

[9] H. Gross, M. Holbl, D. Slamanig, and R. Spreitzer, "Privacy-Aware Authentication in the Internet of Things," *Cryptology and Network Security. Springer International Publishing* (Vol.1, No.2) 2015, pp. 32-39.

[10] Skarmeta, Antonio F., Jose L. Hernandez-Ramos, and M. Moreno, "A decentralized approach for security and privacy challenges in the internet of things," *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 2015.

[11] Danco Davcev, Ljupco Kocarev, Anna Carbone, Vlado Stankovski, Kosta Mitresk, "Blockchain-based Distributed Cloud/Fog Platform for IoT Supply Chain Management," 2018, pp. 51-58.

[12] M. P. Caro and M. S. Ali and M. Vecchio and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)* 2018, pp. 1-4.

[13] Kari Korpela, Jukka Hallikas, Tomi Dahlberg, "Digital Supply Chain Transformation toward Blockchain Integration," *Hawaii International Conference on System Sciences 2017 (HICSS-50)*, 2017, Available: `https://aisel.aisnet.org/hicss-50/in/digital_supply_chain/2/`, Last Visit: 6 September 2018.

[14] Feng Tian, "An agri-food supply chain traceability system for China based on RFID amp;amp; blockchain technology," *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016, pp. 1-6, Available: `https://ieeexplore.ieee.org/document/7538424/authors`, Last Visit: 6 September 2018.

[15] Rafael Bettin-DiazEmail, Alix E. RojasEmail, Camilo Mejia-MoncayoEmail, "Methodological Approach to the Definition of a Blockchain System for the Food Industry Supply Chain Traceability," *Computational Science and Its Applications â ICCSA 2018. ICCSA 2018*, (vol. 10961), 2018.

[16] Thomas Bocek, Bruno B. Rodrigues, Tim Strasser, Burkhard Stiller, "Blockchains Everywhere- A Use-case of Blockchains in the Pharma Supply-Chain," *2017 IFIP/IEEE International Symposium on Integrated Network Management (IM2017)*,2017, Available: `http://dl.ifip.org/db/conf/im/im2017exp/119.pdf`, Last Visit: 6 September 2018.

[17] D. Tse and B. Zhang and Y. Yang and C. Cheng and H. Mu, "Blockchain application in food supply information security," *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2017, pp. 1357-1361, Available: `https://ieeexplore.ieee.org/document/8290114/`, Last Visit: 6 September 2018.

[18] Feng Tian, "A supply chain traceability system for food safety based on HACCP, blockchain and Internet of things," 2017, Available: `http://arxiv.org/abs/1712.02969`, Last Visit: 6 September 2018.

[19] Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram, "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy," *2017 International Conference on Service Systems and Service Management*, 2017, pp. 1-6, Available: `https://ieeexplore.ieee.org/document/7996119/`, Last Visit: 6 September 2018.

[20] T. M. Fernandez-Carames, P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," (vol. 6), pp. 32979-33001, 2018, Available: `http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8370027&isnumber=8274985`, Last Visit: 6 September 2018.

[21] Y. Gupta, R. Shorey, D. Kulkarni, J. Tew, "The applicability of blockchain in the Internet of Things," *2018 10th International Conference on Communication Systems Networks (COMSNETS)* pp. 561-564, 2018, Available: `https://ieeexplore.ieee.org/document/8328273/`, Last Visit: 6 September 2018.

[22] M. Samaniego, R. Deters, "Blockchain as a Service for IoT," *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* pp. 433-436, 2016, Available: `https://ieeexplore.ieee.org/document/7917130/`, Last Visit: 6 September 2018.

[23] Goran Pulkkis, Jonny Karlsson, Magnus Westerlund, "BlockchainâBased Security Solutions for IoT Systems," *Internet of Things A to Z: Technologies and Applications 20180501, Chapter 9*, 2018, Available: `https://onlinelibrary.wiley.com/doi/10.1002/9781119456735.ch9`, Last Visit: 6 September 2018.

[24] B. C. Florea, "Blockchain and Internet of Things data provider for smart applications," *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, 2018, pp. 1-4, Available: `https://ieeexplore.ieee.org/document/8406041/`, Last Visit: 6 September 2018.

[25] R. Li and T. Song and B. Mei and H. Li and X. Cheng and L. Sun, "Blockchain For Large-Scale Internet of Things Data Storage and Protection," *IEEE Transactions on Services Computing*, 2018, pp. 1-1, Available: `https://ieeexplore.ieee.org/document/8404099/`, Last Visit: 6 September 2018.

[26] BlockchainHub: Cryptography Blockchain - Part 1, [Online] Available: `https://blockchainhub.net/blog/blog/cryptography-blockchain-part-1/`, Last Visit: 6 September 2018.

[27] Marko Vukolic, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," *Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science*,(vol 9591) 2016, Available: `https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9`, Last Visit: 6 September 2018.

[28] Blockgeeks: Blockchain Scalability: When, Where, How?, [Online] Available: `https://blockgeeks.com/guides/blockchain-scalability/`, Last Visit: 6 September 2018.

[29] N. Kshetri, „Can Blockchain Strengthen the Internet of Things?," *IT Professional*,(vol. 19, No.4), pp. 68-74, 2017, Available: `https://link.springer.com/chapter/10.1007/978-3-319-39028-4_9`, Last Visit: 6 September 2018.

[30] CERASIS: The Evolution and History of Supply Chain Management, *INFOGRAPHIC*, 2015, Available: https://cerasis.com/2015/01/23/history-of-supply-chain-management/, Last Visit: 6 September 2018.

[31] CISION: The 2016 Food Revolution Study,[online] Available: https://www.prnewswire.com/news-releases/study-ninety-four-percent-of-consumers-say-food-product-transparency-from-brands-an html, Last Visit: 6 September 2018.