TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

Esteban Ramirez 194312IVCM

# PRESERVING INFORMATION'S INTEGRITY AND CONFIDENTIALITY WITH BLOCKCHAIN IN THE SERVICE SUPPLY CHAIN

Master Thesis

**Technical Supervisor**
Jaan Priisalu
MSc
**Academic Supervisor**
Alexander Norta
PhD

Tallinn 2021

# Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Esteban Ramirez ................................

(signature)

Date: 13/05/2021

# Abstract

Supply chain is an essential part of industries globally, and the service supply chain is not the exception. Information is crucial for proper decision making and risk management in a fast paced and interconnected environment such as the one in service supply chains. Information handling is becoming increasingly difficult due to the increased volume and speed at which information is generated which increases risk to information, especially in a heavily information reliant environment such as services.

Current information sharing tools are usually misconfigured or might not be secure enough, at the same time data duplicity, centralization and integrity issues affects the level of trust among parties in the supply chain thus affecting the quality and frequency of the shared information. Is it in the light of these problems that the current research seeks to explore how is information currently shared in service supply chains and its underlying problems and issues to finally develop a framework for the implementation of blockchain technology to preserve the integrity and confidentiality of information in service supply chains.

A case study design was considered appropriate for the research, extensive literature review was conducted as well as interviews with relevant professionals. The findings revealed that some of the current used systems could preserve the integrity and confidentiality of information if configured properly. The findings also showed that the main barriers to blockchain implementations are lack of understanding of the technology, lack of regulation, cost, integrability, resistance to change, scalability, etc. Considering the above mentioned factors, a framework was developed to set the basis for future guidelines, research or implementations of blockchain in service supply chains.

This thesis is written in English language and is forty six (46) pages long, including 5 chapters, 1 table,and 5 figures.

# List of abbreviations and terms

| | |
|---|---|
| SC | Supply Chain |
| SSC | Service Supply Chain |
| SCM | Supply Chain Management |
| ICT | Information And Communication Technologies |
| CSCRM | Cyber Supply Chain Management |
| IOT | Internet Of Things |
| BRICS | Brazil, Russia, India, China, South Africa |
| IT | Information Technology |
| PoW | Proof Of Work |
| PA | Proof of Authority |
| PoS | Proof of Stake |
| CSCRM | Cyber Supply Chain Risk Management |
| SCOR | Supply Chain Operations Reference model |
| GSCF | Global Supply Chain Forum Framework |
| BiTA | Blockchain In Transport Alliance |
| SDK | Software Development Kits |
| TPS | Transactions per Second |
| ERP | Enterprise Resource Planning |
| SaaS | Software as a Service |
| GDPR | General Data Protection Regulation |
| PBFT | Practical Byzantine Fault Tolerance |
| API | Application Programming Interface |
| CIO | Chief Information Officer |
| ZKP | Zero Knowledge Proof |
| EDI | Electronic Data Interchange |

# Table of Contents

# List of Figures

# List of Tables

# 1. Introduction

Supply chains play a major economic and innovative role in countries around the globe. Only in the US, 37% of the jobs in the market are provided by supply chains [1] and are a source of innovation due to their links to other industries allowing for their ideas to spread downstream. Efficient supply chains lead to faster industry growth and development which is crucial for economies.

Due to SC's importance, technology has been used to improve the efficiency and management of supply chains, giving birth to what is known as the cyber supply chain. Cyber supply chain has been widely adopted as the new normal for its capacity of improving communication and visibility between different parties leading to increased level of trust and transparency for the stakeholders. The digitization of supply chains is an essential mean of cost reduction as a better tracking of products and services is available.

There are different types of supply chains, the traditional supply chain deals with manufactured, physical goods, whereas the service supply chain deals with intangible goods. The latter has different nature and characteristics that makes it special during risk management, specially when the technological factor is added.

Regardless of these benefits, the introduction of technology in the service supply chain has at the same time introduced plenty of attack vectors to the integrity and confidentiality of information which need to be addressed with special consideration to the natural characteristics of services and their interaction with technological tools used for information management and sharing. Due to this increased risk, stakeholders of the service supply chain are hesitant to share information with each other, leading to inefficiencies and added cost.

Due to the impact this problem has on organizations, it is necessary to come up with innovative solutions, thus, the option of using blockchain for information sharing in the service supply chain. Blockchain technology also known as distributed ledger technology seems to be growing in popularity and applications in private and public sectors across the world to solve multiple problems.

The main attractive feature of this technology is its capacity of recording immutable transactions that provides total visibility and a clear auditable trail of what has happened with the asset on the blockchain with a decentralized nature. The technology's use has been explored in multiple areas such as finance, healthcare, and traditional supply chain, among others.

This thesis' main goal is to create a framework that would guide the implementation of blockchain technology for information sharing in service supply chains. It will describe the current state of information sharing in service supply chains and through a research methodology investigate how blockchain can affect information sharing and the service supply chain overall.

## 1.1 Problem Statement

Modern day "supply chains are increasingly operating in a massively connected global environment where connectivity and integration happens among people, processes, and devices through information and communication technologies (ICT)"[2], to reduce cost and increase efficiency, which makes all actors within the chain more dependable on each other. The involvement of more organizations, all sharing information through digital means, makes risk management a more difficult task as the attack surface has expanded considerably faster than the risk management methodologies and frameworks could adapt.

It is without doubt that supply chains play a major role in the world economy, they are in charge of moving information, products and finance between different actors across the world. Service supply chains are becoming increasingly important to the gross domestic product of nations around the world, for this reason risk management is crucial in keeping the service supply chain working uninterrupted so that customers around the world can be serviced on time and their expectations are met. This, however, is not an easy task, as mentioned by different researchers who describe the inherent differences of services compared to manufacturing processes, and point out that these render the traditional risk management approaches ineffective in service supply chains [3] [4] [5][6].

It is widely mentioned in the reviewed literature that little has been researched about risk management in service supply chains and even less about cyber-specific risks [3][5][7][8]. Communication between supply chain members is key to minimizing the chance of threats materializing [9], however, this is challenging as there is a lack of trust between members of the supply chain [10],[11][12] as information can be shared with competitors or it can be leaked by malicious actors.

It is clear that there is a need in the service supply chain environment of a tool or technology capable of providing a better and more reliable way of sharing information which can be accessed by the main stakeholders to make better business decisions. Thus, developing an efficient information sharing system which reduces the cost and enhances efficiency will greatly benefit the industry of services worldwide.

## 1.2 Research Objectives

This research aims to examine and analyze the struggles of information sharing in service supply chains and how blockchain technology can be adopted to minimize the risks caused by mishandling of the shared data. The main objectives are:

1. Analyze the current state of information sharing in service supply chains and its inherent problems.
2. Describe how blockchain technology can reduce the risk to information sharing in service supply chains, while increasing transparency and trust.
3. Identify the enablers and barriers facilitating or impeding the implementation of blockchain technology.
4. Create a framework that will set a base for future research or implementations of blockchain to the service supply chain domain.

## 1.3 Research Questions

The main purpose of the research is to explore the uses that the blockchain technology can have in service supply chains to reduce the risk to integrity and confidentiality of information shared between the supply chain members and how effective the technology is at doing this.

From the literature review, it is clear that risk management methodologies for SSC must be different from the traditional SCs and that little has been researched in this respect, at the same time it became clear that SCM is changing as ICTs and innovative technologies are involved to optimize the process by reducing costs and improving efficiency. Blockchain is a technology that is disrupting different industries, however it proved very difficult to find applications of blockchain in a generalized way to service supply chains; most of the cases were to a specific industry/sector. Thus the research questions are derived from the identified research gap.

**RQ: How can blockchain enhance the integrity and confidentiality of the shared**

**information in a service Supply chain?**

In order to expand the research and obtain detailed results the main research question is subdivided, denoted by SRQ as follows:

- SRQ1: How is information currently shared in SSC?
- SRQ2: How can blockchain technology affect the risk to integrity and confidentiality of information shared across the service supply chain?
- SRQ3: How can blockchain be implemented in a SSC.

These subdivided questions are further subdivided into more specific questions which are then included in the surveys.

The questions derived from SRQ1 aim to obtain a better understanding of the current situation in service organizations in regard to sharing information and problems affecting them. SRQ1 is further divided as follows:

- What tools are being used in the service supply chain to share information with stakeholders and customers?
- How trustworthy are those tools/platforms to safekeep the confidentiality and integrity of the shared information?
- What are the main problems with the currently used methods to share information?

The questions derived from SRQ2 seek to identify the effects of implementing blockchain in a SSC to the integrity and confidentiality of information SRQ2 is divided as follows:

- What is the level of security of blockchain to preserve the confidentiality and integrity of information?
- What are the benefits of using blockchain in SSC for information sharing?

SRQ3 is further divided to get a better understanding on how blockchain technology can be used and implemented in SSC and what are the issues and drivers of implementations.

SRQ3 is further divided as well:

- What are the main barriers/drivers of using blockchain in a service organization?
- What are the basic requirements for a process to implement blockchain?
- What is the best type of blockchain and consensus method for a service environment?

## 1.4 Context

Information is a key element for organizations in a supply chain as a competitive advantage [13] as it allows the stakeholders to take better informed decisions in a timely manner. "Supply chains are increasingly operating in a massively connected global environment, where connectivity and integration happens among people, processes and devices through information and communication technologies (ICT)" [14].

The digitization of information facilitates a rapid communication but at the same time has introduced complex problems. Such connectivity considerably increases the volume and speed at which the information is generated and collected which creates the problem of properly handling the data, which translates to increased threats to information, "a perceived increase in vulnerabilities due to revealing information, combined with a lack of incentives to share" [15] have an increased negative impact on information sharing practices. Information asymmetry still exists where information is not shared among the actors of the supply chain and creates room for dishonesty between partners [16] at the same time it is more vulnerable to cyber attacks [17] affecting the integrity and confidentiality of it.

Services have gained great importance globally, World Bank data shows that services contributed to the global GDP 65% in 2018 [18]. The service supply chain (SSC) is an information-based supply chain, where no physical products are transported between entities making it quite different from the manufacturing supply chain in terms of risk management.

Manufacturing supply chain risk management frameworks have been implemented to service supply chains with no positive effect thus requiring the development of new frameworks and supply chain management strategies [3] that reduce information risks. Current data management and information sharing practices are inefficient, some stakeholders store the data offline and in a centralized way, and information is exchanged via the postal system [19]. Additionally, the ability to identify risks decreases as the visibility of the SC diminishes beyond the organizations own functions [3]. This increases costs and reduces efficiency so new ways to manage and share information in the service supply chain need to be explored.

Blockchain is a disruptive tool that became known after the release of Bitcoin. Due to its tamper resistant and decentralized characteristics, other uses have been explored in industries such as healthcare, finance, and manufacturing. Blockchains stores fully traceable and immutable records transformed from the data generated in the supply chain, such as sales information, product information, etc, enabling the authenticity of the data in the supply chain [19] and improving trust between the parties.

Despite the meaningful advance in recent years, blockchain applications and the interaction with supply chain management are still in its infancy [20]. Given the complex issue of sharing information in the service supply chain environment, the use of this new technology is explored to achieve a better cooperation between the actors in the chain by improving the trust and security when sharing information.

## 1.5 Limitations

Even though a thorough research methodology was followed, it is inevitable to find certain limitations due to the research method used. The data collection method used in the study case such as interviews in this case, obtain information that is representative to the interviewees' reality and experience, making it possible to find totally contradictory views, rendering the generalization a problem, at the same time the analysis of the respondents vulnerable to the interpretation and the experience of the analyzer.

Due to the current world pandemic, it was not possible to physically meet with the respondents. All the interviews were conducted via video call and recorded for later transcription. In total, 30 experts were contacted of which a total of 12 agreed for an interview. It is important to note that a higher number of respondents would have made the research more robust, but the difficulty of finding people willing to donate their time for a 60min interview exists.

Finally, it is important to mention that there might be certain conflict of interest from the interviewees as most of them work with blockchain technology implementations so they view of the technology might be biased towards its promotion. Additionally interviewing one of the supervisors could create a conflicting result, however, given that the professional is an academic an objective view of the technology is expected.

# 2. State of the Art

The following chapter provides the theoretical background information for this thesis. The main topics such as blockchain, supply chain and their interactions are defined here. In this section the current state of how information is shared is explored to understand the existing limitations and if/how blockchain can be used to minimize them.

## 2.1 Supply Chain

The globalized world is dominated by commerce between different nations and organizations moving thousands of tonnes of material, money, and information between different entities along the way. This process is defined as a supply chain. A traditional or physical supply chain (SC) is“dominated by the movement of products, finance and information” [21] between different entities.

During the last few decades, supply chains have evolved considerably, becoming more complex as technology is involved to increase their efficiency, reduce costs by better monitoring of inventory pools, and risk reduction by preventing the bullwhip effect among other benefits. Some refer to this technologized supply chain as “cyber supply chain”. “A cyber supply chain is a network of IT infrastructure and technologies that are used to connect, build, and share data in virtual networks” [22].

The inclusion of IT systems has provided a tremendous increase in efficiency and effectiveness, however, at the same time it introduced risk factors that are not linked to the physical product were not accounted for in supply risk management by increasing the attack surface, this has made risk management a difficult task as more organizations become involved in the SC, all sharing information through digital means. It is well noted by the literature that the ability to identify and assess risks decreases as soon as the product or service leaves the organizations’ premises or responsibility domain [3].

There are different types of SCs depending on the flow of information and products transported. Physical supply chains refer to those dealing with manufactured products or materials, however, not all SCs trade with tangible products, these are referred to as SSCs, as they provide services to the end customer. These two types of SCs are very different from each other and the latter deserves a closer inspection due to their complex nature.

### 2.1.1 Supply Risk Management

Supply chain risk management has gained more fame in recent years due to the volatility, evolution and complexity of globalized supply chains and the economic impact that disruptions have. A supply chain risk is defined as “the variation in the distribution of possible supply chain outcomes, their likelihoods, and their subjective values”[23] and “supply chain risk management consists on implementing strategies to manage both daily and exceptional risks along the supply chain based on continuous risk assessment to reduce vulnerability and ensure business continuity” [24].

The traditional supply risk management consists of 4 stages[25]:

- Risk identification
- Risk assessment
- Risk mitigation
- Risk monitoring

It is important that the supply chain actors implement the risk management strategies internally to their organizations, but it is also crucial that a coordinated approach is taken by all members of the chain to effectively manage and reduce the supply chain risks and enhance resilience[26][27][28]. Resilience refers to the capacity the processes have to return to the normal state after a disruption [29], in a connected and complex supply chain it is necessary for all entities to communicate between each other to share useful information that leads to risk prevention, such information besides the regular business data can be recovery reports, incident reports, etc, that can help creating shared-knowledge base.

Given the use of IT systems in the SC, a new construct called cyber supply chain management (CSCRM) has gained momentum. Cyber supply chain management includes the strategy and initiatives focusing on the assessment and mitigation of cyber and information risks across the end-to-end operations of a supply chain [30][31]. Unlike cyber security, which gives more importance to the technical controls to prevent risks from disrupting IT systems’ operations and the traditional SCM, CSCRM emphasizes to link together processes, people and technology to achieve a “relationship dimension” [32][12]. This is done to enable a high level of integration between the different parties that conform a supply chain and that share information and risks.

### 2.1.2 Service Supply Chain

Services attention worldwide is increasingly growing as the world economy becomes more dependent on them. For example, “in developed markets such as the US, it is reported that over 90 percent of the GDP comes from the service industry. Even in developing countries, such as Brazil, Russia, India, China, and South Africa (BRICS), the service industry is developing rapidly” [33].

Despite their growth and importance in international business, risk management in the field is still in its infancy [3]. Service supply chain (SSC) is defined as “a network of suppliers, consumers, service providers and other supporting units that provide the resources necessary to produce services, transform resources into supporting and core services and then deliver these services to customers[34].”

The approach to risk management in SSC and product supply chain must be different due to the inherent nature of services[4][35][36]. SSC is characterized by using the IHIP attributes: intangibility, heterogeneity, inseparability, and perishability [6][4].

- Intangibility: This attribute implies that services do not have a physical existence.
- Heterogeneity: Refers to the fact that most services are very different from each other.
- Inseparability means that the service is produced and consumed at the same time, this requires a constant collaboration between the producer and the customer
- Perishability means that services cannot be stored in inventories, they depend on the time they are produced.

The IHIP attributes make the SSC more complex from the risk management perspective as its heterogeneity; differences in customer needs, and involved personnel render the conventional standardized risk model of the traditional supply chain impractical as there are no standard inputs or outputs. Secondly the intangibility, inseparability and perishability nature of a service creates a different level of complexity as it cannot be stored in inventories and is in constant change contrary to the traditional SC where the goods can be stored in buffer inventories, this creates a problem, if the supply chain is interrupted the service itself would cease, directly affecting the customers. Thus, the traditional supply chain management has not been able to meet the demands of the SSC and new tools and strategies need to be developed[4].

### 2.1.3 Information Sharing challenges in Service Supply Chain

Information in a global digital supply chain is in constant flow as it is being constantly generated during the production of the product or service. There are many different types of information that can be produced and shared in a SSC, some of the most common can be categorized as: sales data, sales forecasting, order information, exploitation information of new products [37]. The SSC is heavily reliant on information, as a source of competitive advantage, allowing educated managerial decisions, cost reduction, increased visibility [37].

With the introduction of IT systems a large quantity of information is shared between all members of the chain. Managing all this data is a challenging task for organizations due to the volume, speed of transmission and growing variety of types of information [38] increasing the information risk.

It is well noted that coordination among all the members of a supply chain is crucial to a proper management of cyber risks [38], "this coordination can be achieved through synchronization, intended as a tool enabling effective information-sharing among supply chain partners and supporting decision-making, especially during disruption responses" [39] and "shared knowledge, i.e. sharing of experiences among supply chain partners after disruptions are overcome with the aim to create post-incident reports accessible to all" [40].

The importance of information is evidenced in a thorough survey conducted to different New Zealand's supply chain managers of different size organizations who all agree that data exchanges play a critical role in their businesses [9]. However there are certain information risks and challenges. Information risk is "the probability of loss or degradation of the main security goals: confidentiality, integrity and availability arising because of incorrect, incomplete, or illegal access to information" [41][42] which can render it useless or insecure to use.

The main cause of failure in the SCM is wholly linked to the lack of trust and transparency [43] as usually the members of the SC don't trust each other due to the risk of information being leaked, unauthorized disclosure and maliciously modified [44]. "Confidence in the perceived security of supply chain information systems determines the willingness and capability of a firm to share confidential data with trading partners" [45]. According to [44],[46] and [47] the main issue of securing information in digital supply chains are:

- Lack of mechanisms to communicate owner's policies associated with information on the protection frameworks of the partners of a SC.

- Lack of common information sharing standards for protecting the information in the SC. Each organization has its own security requirements, these reduce the ability to ensure enforcement of required policies on the shared information among all members of the SC causing security concerns. The information is dispersed in different information systems and sources.
- Evolution of security measure to meet business models, regulatory and other requirements. This created the need for organizations to not only update their own systems and security policies and measures but to also coordinate with all the other entities in the SC to enforce the new policies and security required.
- Information doesn't flow fast enough
- Information is not sufficiently documented/updated
- Internal culture, it is very difficult to change the mentality and established way of an entire organization and staff of doing things, which makes the adoption of changes and implementation of new and better tools harder.

As stated by [11] the main information risks in a supply chain include:

- risk to information confidentiality, which relates to the potential loss of control over sensitive information/data across the supply chain.
- risk to information privacy, which relates to the potential misuse of data out of the principal purpose of releasing data by the data owner.
- risk to information integrity, which relates to the potential corruption and damaging of data/information stored in information technology (IT) systems across the supply chain network.

"Among the various risks that organizations face include relational risks such as a business partner's engagement in opportunistic behavior (e.g, cheating, distorting information)[48][49]."

The new cyber supply chain offers a wider attack surface from where attackers can extract customer records, competitive data, and intellectual property. Existing supply chain manufacturing frameworks such as Hewlett-Packard's model, Supply-Chain Operations Reference model (SCOR), and the Global Supply Chain Forum Framework (GSCF) have been analyzed for their application to the SSCs, of all three models the GSCF and SCOR proved useful when modified, nevertheless with limited success as neither one of these frameworks has been tested outside of their conceived scope for applicability or generalizability [35][34][50].

Different frameworks are used to protect the integrity and confidentiality of the information circulating through a supply chain, for example, GS1 Standards, NIST guidelines, and Secure Supply Chain protocols, however, these have their own deficiencies so different researchers [44] proposed a new framework to assure end-to-end security in business processes of organizations that compose a digital supply chain, such framework was adapted from a web-services environment, nevertheless their proposed method has not been developed into an application prototype nor has it been tested in a real scenario.

The currently used tools to share information in a SSC range from different levels of complexity and security. The most commonly used tools to share information are detailed by [46] as:

- Enterprise Resource Planning Systems: these are systems used across the entire organization to automate and control as many functions of a business, some of the most known providers are SAP, Oracle, Baan.
- Electronic Data Interchange Systems: These systems are used to facilitate transactions and information sharing between organizations.
- Web services which are applications accessible via the internet using XML
- Electronic commerce tools. This category includes any other tool used for business in a paperless way, such tools are: email, shared databases, electronic fund transfers, bulletin boards, etc.

## 2.2 Cybersecurity and Cyber Risks in Supply Chain

Cybersecurity is a domain that continues to grow and gain importance due to the interconnected world through IT systems which facilitate the communication and movement of information and goods. Kaspersky [51] succinctly defines it as “the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.” As SC becomes more digitized the need for cybersecurity to protect the IT systems interconnecting the SC from the cyber risks becomes more evident as well.

Every year many cases of SC attacks come to light with devastating effects and with a very complex nature, making them hard to investigate. SC attacks increased 78 percent in 2018 compared to the previous year [52] causing catastrophic economic consequences. As an example, the very recent supply chain attack that is causing major concerns is the SolarWinds attack.

SolarWinds is a software company whose most widely deployed product is a network management system called Orion. The company claim to have over 300 000 customers of which some are big companies such as 425 companies from the US Fortune 500, the US Federal government, and hundreds of other customers around the globe. The attack on SolarWinds was deployed through a legitimate update to Orion provided by SolarWinds' own servers and digitally signed by a valid certificate under their name which strongly points to a SC attack [53]. It is still unknown how SolarWinds was breached at the time of writing, however the impact to many of the affected organizations is starting to come to light. Microsoft's source code is said to be stolen and the US Department of Justice admitted that their email environment was accessed by the hackers as a result of the attacks with possibly bad consequences [54].

Data breach is another latent threat for supply chains, according to a 2020 data breach report by Verizon [55] there were 3950 confirmed data breaches in 2020, of which 8% were due to misuse of the information by authorized users. Around 30% of the breaches involved internal actors. This report highlighted the increase of errors as being one of the most frequent reasons of data breaches, either misconfiguration errors, or human error referred to as misdelivery, which means an employee sending an email to the wrong contact, the former has been increasing since 2017 which is in large part due to the internet-exposed storage.

## 2.3 Blockchain

Blockchain is a technology that gained fame after 2009 with the launch of the Bitcoin network, and since then it has been widely explored for other uses in healthcare for securing patient information [56], financial [57], and cryptocurrency [58] sectors to mention some, and supply chain [59] is not the exception. The technology has become so popular that organizations such as Blockchain In Transport Alliance (BiTA) are formed to implement, educate, and research the technology for its application in the transportation and logistics sectors.

"Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government) [60]". The underlying function of the technology enables a group of users to record and change transactions stored in the distributed ledger which is not overseen by anyone and which under normal circumstances cannot be modified after its creation. Essentially it is "a protocol for establishing consensus on valuable information within a flat network without hierarchy [61]".

Blockchains consist of data records or interconnected blocks which are filled with transactions generated by the users. Each block is added to the next in an irreversible chain and transactions are blocked together, once these blocks are collected in a chain, they cannot be changed or deleted by a single actor. Instead, they are verified and managed using governance protocols [62], a general blockchain process is depicted in figure 1. This means that no single user in the chain owns the information, instead every user can directly verify the information previously stored without the need of any intermediaries [63]. The open verification process along with modern encryption methods prevents modification and unauthorized access of the shared information in a blockchain. Given that the blocks already recorded in a blockchain cannot be modified or deleted, the data can be easily audited as there is full visibility of all records [64].

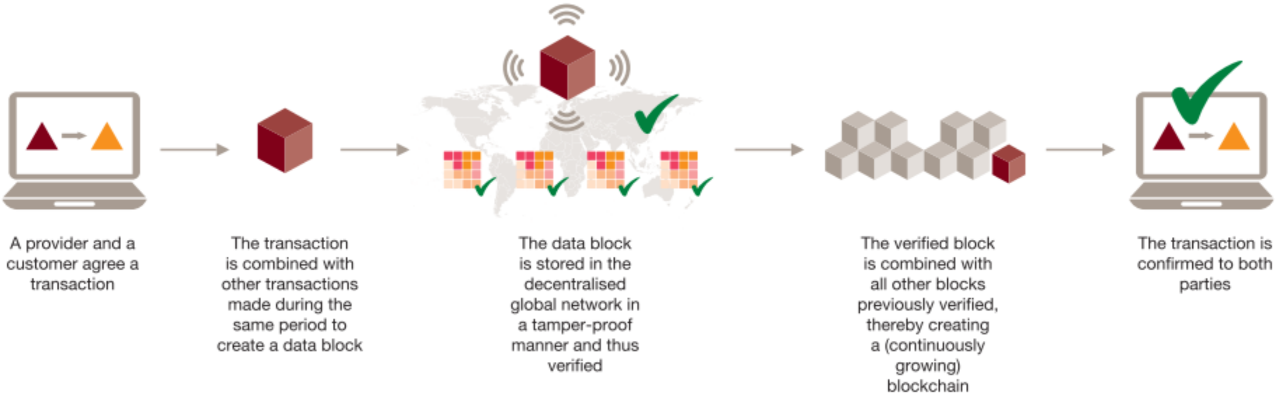

A provider and a customer agree a transaction
The transaction is combined with other transactions made during the same period to create a data block
The data block is stored in the decentralised global network in a tamper-proof manner and thus verified
The verified block is combined with all other blocks previously verified, thereby creating a (continuously growing) blockchain
The transaction is confirmed to both parties

Figure 1. *The blockchain process.* Source: [65]

### 2.3.1 Blockchain Architecture

Blockchain consists of a sequence of blocks chained together as shown in figure 2, the first block of the chain is called genesis block, it has no parents, and all other blocks are related to it.

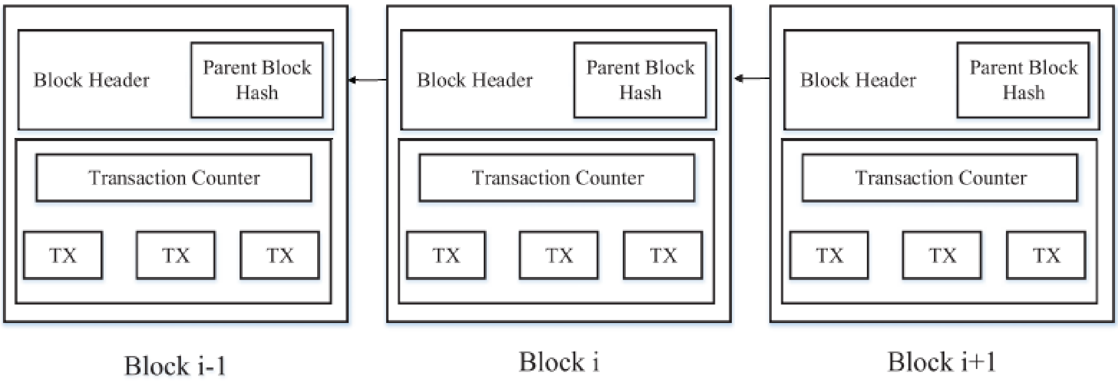


Figure 2. *Blockchain example.*Source:[66]

Each block consists on a block header and a block body as shown in figure 3. The block body contains all transactions and the transaction counter, while the block header contains different elements defined by [66] as:

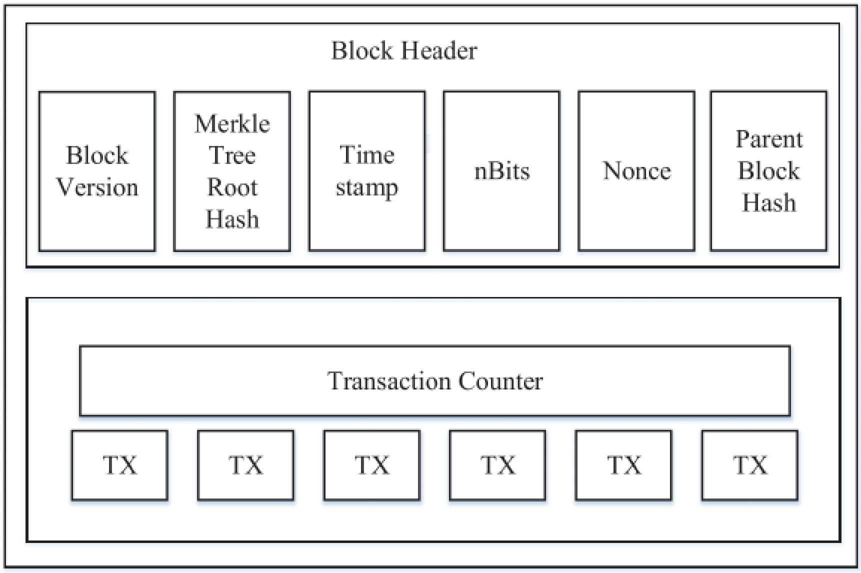


Figure 3. *Blockchain structure.* Source:[66]

- Block version: indicates which set of rules to follow for the validation.
- Merkle tree root hash: the hash value of all the transactions in the block.
- Timestamp: current time as seconds in UTC.
- nBits: target threshold of a valid block hash.
- Nonce: a 4-byte field starting at 0 which increases for every hash calculation.
- Parent block hash: a 256-bit hash value that points to the previous block.

### Key Characteristics of Blockchain

In summary, the main characteristics of the blockchain technology are as follows [66]:

- Decentralization: There is no need for a third party approving any transaction or operation in the blockchain opposing to the conventional centralized transaction systems.
- Persistency: It is very hard or impossible to change any information already posted to the blockchain
- Anonimity: Each user remains anonymous as they participate with a generated address, however, total privacy cannot be ensured
- Auditability: All transactions are recorded and cannot be modified and each block refers to the previous one, so it is easily auditable.

### Basic Technological Features of Blockchain

**Cryptography**: The transactions recorded on a blockchain are recorded using asymmetric cryptography [67], also referred to as public key cryptography. Asymmetric cryptography consists of a pair of public-private keys mathematically related. The private key must remain secret from everyone in the process except the holder while the public key can be shared with anyone without compromising the security of the process. Computation speed is often mentioned as an issue of this type of encryption [60].

**Real time:** Transactions are posted nearly as soon as they are pushed, providing nearly real-time transaction records and reconciliation of accounts [68].

**Hosting of Smart Contracts:** Smart contracts consist of "a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries." [69]

### Types of Blockchain

There are discrepancies in how many types of blockchains exist. Some sources mentioned 2 types: Permissionless and permissioned and further subdivide the permissioned type into private and consortium depending on who controls the access [70]. Other research refers to three main types of blockchains in terms of access control, i.e who can read and submit transactions; permissionless, permissioned and consortium blockchains [71]. The latter approach is used in this research to clearly differentiate from private and consortium.

The public or permissionless blockchain is open to anyone who wishes to download, read and write to the blockchain. This openness can become a problem as malicious users might try to publish blocks in a way that subverts the system. To prevent this, a consensus system is implemented in which the user that tries to publish blocks has to maintain or expend resources. Examples of such systems are proof of work and proof of stake methods [60]. Public blockchains are unlikely to be the right platform for SC operations in a private organization due to uncertain block settlement times and unpredictable network congestion [59].

The second type is the permissioned blockchain in which one organization is responsible for administering the write and read permissions which can be either public or restricted to an extent [72]. Permissioned blockchains "provides a way to secure the interactions among a group of entities that have a common goal but which do not fully trust each other, such as businesses that exchange funds, goods, or information [73].” Some permissioned blockchains can selectively reveal transaction information based on the identity or credentials of the user and who can issue transactions in a permissioned blockchain. It can be instantiated and maintained using open source or closed source software. These organizations can determine the consensus method on the level of trust of each other, securing the transparency and improving trust between the partners [60].

The third type of blockchain is the consortium blockchain in which the consensus process is controlled by a pre-selected set of nodes [74]. For example one might imagine a consortium of 15 organizations in a supply chain each of which control one node and of which 10 must sign every block in order for the block to be valid. In this case, the read access might be public, private, or hybrid depending on the consortium needs. Consortium blockchains are faster when compared to the other two, also they are more efficient in terms of privacy and verification [75].

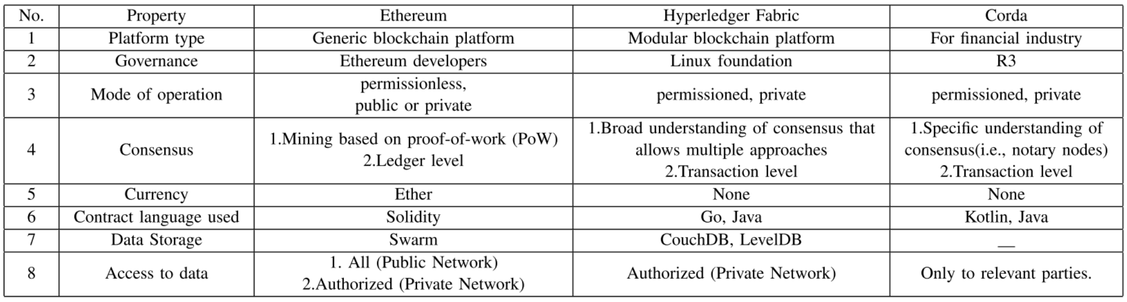
### 2.3.2 Blockchain Platforms

Since the creation of Bitcoin, different architectures, platforms and frameworks have been developed which have evolved considerably for other uses with important efficiency, security and performance improvements, thus gaining more recognition. Every type of blockchain uses a specific type of platform to run. There are countless types of platforms from where to choose. For example, permissioned blockchains can use Tendermint, Quorum, or Hyperledger to mention a few; the latter can be further subdivided into 5 different frameworks including Fabric, Burrow, Indy among others, whereas a permissionless blockchain can use Ethereum, Bitcoin, Enigma, or IOTA among many others. All these platforms use different consensus methods. In this case a few of the permissioned blockchain platforms are described as these are the most common in enterprise use.

*Hyperledger*: Hyperledger is a more flexible platform that supports modular consensus protocols. “It offers a scalable and secure platform that supports private transactions and confidential contracts [76]”, it was developed by Linux Foundation and is backed by important organizations such as IBM, Cisco and SAP [63][73] and was mainly developed for private enterprise use. Fabric consensus is more refined and provides a more detailed access control to records enhancing privacy, making it great for enterprise applications [77].

*Ethereum*: is an open source generic platform with the capacity of executing smart contracts and monetary transactions. It relies on mining based on the proof-of-work (PoW) which unfavorably affects the performance of transactions processing [63]. Ethereum can be deployed as a permissioned blockchain under Hyperledger Burrow.

*Corda*: Corda is a platform used for recording and processing financial agreements [78]. It supports smart contracts and is great for reaching consensus between organizations for individual deals, and coordinating the flow between organizations without the need of a central controller [79].



| No. | Property | Ethereum | Hyperledger Fabric | Corda |
|---|---|---|---|---|
| 1 | Platform type | Generic blockchain platform | Modular blockchain platform | For financial industry |
| 2 | Governance | Ethereum developers | Linux foundation | R3 |
| 3 | Mode of operation | permissionless,<br>public or private | permissioned, private | permissioned, private |
| 4 | Consensus | 1.Mining based on proof-of-work (PoW)<br>2.Ledger level | 1.Broad understanding of consensus that allows multiple approaches<br>2.Transaction level | 1.Specific understanding of consensus(i.e., notary nodes)<br>2.Transaction level |
| 5 | Currency | Ether | None | None |
| 6 | Contract language used | Solidity | Go, Java | Kotlin, Java |
| 7 | Data Storage | Swarm | CouchDB, LevelDB | __ |
| 8 | Access to data | 1. All (Public Network)<br>2.Authorized (Private Network) | Authorized (Private Network) | Only to relevant parties. |

Figure 4. *Differences between Ethereum, Hyperledger and Corda.* Source:[78]

**Technological differences between Blockchain types**

These three types of blockchain have important differences as mentioned by [6] [66] which are described below.

*Consensus determination*: The permissionless blockchain is completely trustless and immutable as intermediaries or central authorities are not needed at all as all miners can participate in the approval of the transactions, on the other hand the permissioned one is not completely trustless as it depends on the architecture of the consensus method or the consortium of members, finally, the consortium requires only a set of nodes to validate the block.

*Read Permissions*: In the permissionless version, each participant in the network maintains an identical copy of the entire blockchain, all records are visible to the public, however, the permissioned and consortium depend on the permissions set by the organization or consortium, these do not offer complete transparency as the master copy of all records is not distributed to all participants.

*Immutability*: Since there is a big number of participants on a public blockchain it is very hard to tamper or modify the information stored in it, on the other hand, managers have full control over the private blockchain which could limit its tamper resistance [80].

*Efficiency*: It is widely known that public blockchains transaction throughput is limited as it requires plenty of time to process transactions due to the large number of participants and the block size, the number of transactions per second (TPS) vary depending on the consensus method used, for example Bitcoin can process 7 TPS [81] which is minuscule when compared with the 24000 TPS that Visa can process[82]. On the other hand, private blockchains have fewer participants making them more efficient, the number of TPS they can process depend on the number of nodes on the network, the more nodes present in the network translates to a reduced efficiency [83].

Estimating a generalized throughput of private blockchains is complicated as they greatly vary with every use case. Different researchers have compared the throughput of Hyperledger Fabric and Ethereum, concluding that the former is capable of more TPS under different scenarios [84] [85]. New protocols have gained popularity with increased throughput such as EOS.io and ParallelChain, capable of processing 6000 [86] and 144,000 [87] transactions per second.

*Centralized*: There is no centralization in the permissionless blockchain as all participants can participate in the validation process. The consortium blockchain is partially centralized as a set of different nodes validate the transactions, whereas the private blockchain is totally centralized as only one organization handles the information [75].

*Energy Consumption*: Public blockchains such as Bitcoin require massive amounts of energy estimated between 60 and 125 TWh per year for Bitcoin which equals $10^9$ J per transaction [88], this is mainly due to the PoW consensus method where all the nodes on the network need to search for the same solution even though only one of them is rewarded [89]. Bitcoin mining consumes more electricity per year than Ireland [90]. A public blockchain using a consensus method other than PoW will use less energy however, it is still considerable in the magnitude of $10^3 J$ per transaction [88].

Different solutions for the energy consumption issue are being explored for PoW blockchains and are categorized into two types as shown in [66]: Optimizing the storage of the blockchain, to accomplish this, different methods have been proposed; one of them consists in removing or “forgetting” the old transactions by the network [91]. The second category is completely redesigning the blockchain: Bitcoin-NG redesigns the conventional block by dividing it into two parts: key block and microblock to store transactions by doing this, it is possible for microblocks to be weightless [92]. On the other hand a small scale enterprise blockchain using Hyperledger Fabric with 10 nodes capable of handling 3000 transactions per second would consume 1J per transaction [88]. A consortium blockchains using Proof of Authority (PoA) consensus method require less energy, however, they are highly sensitive to the network size [88].

For non-PoW blockchains the consensus method doesn’t consume enormous amounts of energy, instead, redundancy can highly impact the energy consumption. Two approaches can be taken to reduce the redundancy of the blockchain: reducing the degree of redundancy, which means reducing the number of nodes that perform certain operations, and the workload associated with operating a transaction [88], a concept called *Sharding* is often mentioned for this purpose. The chain size can increase considerably when all the blocks are stored in it, so instead, nodes are split into groups called *shards* and make each shard process different blocks. In addition to reducing energy consumption it can increase throughput by parallel processing transactions, however, it can make the blockchain more vulnerable to 1 percent attacks if the attacker obtains full control of any single shard [93]. Reducing the degree of redundancy makes the blockchain more centralized so it needs to be weighted against security, liveness and trust [88]. Another approach is the *off-chain* solution in which the transactions are processed outside of the blockchain

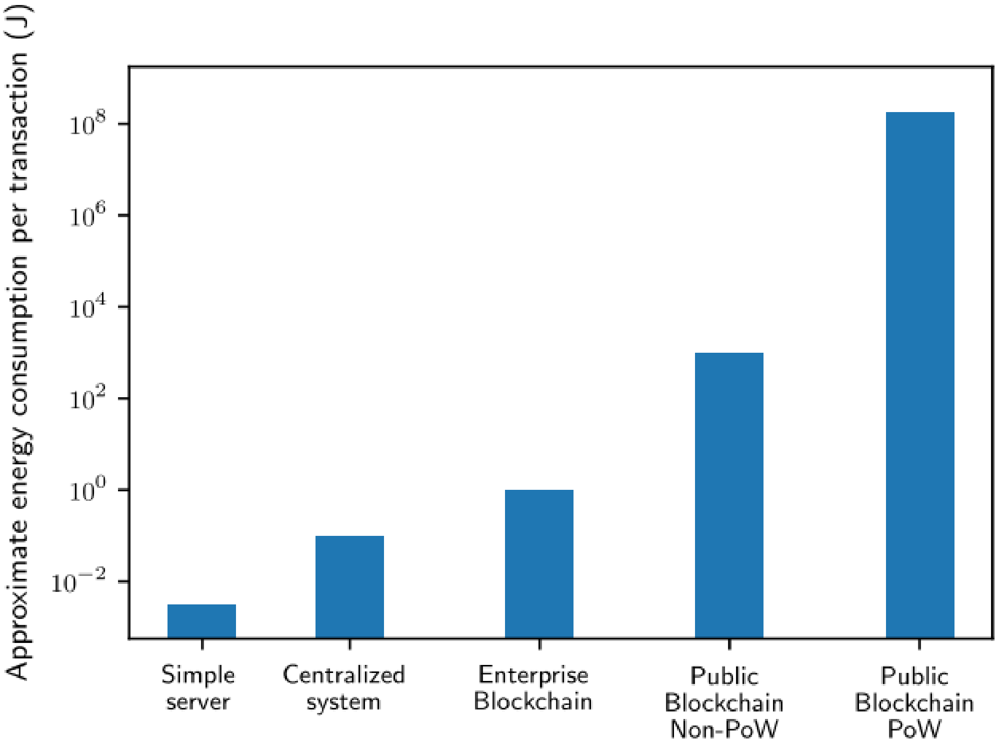


Figure 5. *Energy consumption comparison of different blockchain architectures.* Source:[88]

| Features | Permissionless | Permissioned | Consortium |
|---|---|---|---|
| Consensus determination | All miners | One organization | Selected set of nodes |
| Read permission | Public | Could be public or restricted | Could be public or restricted |
| Immutability | Nearly impossible to tamper | Could be tampered | Could be tampered |
| Efficiency | Low | High | High |
| Centralized | No | Yes | Partial |
| Consensus | Permissionless | Permissioned | Permissioned |
| Energy consumption | High | Depend on network size | Depend on Network Size |

Table 1. *Differences between types of blockchains. Adapted from: [66]*

### 2.3.3 Blockchain Security Issues and Challenges

Blockchain like any other piece of technology in the world, is vulnerable to cyber attacks. The vulnerabilities depend on the type of blockchain, the consensus method used and the underlying technological platform. Public blockchains (mostly cryptocurrencies) are less secure than private blockchains, the difference is the limited and restricted access that the latter have [94] . In this section the security problems are categorized in concept issues which are directly related to blockchain technology itself and implementation problems which are more related to how blockchain is deployed.

### Concept Issues

Blockchain suffers from different security core issues which depend on the consensus mechanism and type of blockchain, some of these vulnerabilities are described below:

**51% attacks:** When PoW consensus mechanism is used, the success rate of mining a block depends on the work done by the miner so when 51% of the network is under control of one entity then that entity would be able to control the block verifying transaction and modify the transaction data [95] [96].

**Fork Problems**: Ledger networks may get split and replicated into parallel fork chains, creating ambiguity between child blocks for parallel parent fork chains. This replication may be susceptible to several attacks in parallel fork chains [97].

**Double Spending**: This attack refers to the same consumer using the same cryptocurrency multiple times for transactions. In blockchains using PoW it's easy to deploy a double spending attack because the attacker can exploit the time between two transactions' initiation and confirmation [98].

**Selfish Mining**: Miners with bad intentions and more computing power can refuse to publish their mined blocks until they have accumulated a long chain of blocks without competitors, this new chain becomes the largest and thus is accepted as the main chain causing the blocks mined before to be rejected [94].

### Implementation Issues

Some of the vulnerabilities in the blockchain implementations are in the underlying technology used, for example, in private blockchains the Hyperledger Fabric framework is mostly used which offers "a number of Software Development Kits (SDKs) for different programming languages, including Node.js and Java SDKs. Node.js has a set of security flaws that make it susceptible to a remote DoS attack and can be exploited to execute code remotely resulting in a DNS rebinding vulnerability [97]".

Another set of problems lie in the Docker containers used to run the Fabric chaincode. Even though this chaincode is isolated from the endorsing peer process, there is still a risk that malicious chaincode is written into the container. Remote Access Trojan malware can be used to initiate access into an organization's network from which the attackers can then scan and attack other systems [97].

Lastly, there is a problem of maintaining the confidentiality of transactions on public blockchains due to the "peer-to-peer network, this protocol allows all users to get involved in updating (i.e., initiating a new transaction) and maintaining (i.e., mining a new block) the shared database (i.e., blockchain). Therefore, all users have access to every transaction's detail, such as the sender, recipient and amount[80]". This can become a concern when anonymity is needed.

Different general vulnerabilities have been identified in the private implementations of the blockchain technology. The main identified risks by [97] are:

Poor network design: Ledgers may be susceptible to DoS or transaction spamming if proper identity management is not set for private blockchain.

Poor cryptography: private blockchains' security depends on cryptographic keys for encryption of the information to ensure maximum security, however, if these keys are not handled properly, the security can get compromised.

| **Main Security problems in blockchain** | | |
|---|---|---|
| **Attack/ Vulnerability** | **Description** | **Weaknesses of Technology** |
| 51% attacks | Control over 50% hash power from total hash power | Fundamental problem of blockchain system. POW base system more vulnerable |
| Fork Problems | A blockchain is divided into two different ones. It is up to the miners to decide which one they use | Fundamental problem of blockchain system. |
| Double Spending | User uses the same cryptocurrency for different payments | Fundamental problem of blockchain protocol |
| Selfish Mining | Attacker not broadcasting blocks immediately on the network and publishing blocks on selective time | Fundamental problem of blockchain. PoW based blockchains more vulnerable. |

| | | |
|---|---|---|
| Programming language vulnerabilities | Hyperledger uses SDKs for different programming languages which are vulnerable to remote code execution | Blockchain implementation |
| Insufficient chaincode sandboxing | Malicious chaincode can be written to isolated Docker container. | Blockchain implementation. |
| Mishandling of cryptographic keys | If keys are not stored or maintained properly it could lead to compromise or disclosure leading to fraudulent transactions | Blockchain implementation issue |

Table 2. *Blockchain security issues.* Source:Author

## 2.4 Service Supply Chain and Blockchain

The use of blockchain in SC management and the issues that it helps solving are being explored by different organizations and researchers. The most influential factor driving interest in blockchain within SC management is trust [63]. Ensuring that the information is reliable is crucial and blockchain would provide improved visibility which provides an auditable trace of the footprint of a product or piece of data [70]; for example, it can be used for identity management in order to know who is doing what, when and where. It helps providing symmetric information to all; monitoring the performance throughout the SC without the possibility of making any changes by any of the parties as once the information is in the ledger, it is immutable [99]. This would ensure that all members in the supply chain can obtain verified information which enhances collaborative partnerships [16].

Blockchain technology can be used as well to monitor the location and movement while ensuring the integrity and confidentiality of the information across the SC, for example instead of storing SC data such as inventory of critical hardware or time, date of patch for critical software, critical SC data is stored in the distributed escrow of the blockchain, which maintains time stamped data blocks that cannot be modified retroactively, which increases the trustworthiness and integrity of the data [100].

Some of the areas in which blockchain would be most valuable for SC management, would be in extended visibility and traceability [63] as it would provide :

- An increase in transparency of a systems' machine state integrity and the ability to audit the system and network throughout the entire life cycle.
- Software, hardware, and firmware records that are archived and tracked in an im-

mutable distributed ledger.

- Increased accessibility and visibility of SC data that enhances and expedites inter-vendor cooperation.
- Component/information traceability throughout the entire life cycle of the system to assure efficient and secure processes.
- Improved monitoring of critical cyber assets, both hardware and software, which facilitates auditing, security and compliance [100].

There are however barriers to the extensive implementation of blockchain technology in SC, [101] reviews the major barriers to widely applying the technology in industries and services alike.

- Current economic winners may resist change out of the fear of losing revenue models, it is understandable that certain intermediaries in the SC would be removed which would create resistance to its implementation [102]. "Other supply chain actors might not want the total transparency provided by a blockchain" [63].
- Additionally, there are issues in its scalability capacity, "usage of Distributed Ledger Technology relies heavily on the designated block-size of the transmitted information, speed of transmission through the network, the underlying proof-of-work protocol and the verification of miner information on every node which are limited compared to existing methods of transactions like Visa or Paypal"[103]. This issue is addressed by [104] who proposes the blockchain-indexed storage (BIS) to provide scalable and secure IoT-enabled SC traceability.
- Another issue mentioned is sending wrong information through the blockchain which would lead to an incorrigible mistake due to the immutable nature of the technology [105].
- Blockchains suffer from severe technology challenges [101]. "Often the protocol updates cannot roll seamlessly due to the presence of a software bug, or inconsistencies in the blocks of a particular user that may compel the entire blockchain to split unnecessarily" [106].
- Another extensive problem in blockchains can occur with the loss of cryptographic keys. If any user loses the set of public/private keys, they are stolen, or the user expires, then those blocks cannot be retrieved [107].
- The cost of implementing or participating in a blockchain system may also be an issue, due to the technical and specialized expertise required for participation [108].
- The energy consumption seems to be another problem as blockchains using the PoW consensus method demand big amounts to maintain the network [109]. The main reason for this high energy consumption is that all nodes in the network are trying to find the same solution but only one will succeed [89]. In the case of permissioned

blockchains using PoA consensus method the consumption increases along with the complexity, for example Practical Byzantine Fault Tolerance (PBFT) consensus overhead increases quadratically with the number of nodes in the network making it highly sensitive to the network size [88].

- Data retrieval is a mentioned problem due to inefficiency. Both retrieval by full node or lightweight mode present issues with efficient data retrieval and privacy, respectively [19].
- Privacy leakage is a known issue in public blockchains such as Bitcoin where due to its nature attackers can link the transactions back to a common user despite the widespread use of ephemeral wallets [110].
- Another important consideration pertains to the application of the current privacy laws of different regions to decentralized systems such as a public blockchain as traditionally these laws consider a single entity as the controller of both the collected data and their service provider relationships [111].
- Blockchain integration with existing supply chain technological solutions and ERP tools built with conventional technology stack can generate additional risks and cost when introduced in the SC operations [59].

Despite the meaningful advances in the last years, blockchain applications regarding operations and SC management are still in their infancy [112] [43]. Little is known about the role of blockchain in terms of operations' traceability, as well in areas such as e-commerce, agriculture, public services, etc . Most of the research of blockchain is focused on developed and highly industrialized countries like USA, China, UK among others. It would be beneficial for research to explore the use of cutting edge technologies in developing countries to further expand the knowledge base [20].

# 3. Research Methodology

## 3.1 Introduction

In the first sections of this document the research problem is presented to guide the rest of the research, next the theoretical background was detailed to provide a better understanding of the blockchain technology and its potential relationship with service supply chain. From the previous literature review it was possible to identify a research gap in risk management in service supply chains as well as the information risks that affect it. At the same time blockchain technology is explored as a possibility to reduce the risk to information in the SSC domain. This research tries to fill this mentioned gap by providing a framework that future researchers and implementations can base their work on. This following chapter details the research design and data collection process and analysis for this thesis.

## 3.2 Case Study Design and Selection

A case study is "an empirical inquiry that investigates a contemporary phenomenon within its real- life context, especially when the boundaries between phenomenon and context are not clearly evident [113]." Another definition is "a case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organization). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental control or manipulation is used [114]." From the previous definitions, it is clear that case studies analyze real life problems, and the information sources can come from different entities, this process is referred to as triangulation and ultimately improves the analysis by contrasting different perspectives [115].

Furthermore, a case study can be classified as a single case study or multiple case study. The main difference between these two is that the latter uses different sources to understand the differences and similarities between the cases [116] which makes the collected data more reliable [117].

Empirical research, or in this case a case study can either be classified as *Inductive* or *Deductive*, in the former the researcher first observes the topic of interest, identifies patterns from which hypothesis are formulated and then relates them to the existing theory or formulates new ones, whereas the latter starts with existing theory, from which hypothesis are formulated to finally make the observations which will either confirm or reject the hypothesis [115]l. A deductive case study seems to fit the best to the current research as the existing theory on SSC and blockchain is analyzed, different hypotheses are formulated and then different professionals with different backgrounds are interviewed to understand their problems and perspective on whether blockchain is an effective and potential solution.

## 3.3 Data collection Procedure

Data collection is "the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes [118]". In this case data collection will be done by means of qualitative research.

One of the main tools of qualitative research are interviews which are used to explore the views, experiences, beliefs, and/or motivations of individuals on specific matters and are therefore most appropriate where little is already known about the study phenomenon or where detailed insights are required from individual participants [119]. In this particular case, semi-structured interviews will be conducted to a set of experts in the relevant fields, the questions included in this interview comprised mostly open-ended questions to get a more detailed answer and additional details relevant to the topic.

In total 12 respondents participated in the interview, most of them have had extensive experience with blockchain implementations in supply chain environments and come from different countries such as Costa Rica, Estonia and India. Another perspective was obtained by interviewing supply chain experts who provided insights of their concerns, needs, and their knowledge of blockchain technology.

**Document Review**

Document review refers to the exhaustive analysis of existing documents relevant to the research, such as papers, theses, grey literature and white literature. Documents can be used to corroborate evidence from other sources as well as to gather background information on the case study topic [113]. From the document review, the theoretical basis for the research is constructed and different study cases are identified.

In the current research, the document review set the background theory about multiple topics of the research such as supply chain and the different types of SC, the challenges of information sharing in SSC and the definition of blockchain, its types, drivers and barriers to the application in SSC. It is important to note that as mentioned by the literature, not much has been researched in service supply chain so contemporary works on this subject were difficult to find, for this reason the interviews will be used to measure the current state of the methods used for information sharing among other aspects in service supply chains to better characterize them and will either validate what the literature said or provide new information which is useful in either case.

### Interviews

The most common types of interviews used in qualitative data collection can be divided into 3 types: structured, semi-structured, and unstructured. In this case a semi-structured interview method is used. The semi-structured interviews consist of a set of questions that are used as a guide during the interview but at the same time allow the interviewer or interviewee to diverge to provide a more detailed answer or idea [120][119].

The interviewed professionals need to have good knowledge in supply chain, blockchain, cybersecurity and cryptography fields to gather information about the current state of information sharing practices in SSC (in the case of SSC professionals) and their knowledge of the possible application of blockchain in service supply environments and its effectiveness in preserving the confidentiality and integrity of the information shared in the service supply chain to ensure this, a set of questions evaluating their knowledge in these topics is included at the beginning of the interview.

The reasons for using this method are twofold, first to document the characteristics of SSC and methods used by professionals when sharing information second, there are few people familiar with the technology and few organizations in the world who have implemented it in service supply chains [63][61][121][99].

### Sample Selection for Qualitative Interviews

In order to obtain quality information from the surveys it is necessary to carefully create an expert profile to identify the professionals that would suit best to the research, taking into consideration their areas of expertise, educational level, and work experience.

Since it’s impossible to separate blockchain technology from cryptography then consulting with experts with at least some basic understanding of cryptography is necessary to make sure all the technical aspects from the encryption and security perspective of the technology are considered in the framework.

Given that the application of blockchain technology is being evaluated in service supply chain then it is necessary to consult with experts that are actively involved in blockchain implementations in SC and/or supply chain to obtain their insights.

At the same time, cybersecurity experts have the responsibility of protecting the cyber assets of organizations such as the shared information, so their point of view would be beneficial to the research.

The required experts need to have:

- Knowledge of one of the previously mentioned fields.
- Minimum of a Masters' degree in cybersecurity, a computer science/IT related field or supply chain/logistics.
- Work experience in cryptography, blockchain, cybersecurity or supply chain/logistics.
- Preferably some research in their respective fields.

### 3.3.1 Interviewees profiles

The following table provides a summary of the profile of the interviewed professionals that collaborated with the research.

| **Interviewees profiles** | | | | |
|---|---|---|---|---|
| **Name** | **Education** | **Work Experience** | **Years of experience** | **Country** |
| Chibuzor Udokwu | PhD student | Logistikum retail | 2 years | Estonia |
| Gabriel Silva | PhD | University professor at ITCR | 10+ years | Costa Rica |
| Alexandr Kormiltsyn | PhD | Senior Software Engineer at Arvato | 5+ years | Estonia |
| Silver Kelk | MBA | Business Development & Partnerships at Guardtime | 2+ years | Estonia |
| Alexander Norta | PhD | Lecturer/associate professor at Taltech | 7+ years | Estonia |
| Shabahat M. Ayubi | BSc | Coalescence technologies | 2+ years | India |

| | | | | |
|---|---|---|---|---|
| Otto Mora | MBA | Blockchain consultant at EY | 2+ years | Costa Rica |
| Xavier Fernandez | BSc | Co-founder of EOS Costa Rica and blockchain developer | 3+ years | Costa Rica |
| Andres Gomez | PhD | Blockchain Security Researcher at EOSIO CR | 1+ year | Costa Rica |
| Edwin Iraheta | MBA | Digital Innovation Manager at GBM | 2+ years | Costa Rica |
| Peeter Sepp | MSc | Supply Delivery Manager at Ericsson | 1+ year | Estonia |
| Riivo Pilvik | MSc | Co-founder and CIO of SkillBill.io | 3 years | Estonia |

Table 3. *Interviewees profiles* Source:Author

### 3.3.2 Analysis Procedures

In this stage, the collected data is analyzed to understand what has actually happened in the studied case and patterns in the information are sought to gain insights on the details of the research [115], this process of analysis is called thematic analysis and the 6 steps approach described by [122] are used in this research, which are as follows:

1. The first step is transcribing the data from the interviews, this will allow familiarization with the collected information.
2. Code generation: important text is highlighted and included into codes to categorize it using NVIVO tool.
3. Once the codes are created then they are categorized into themes
4. The identified themes are revised and crosschecked against the existing codes to ensure the validness of the identified themes.
5. After a careful review of the themes is performed, the remaining ones are defined and named, at this point, more analysis is done to further improve the themes.
6. The final step is to produce the report containing the interpretation of the analysis that relate the best to the research questions, themes and literature.

### 3.3.3 Validity Procedures

The validity of the results “denotes the trustworthiness of the results and to what extent the results are not biased by the researchers’ subjective point of view” [115]. In [123] describes the criteria used to ensure trustworthiness in qualitative research projects which are credibility, transferability, dependability, and confirmability.

Credibility references to the fact that the research measures what was actually intended, in other words, it refers to how congruent the results are with the real world. Credibility can be assured by a set of provisions taken during the research such as:

- Triangulation which refers to the use of different sources of information, in this case, different interviewees perspectives tend to strengthen the study.
- Tactics to ensure honesty in the answers obtained from the interviewees need to be implemented when contacting potential respondents. This is done by building rapport and ensuring the interviewee is really willing to be part of the research and will provide information freely.
- Iterative questioning is a way to ensure that the answers received are honest and as detailed as possible as the researcher returns to previous questions in case clarification or more information is needed.

The above mentioned measures were taken when contacting and carrying out the research to make it credible to other researchers and peers.

Transferability refers in this case to the extent to which the results or findings of a study can be applied to other situations or populations, in this case a detailed description of the case study has been provided so that any other investigator can apply the same methodology.

Dependability refers to the reproducibility and repeatability of the study. By using the same research methods with the same participants, the same results are obtained. In this case clear and detailed procedures are presented for any other researcher that would like to apply them and should obtain similar finding. Finally, confirmability means that the results and findings belong to the real view and reality perceptions of the respondents and are far from the subjective view of the researcher.

### 3.3.4 Summary

This chapter describes in detail the research methodology taken for this research, initially describing how the research questions were obtained, what is a case study and why it is suitable for this particular case and the different methods used to collect, analyze and validate the information obtained.

# 4. Results

## 4.1 Introduction

This chapter details the background of the case of this research, provides a detailed profile of the subjects participating in the research, as well as the analysis of the collected information which was analyzed using the NVIVO software.

## 4.2 Case and Subject Description

The case for this research are service supply chains. The services industry continues to grow around the world contributing millions to countries' economies. Service supply chains are different in nature to the conventional SC due to the IHIP attributes mentioned in Chapter 2 it is hard to standardize tools or solutions in these kind of environments to help with the risk management as most of the processes are very different due to the customers and personnel providing them.

SC suffer from great dangers such as cyber attacks resulting in data breaches, reputational damage, customer attrition and supply chain attacks and service supply chains are not the exception. SSC heavily relies on information as a source of competitive advantage allowing managers to make informed business decisions, therefore real time sharing of quality information is crucial and especially important when dealing with risks as a coordinated risk management approach taken by all the parties in the SSC can considerably improve the success of the mitigation and control strategies.

Information systems have an essential role in achieving better performance and efficiency in SSC, some of the benefits the implementation of IT systems have brought include improvements in customer service, efficiency, information quality and agility, however, certain IT-related issues were also introduced such as poor information visibility and multiple tools which also function as hindrances to integration, at the same time the attacks surface was substantially expanded.

IT systems have without doubt made easier information sharing, however, as reviewed in the literature, information management is becoming increasingly difficult for organizations as the volume and speed of information created and transferred is only increasing while the types of attacks received are becoming more sophisticated and in some cases the tools used to share information are not upgraded accordingly and do not meet the speed and security characteristics required in the SSC.

Lack of trust between members of the SC is one of the most mentioned issues in the SSC, confidence in the perceived security of SC information systems determines the willingness of an enterprise to share confidential information with other parties [45]. Another source of distrust when sharing information is the risk of competitors accessing the information or 3rd parties maliciously modifying it, this lack of visibility and control in the integrity of the information has a deep effect on the processes.

Currently there are different frameworks specially designed to preserve the integrity and confidentiality of the information being exchanged in the traditional SC, however, none of these tools have been successfully applied to the SSC environment. New frameworks have been developed, however, they still present certain deficiencies when applied to SSC, as they have not been generalized, applied in a real scenario or is still in its prototype stage.

## 4.3 Presentation of Findings

This section details the results of the collected information obtained and analyzed from the interviews. As mentioned in the previous chapter the interview method consists of open-ended questions that elicit a detailed and profound answer from the respondent, the questions are divided into different themes, the first one collects general information about the respondent's background to certify that they have experience with the research topic and their answers are valid for the research questions. Such interviews were recorded and transcribed to later feed an analysis software, NVIVO in this particular case, where different words and phrases were coded to create identifiable themes.

### 4.3.1 Respondents Description

This section describes the respondents who agreed to be interviewed. The main bulk of interviewees belong to organizations who have or had experience with blockchain implementations, at the same time professionals in supply chain were interviewed to reflect their knowledge, reality of the current situation, and understanding of how blockchain can help or not their daily activities. Interviewees were selected from two main areas, professionals working or involved with an Estonian organization and professionals from Costa Rica implementing, studying or observing blockchain technology. The interviewed experts' descriptions are listed in Appendix 1.

From the interviewees descriptions and their answers, it is evident that they have wide experience with blockchain and the surrounding technologies and concepts such as cryptography, cybersecurity, and supply chain implementations. Most of them have over 2 years of experience in their respective fields, making them more than sufficiently competent to make meaningful contributions to the research.

### 4.3.2 Understanding the current methods of information sharing in SSC

Understanding how the information is shared between different parties in the service supply chain is crucial to understand the role that blockchain could play as well as the benefits that it could provide. Hence, it is necessary to address the question "what are the tools or platforms used in service industry to share information with stakeholders and customers?"

In the service environment the used tools can be classified into different groups, one of them being proprietary systems; rest APIs, web services. The second group consists of file sharing systems, either designed by the own organization or existing ones such as Dropbox, Google Drive, where in many cases important information is shared in an Excel or CSV file, EDI systems are rare nowadays however some respondents mentioned them, ERP systems were widely mentioned as being one of the main tools, among which Oracle and SAP can be mentioned.

Lastly common information exchange tools such as emails and SMS are used to share information quickly. Among the mentioned data storage tools used are the common SQL servers, MongoDB, MariaDB postgressql, and Cloudera.

**Trustworthiness of current tools**

The main purpose of this section is to answer the question "How trustworthy are the currently used tools/platforms to keep the confidentiality and integrity of the information stored and shared in the SSC?

The experts answers were pretty divided in this case due to variety of experiences, some of them had dealt with very basic, insecure and misconfigured tools such as simple email communication, csv or excel files used for exchanging information, such was the case of Riivo who said: "*Rather bad or low if you look at all of these emails and excels and stuff, so it's basically doesn't have any any, let's say security almost at all. So it's yeah* *it's good that if they have, let's say secure email or or let's say SSL at least, but that's about it. So I would say no, no security.*", while others agreed that the current tools possess the proper security measures such as encryption making them secure as long as they are properly configured as stated by Andres "*They provide some security services like for example Cloudera allows encrypting of the stored information and there are others that as I know don't have that encryption service, that service is optional, you need to know how to configure and create security improvements around these platforms.*".

On the other hand other experts mentioned that the problems are not in the trustworthiness of the tools but they rather rely in the scalability and control of the tools as mentioned by Silver "*it's it's usually not the trustworthiness that creates problems for them. It's rather the scalability or just that kind of, I don't know. Ability to transform them to make more modern and so on where they are seeing weakness is not in the trustworthiness*".

Another essential issue mentioned that would be hard to overcome with the current tools is the insider threat, as Alexander Norta mentioned "*just because you have a tool that's very nice, yeah? But it's I'm afraid it doesn't mean a heck of a lot because. Just just because you use some sort of securing tool. Uh, there's still the entire social attack spectrum available to still hack into somebody's systems, whether you have a tool or not.*", which according to Andres blockchain can overcome with improved access control. "*In that sense blockchain does have an advantage, as an access control system blockchain is great, this allows users to identify themselves without having to send everything that huge amount of information to a centralized organization and then that same identification is more trustworthy to be used to login into a lot of companies.*"

### 4.3.3 Aspects of Current Systems To Be Improved

**Integrability**: Most of the respondents declared that an organization can use multiple tools which makes their integration with one another complicated and unfeasible in some cases due to different used standards as indicated by Alexandr Kormiltsyn: "*one company uses some internal standard like in healthcare when we established the data sharing with external laboratory company laboratory provider like currently Synlab. I remember that Synlab at that time used to [unintelligible]. And so our polyclinic used this Estonian internal standard, it doesn't have specific name just doesn't respond to [unintelligible]. Yeah, and so this was a problem because different standards and different analysis pools and so on*". In many cases the experts mentioned that the current used tools are specifically designed by the organization and were categorized as "rather closed systems".

**Data integrity/heterogeneity**: Some of the respondents mentioned that due to the multiple tools used to share and store information in organizations, it is hard for a certain participant in the process to be sure that the data is correct along all the sources and points of transit as stated by Chibuzor, the recording of the information "*is a manual process so it takes time and there might be data loss*", the same was mentioned about data getting lost and/or duplicated, even in very standardized systems such as ERPs, there is a lot of data duplicity, this problem is enlarged when information is shared with external parties as in most supply chain environments as pointed out by Otto "*information duplicity, since a lot of organizations have multiple systems even from within, like a CSR, ERP, etc, even if they use an ERP which standardizes a lot, there is a lot of data duplicity so it is hard to say: This is the official source of this piece of data*"

**Centralization**: As stated by Andres currently "*you need to trust in the organization that owns the database and blindly trust that they are handling it the right way, privately and transparently which in most cases it's not possible to know, the main issue is that people are providing information to these centralized organizations however most of the cases the information ends up on the internet*". All the participants need to trust that the entity managing the information is doing this in the appropriate way, taking into consideration the CIA triad to ensure that the information does not end in the wrong hands. On the other hand, many respondents mentioned that such trust is not impossible to achieve, however, many tools would need to be implemented and integrated to achieve the same results that blockchain would be able to provide in a more integrated and sound solution. **Configuration:** It was often mentioned misconfiguration to be the reason of data breaches or loss of information as stated by Shabahat "*[A vendor] will set up your hardware, infrastructure and even when they go for the cloud infrastructure due to inexperience or do any such reason they have not configured properly. It's not secure like even when you're putting it up on AWS. It's a very basic mistake which almost every new person into the whole cloud computing domain does is they open all the ports and they open the database port and they forget to add a password to that.*"

### 4.3.4 Blockchain implementation obstacles

Most of the respondents identified and agreed with the following obstacles to a successful blockchain implementation.

**Lack of understanding**: A recurrent obstacle is the lack of understanding by the organization and management of the capabilities of blockchain and the possible uses it can be given to their respective use cases, many organizations want to use it because it is trending. As mentioned by Silver "*what is hard is actually that kind of first architecture or understanding why are you using blockchain? That kind of understanding what blockchain* *can do and what they can't do. What consequences will emerge once you implement it in your business process? And so on. I think that knowledge is often missing from the companies that have that kind of high level willingness or interest in the blockchain technologies*". Another issue is that blockchain is usually associated with Bitcoin which still has a negative perception among people, deterring them from trusting the technology. Additionally organizations have privacy and confidentiality concerns and are unwilling to upload very sensitive information to the blockchain and to have their identity disclosed even though there are ways to overcome this issue by using Zero Knowledge Proof (ZKP).

**Lack of regulation**: The lack of regulation in certain countries deters organizations from implementing blockchain as mentioned by Andres "*lack of regulation on the matter, many organizations feel there is no legal or regulatory stability to use blockchain*". This is the case for Costa Rica where there are no clear guidelines for the technology. Another important factor mentioned by the reviewed literature is the conflicting nature of blockchain with certain legislations such as GDPR and privacy protecting laws, since these are by nature based on centralized systems. It was mentioned although that these issues can be overcome by not submitting any highly sensitive information to the blockchain, instead hash it and upload the hash.

**Cost**: Cost is one of the main barriers to implementing blockchain in enterprises as mentioned by the reviewed literature. Respondents primarily dealing with implementations of blockchain in real life environments had disagreeing views on the cost of the technology. Most of the respondents mentioned that the cost is considerable for a small company, as mentioned by Otto "*It is expensive, the proof of concept is around $100,000 for 3 months*". The cost is of such magnitude in part due to the lack of developers working with blockchain languages, one mentioned alternative is to hire developers expert in other areas, however, they need to be trained in the new programming languages which takes time and resources. Some organizations are working on implementing SaaS to reduce the cost of blockchain technology. On the other hand other respondents mentioned that there are open source options that would considerably reduce the cost of the implementation.

**Integrability**: Due to the multiple tools used by organizations to share their information, it is hard to create a blockchain tools that can fit to all. It was widely mentioned that when implementing blockchain, organizations are not willing to dispose of all the current tools and the investment they represent to implement blockchain, instead they expect the technology to integrate with all the current tools, as mentioned by Shabahat "*so that was one of the core issues which came across the solutions was either you integrate with this software and the number of software can go in hundreds, maybe thousands. So you have to have that many integrations with the core software which [they] are building. Or you* *can ask all of them to come on your software which is running on a blockchain.*".

**Resistance to change**: Organizations are used to the current centralization paradigm and tools, therefore, are usually adverse to the risks that implementing a new technology can cause. This can be caused by the unwillingness from organizations to give up the control of the data, fear of losing the business model by being displaced, such is the case of middlemen who would lose the competitive advantage due to the transparency provided, as well as technocratic considerations as organizations don't know the real social and business implications of implementing the technology. Alexander Norta mentioned: "*My experience is that big organizations do not want to use blockchain technology because they are all entangled and geared up in this centrally planning centrally controlling top down paradigm. Yeah. They have massive middle management bureaucracy. Very often blockchain technology, really it's a killer for most of what large organizations do*"

**Added value is not justified**: It was mentioned that for some organizations the added value provided by the transparency and security is perceived as lower compared to the risk and/or investments required to start working with blockchain. This was the experience of Riivo who said: "*Was there kind of some added value about this kind of transparency and security? It was kind of perceived less than compared to the, let's say, risk or let's say, the huge investments, they need to undertake in order to start using some kind of blockchain approaches, especially if they don't have this kind of their, let's say, existing systems. What to integrate with this*"

**Agreeing on initial consensus**: Edwin Iraheta stated that the biggest issue he has faced is "*how to generate the initial consensus for the first block. This is the obstacle for some initial pilots because the parts cannot reach a consensus on the consensus method to use for the blockchain*" as not all of them trust and feel comfortable with it.

**Scalability**: The respondents were very divided when evaluating the scalability of current blockchain platforms and consensus methods. Some mentioned this is no longer a problem since there are ways to overcome the issue such as just submitting hashes to the blockchain to ensure the integrity of the original data as stated by Silver "*we only work with hashes, we are not dealing with the data itself [in the blockchain], only the hashes. And we use the SHA-256, so it's 256 bits just to approve.*". Due to block size limitations it is not very efficient to store documents on the blockchain as pointed by Xavier "*[...]in EOS IO the protocol we work with each block has a max of 1 MB so a new block is created every 500 ms but there is a max space per block so you need to manage the resources so that all the parties have their resource quota and there is no DoS, but in short it is very expensive and inefficient to save docs on the blockchain, there are projects that do it, in EOSio there are* *customers that saved the docs on the blockchain but we save the hashes on the blockchain and the files on IPFS so there is a timestamp of the document, and hashes, in IPFS*". Some other platforms were mentioned that are capable of processing millions of transactions per second, such as EOSIO and the solution developed by Guardtime.

It is important to note that certain implementation obstacles mentioned in the literature were not present in the responses, several of the interviewees agreed that the high energy consumption of blockchain is no longer a problem unless PoW is used, as there are other alternatives such as private or permissioned blockchains which can be deployed using the platform EOSIO, which Xavier claims to be really efficient where the parties are validated in different ways other than PoW for example and the scalability is no longer an issue as it is capable of processing millions of transactions per second.

### 4.3.5 Capacity of blockchain to preserve integrity and confidentiality

This section answers the question "What is the level of security of blockchain to preserve the confidentiality and integrity of information?" The main reason of this question is to clarify the privacy concerns of some people who mention that blockchains can preserve integrity but not the confidentiality of the shared information.

It was declared by the respondents that there are indeed privacy issues with blockchain, especially when dealing with a permissionless blockchain implementation where anyone can access the information that is stored in the blockchain. This is a problem as organizations sometimes deal with information that gives them a competitive advantage over others, if this data were to fall into the wrong hands, their business would be negatively affected.

The experts mentioned that there is a way of overcoming such problems, such as Hyperledger Besu mentioned by Andres "*where each node has a private database where the transactions are sent, the hash of the data is what is sent to the blockchain*". Andres also mentioned that "*current cryptographic algorithms are not ready for quantum computing.*" What most of the experts could agree on is that very sensitive information should not be stored in the blockchain, instead a hash can be uploaded to guarantee the integrity, provide traceability and at the same time yield some level of confidentiality.

### 4.3.6 Blockchain Benefits

Among the main benefits mentioned by the respondents are:

**Data traceability**: According to the interviewees, blockchain provides a clear trace of what has happened to the information shared across multiple parties in the process, this is especially important in cross-organizational processes when 3rd parties are involved.

**Automation**: Certain processes can be automated with smart contracts such as payments, invoice generation, etc, which results in cost reduction, and higher process velocities which translate in better service level.

**Increased trust between SSC partners**: By providing wide visibility and decentralizing the control of the data, the trust among the parties is increased. It is important to note that not in all cases this decentralization is wanted or needed as pointed by the experts, for which case a private blockchain can be used where organizations still retain a certain degree of control on the participation.

**Auditability**: This was a widely mentioned benefit which depends a lot on the business case, however, is a direct result of the traceability and transparency provided by blockchain as processes can be audited more easily and results can be better trusted.

**Improved security**: The redundancy provided by blockchain was mentioned by different respondents as a clear benefit when being attacked by ransomware or malware. Another important security feature is the encryption provided by the technology which prevents a restricted third party to access the data. Blockchain is an integral tool that secures information from the data source point and during the exchange.

**Dispute handling**: Due to the transparency and traceability of information, it is easy to solve or simplify any disputes originating from a service discomfort or problem, this reduces the cost of litigations.

### 4.3.7 Requirements to implement blockchain

This section seeks to answer the question: What are the basic requirements to implement blockchain in a service organizations' process? Most of the respondents agreed that one of the primary conditions that need to be met to consider blockchain is having cross-organizational processes where trust between the parties is critical for business development and risk management and complex business rules are utilized, as stated by Otto "*[blockchain is useful] when there is a process involving several organizations sharing information with complex business rules*". It is pointless for a single enterprise or two that simply want to have an additional layer of security to implement blockchain as the cost is too high for the added value and other cheaper solutions are available.

Another requirement is having the technological know-how and maturity in the organization for the implementation. It's very important to train all the staff on the implications of the implementation both from the social and technological aspects. Chibuzor also mentions that "*regulation in the organization to implement blockchain*" is needed as well as in the country to regulate what can be done with the technology.

One additional requirement for blockchain implementation as mentioned by Gabriel is having a *data governance and security information policy that sets the way on what needs to be secured and how*, without these the used tools might not have the effect or the level of security needed.

### 4.3.8 Blockchain type and consensus method

This section covers the question: What is the best type of blockchain and consensus method for a service environment? Such question was asked to detect a tendency of the type of blockchain implementation that is more frequent and understand if any of the types is not used due to technological or regulatory issues.

In regard to the type of blockchain to be used, most experts agreed on a permissioned implementation as it provides control on the participants, consensus method, regulatory compliance in the case of dealing with very sensitive information and a certain level of internal privacy that eases the enterprise's privacy concerns as stated by Silver "*It has a clear owner, usually who is developing and providing this often as a service or that kind of you have some counterpart to turn to*".

Some experts such as Otto mentioned that "*to start a private one, but the real benefits of cost reduction are in public blockchains, the more nodes in the network the more secure and [increased] hashing power. The private one is only to get organizations to familiarize themselves with the technology.*" This same view of improved security and extra benefits is shared by Alexander Norta who believes that the public blockchain is more secure as it has been exposed to the public, being subject of all kinds of attacks and survived.

As for the consensus method as expected, the answers considerably varied as the experts had experience and preference to different ones, however the names that were mentioned are Proof of Authority and Proof of Stake. It is important to note also that most of the respondents didn't mentioned PoW as they all agreed that it has scalability and efficiency issues and consumes enormous amounts of energy.

## 4.4 Framework

### 4.4.1 Promote understanding of the technology

Lack of understanding of the technology is one of the main reasons why implementations have problems from the beginning so it is essential for organizations to set up a committee formed by professionals of different backgrounds who can, review and investigate the potential use and benefits of implementing blockchain in the organization can have, if such professionals are not available then it would be wise to consider training the staff in the technology both before, during and after the implementation.

Another fundamental role should be taken by universities to promote the understanding of the technology by providing seminars, and creating technical guidelines and/or manuals of the technology with the intention of disseminating knowledge and facilitating implementations. By better understanding the technology, enterprises could better foresee if the technology represents some kind of added value to the business.

### 4.4.2 Review of local regulations

The current regulations or the lack of thereof doesn't promote the use of blockchain technology much less when it the potential use is to store sensible or important information. This situation varies from country to country, there are some more advanced and prepared nations in terms of legislation, national frameworks, and/or guidelines for the use of blockchain, however, some others like the example of Costa Rica where the government has taken no positive stance towards the technology, greatly reducing the number of options for its implementation. Each government must set out policies and guidelines for the use and application of blockchain in private environments.

Another important aspect noted from the reviewed use cases is to avoid submitting important and highly sensible information to the blockchain due to privacy concerns and conflicting laws and regulations such as the GDPR. Instead, it is recommended to hash the document or a piece of data and upload this hash to the blockchain, this way it can be later ensured whether the information has been modified or not.

### 4.4.3 Evaluate Integrability and Interoperability

The capability of systems to integrate and operate with each other is key to having an efficient and highly functional information sharing system between different parties of the supply chain. As mentioned before, organizations implement multiple tools and platforms for information sharing depending on their business needs, which needs to be considered when thinking about a blockchain implementation. The capability of integrating blockchain with the existing ecosystems might not be possible due to the difficulty and extra overhead caused by the technology, so it is important for enterprises to evaluate their current systems, the real need of using blockchain and if the same goals cannot be obtained with the current tools

### 4.4.4 Run Pilot Projects

It was noted from the interviews that many organizations who successfully manage to implement blockchain technology start with a small pilot project to start learning what the technology is about and its capabilities. It was mentioned in some cases such pilots are run in private blockchains to slowly introduce the organization to the implications of the technology and how it works and once they trust it, then the implementation can be carried over to a public blockchain where the biggest security benefits are. This type of approach greatly reduces the financial and operational risks in case of failure.

### 4.4.5 Increased Collaboration

In a regular SSC environment collaboration is needed for normal business operations, this shouldn't be different when implementing new technologies. It is recommended that organizations sharing information with each other should set cross-organizational information security policies and standards that define and standardize the level of confidentiality, availability, and integrity of the information being exchanged as well as their update frequency and communication methods. This collaboration must take into consideration all the members in the supply chain, their capabilities, maturity, and investment capabilities, so that realistic standards can be adopted by everyone. It is vital to include blockchain experts in these collaborations to make implementations more robust from the technical and administrative perspective. By adding this level of collaboration, the trust issue among the members is further addressed beyond the technological level as there is a global framework for securely sharing information.

## 4.5 Summary

This chapter went over the background of the case to provide a better understanding of the results that were going to follow. Then the process of analyzing and extracting the useful information from the interviews is explained, as well as the specifics of the type of interview and how the answers were obtained with as much detail as possible.

A special section was dedicated to describing the participants in the interview to give credibility and validity of their answers, and finally the findings are detailed by dividing them into sections which all answer a specific research question as detailed in Chapter 3.

# 5. Conclusions and Future Work

The supply chain is becoming more interconnected and digitized worldwide, making them more information reliant, especially the service supply chain. The handling of the produced information is essential for the efficient and cost effective functioning of the supply chain.

Currently due to distrust between parties in the supply chain, information doesn't flow as fast, accurately and to all the entities that need it causing inefficiency, increased cost and higher risk threats. The current research aims at understanding how information is shared in the service supply chain and the role that blockchain can have in preserving the integrity and confidentiality of the information shared between the different parties to minimize the risk to information.

The results allowed to better understand how information is currently shared, which tools are used, how trustworthy they are at preserving the integrity and confidentiality of the information and their current problems as seen by the experts. The currently used tools are widely used by most organizations nowadays, ERPs, cloud-based systems, EDI systems, databases, and more informal ways such as file sharing via emails or file sharing systems. The opinion was quite divided when it comes to the trustworthiness of these tools, as the proper configuration of the tools plays a major role on how capable they are at securing the information's integrity and confidentiality. It was pointed out that multiple tools are needed to achieve the level of protection blockchain provide from end to end.

Difficulty with the integration of multiple tools/software/platforms required by organizations to carry out daily business activities was a mentioned problem within the results, in many cases due to the lack of integration between the platforms, many organizations experience a lack of homogeneity in the data shared across the supply chain as it is hard to maintain the integrity and avoid duplicity of the data with current tools, even when ERPs are used which are mentioned to standardize information input and storage.

A distributed ledger such as blockchain can be effective at keeping a clear traceable record of how the information has been handled making it easier to audit which has the potential of increasing the trust between the SC partners. Disputes are not uncommon given the nature of services, therefore, blockchain could play a fundamental role in solving such disputes cost effectively and in a reduced time compared to how they are currently handled.

Blockchain is a technology characterized by its decentralization, immutability, transparency, and visibility, which make it a useful tool for securing the integrity and confidentiality of shared information in a SSC. However, its successful adoption depends on the maturity of the organization, the use case, the understanding of the technology by the enterprise among other specific measures that need to be adopted/improved. Consequently, the guidelines presented at the end of chapter 4 are presented for the adoption of blockchain technology in a SSC environment. Such guidelines are summarized in table 4.

Figure 6 shows the interaction (dependency) between different obstacles to the implementation of blockchain. It's important to note that many of the obstacles stem from the lack of understanding of the technology which directly impacts the lack of regulations in certain countries, the resistance to change within the organizations as they don't fully understand what the technology is capable of.

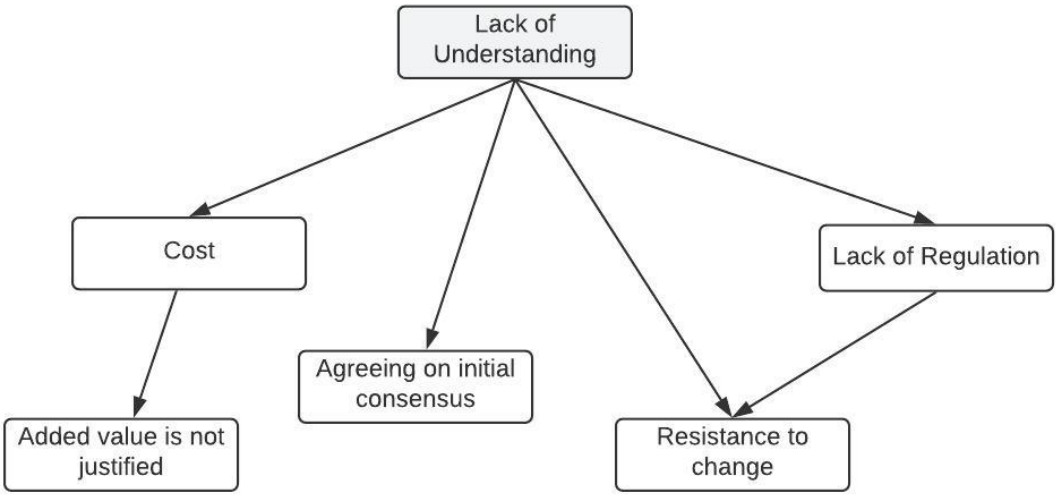


Figure 6. *Blockchain obstacle implementation dependency graph* Source:Author

Cost is also influenced by lack of knowledge in the technology by professionals as reduced number of people are capable of working with it, elevating the cost of the ones who can, this at the same time influences the added value which in some cases due to the high cost is not justified with the benefits it would bring to the enterprise. Lastly, agreeing on the initial consensus is also difficult if the knowledge of how it works is not clear or nonexistent.

While the reduced number of interviewees limits the generalizability, this thesis has been able to show based on qualitative research that blockchain is a tool to consider for information sharing in SSC given the right circumstances and set to create a framework for its adoption in the SSC environment to protect the shared information between the different parties. The technology needs to be more understood by the public and enterprises in order to be easily adopted.

| **Framework for blockchain implementation in Service Supply Chains** | | | |
|---|---|---|---|
| **Recommendation** | **Descriptions** | **Parties** | **Requirements** |
| Promoting understand of technology | Educate organizations, public institutions and general public about the technology | Universities, experts | Events, conferences, forums |
| Review of local regulations | Public and governmental institutions need to create or improve laws and regulations for the technology | Government, Experts | Private-public collaboration |
| Integrability and interoperability | Evaluation by organizations of the possibility of integration with existing blockchain platforms before implementation | Enterprises | Knowledge of technology, regulations |
| Run a Pilot Projects | Start implementation on a small scale to reduce economic risk and better understand the technology | Experts and stakeholders | Funds, expertise, infrastructure |
| Increased Collaboration | Organizations must collaborate to set cross-organizational information security policies and standards and ensure these are properly communicated. | Organizations, experts, stakeholders | Expertise, infrastructure, regulations |

Table 4. *Summary of recommendations.* Source:Author

## 5.1 Impact/Implication

This research reviewed the current state of information sharing in service supply chains and the risks involved in this process. Due to their nature, service supply chains cannot be treated equally to the traditional supply chain, so blockchain was considered as a potential tool to help reduce the information sharing risks. The study tried to shed some light on how information is currently shared as mentioned directly by the interviewed experts and contrasting this with the literature and how these systems or methods could be further improved using blockchain.

The use of blockchain to protect information shared between different entities is further explored to understand how effective it would be at tackling the issues, its applicability to SSC, among other important considerations and then developing the guidelines for the adoption of blockchain in a SSC environment.

## 5.2 Future Work

Further studies are required to better understand how blockchain can benefit and be better implemented in service supply chain environments successfully. Supply chain experts need to better understand the implications of the technology in their businesses from the privacy, social, and technical aspects and how it can coexist with the current systems and entities in the SSC. This is vital to develop better information sharing policies that can be implemented by all the members of the chain.

This research was carried out with experts located in 3 different parts of the world to try and reflect different realities and perspectives, however, the findings cannot be considered transferable to other nations not considered in the study. It is possible that by following this same research methodology in other countries with different levels of development would yield different results thus further research in such environments is encouraged to have a wider view of the existing problems.

This research focused on developing a framework for the implementation of blockchain in service supply chain environments, however, the technical aspects were not considered. New research should look with more detail the technical aspects of blockchain and the systems used in SSC

# Bibliography

[1] Mercedes Delgado and Karen Mills. “The Supply Chain Economy and the Future of Good Jobs in America”. In: (2018). URL: https://hbr.org/2018/03/the-supply-chain-economy-and-the-future-of-good-jobs-in-america.

[2] Mehrdokht Pournader, Andrew Kach, and Srinivas Talluri. “A Review of the Existing and Emerging Topics in the Supply Chain Risk Management Literature”. In: *Decision Sciences* (2020).

[3] Jyri Vilko and Teemu Santonen. “Managing Supply Chain Service Value Risks: Organizational Roles and Social Connections”. In: (2017).

[4] Jyri Vilko and Paavo Ritala. “Service supply chain risk management”. In: *Operations and Supply Chain Management* 7.3 (2014), pp. 139–140.

[5] Thi Huong Tran and Sebastian Kummer. “Service Supply Chain Risk Management: Distinctions from Manufacturing”. In: *Innovations and Strategies for Logistics and Supply Chains: Technologies, Business Models and Risk Management. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 20*. Berlin: epubli GmbH. 2015, pp. 503–532.

[6] Weihua Liu et al. “Service supply chain management: a behavioral operations perspective”. In: *Modern Supply Chain Research and Applications* 1.1 (2019), pp. 28–53. ISSN: 2631-3871. DOI: 10.1108/mscra-01-2019-0003.

[7] Abhijeet Ghadge et al. “Managing cyber risk in supply chains: A review and research agenda”. In: *Supply Chain Management: An International Journal* (2019).

[8] Tonmoy Toufic Choudhury et al. “A systematic literature review on the service supply chain: research agenda and future research directions”. In: *Production Planning and Control* 31.16 (2020), pp. 1363–1384. ISSN: 13665871. DOI: 10.1080/09537287.2019.1709132. URL: https://doi.org/10.1080/09537287.2019.1709132.

[9] Thi Thanh Huong Tran, Paul Childerhouse, and Eric Deakins. “Supply chain information sharing: Challenges and risk mitigation strategies”. In: *Journal of Manufacturing Technology Management* 27.8 (2016), pp. 1102–1126. ISSN: 1741038X. DOI: 10.1108/JMTM-03-2016-0033.

[10] Imran Ali, Sev Nagalingam, and Bruce Gurd. "Building resilience in SMEs of perishable product supply chains: enablers, barriers and risks". In: *Production Planning & Control* 28.15 (2017), pp. 1236–1250.

[11] Yanjun Zuo and Wen-Chen Hu. "Trust-based information risk management in a supply chain network". In: *International Journal of Information Systems and Supply Chain Management (IJISSCM)* 2.3 (2009), pp. 19–34.

[12] Shipra Pandey et al. "Cyber security risks in globalized supply chains: Conceptual framework". In: *Journal of Global Operations and Strategic Sourcing* (2020).

[13] Patricia J Daugherty et al. "Is collaboration paying off for firms?" In: *Business horizons* 49.1 (2006), pp. 61–70.

[14] Evelyne Vanpoucke, Ann Vereecke, and Steve Muylle. "Leveraging the impact of supply chain integration through information technology". In: *International Journal of Operations & Production Management* (2017).

[15] "Design of a software architecture supporting business-to-government information sharing to improve public safety and security: Combining business rules, Events and blockchain technology". In: *Journal of Intelligent Information Systems* 52.3 (2019), pp. 595–618. ISSN: 15737675. DOI: 10.1007/s10844-017-0478-z.

[16] Paul Kengfai Wan, Lizhen Huang, and Halvor Holtskog. "Blockchain-Enabled Information Sharing within a Supply Chain: A Systematic Literature Review". In: *IEEE Access* 8 (2020), pp. 49645–49656. ISSN: 21693536. DOI: 10.1109/ACCESS.2020.2980142.

[17] Diana Fischer-Preßler et al. "Information technology and risk management in supply chains". In: *International Journal of Physical Distribution and Logistics Management* 50.2 (2020), pp. 233–254. ISSN: 09600035. DOI: 10.1108/IJPDLM-04-2019-0119.

[18] Ramji Nagariya, Divesh Kumar, and Ishwar Kumar. "Service supply chain: from bibliometric analysis to content analysis, current research trends and future research directions". In: *Benchmarking: An International Journal* (2020).

[19] Hanqing Wu et al. "Data management in supply chain using blockchain: Challenges and a case study". In: *2019 28th International Conference on Computer Communication and Networks (ICCCN)*. IEEE. 2019, pp. 1–8.

[20] Samuel Fosso Wamba and Maciel M Queiroz. *Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities*. 2020.

[21] Helen Peck. "Reconciling supply chain vulnerability, risk and supply chain management". In: *International Journal of Logistics: Research and Applications* 9.2 (2006), pp. 127–142.

[22] Grafton Elliot Smith et al. "A critical balance: collaboration and security in the IT-enabled supply chain". In: *International journal of production research* 45.11 (2007), pp. 2595–2613.

[23] Uta Jüttner, Helen Peck, and Martin Christopher. "Supply chain risk management: outlining an agenda for future research". In: *International Journal of Logistics: Research and Applications* 6.4 (2003), pp. 197–210.

[24] Andreas Wieland and Carl Marcus Wallenburg. "Dealing with supply chain risks". In: *International Journal of Physical Distribution & Logistics Management* (2012).

[25] William Ho et al. "Supply chain risk management: a literature review". In: *International Journal of Production Research* 53.16 (2015), pp. 5031–5069.

[26] Richard Wilding et al. "Supply chain risk management: a new methodology for a systematic literature review". In: *Supply Chain Management: An International Journal* (2012).

[27] Joao Pires Ribeiro and Ana Barbosa-Povoa. "Supply Chain Resilience: Definitions and quantitative modelling approaches–A literature review". In: *Computers & Industrial Engineering* 115 (2018), pp. 109–122.

[28] Md Maruf Hossan Chowdhury and Mohammed Quaddus. "Supply chain readiness, response and recovery for resilience". In: *Supply Chain Management: An International Journal* (2016).

[29] Simin Davoudi et al. "Resilience: a bridging concept or a dead end?"Reframing" resilience: challenges for planning theory and practice interacting traps: resilience assessment of a pasture management system in Northern Afghanistan urban resilience: what does it mean in planning practice? Resilience as a useful concept for climate change adaptation? The politics of resilience for planning: a cautionary note: edited by Simin Davoudi and Libby Porter". In: *Planning theory & practice* 13.2 (2012), pp. 299–333.

[30] Sandor Boyson. "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems". In: *Technovation* 34.7 (2014), pp. 342–353.

[31] Theresa Sobb, Benjamin Turnbull, and Nour Moustafa. "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions". In: *Electronics (Switzerland)* 9.11 (2020), pp. 1–31. ISSN: 20799292. DOI: 10.3390/electronics9111864.

[32] Robert E Spekman and Edward W Davis. "Risky business: expanding the discussion on risk and the extended enterprise". In: *International Journal of Physical Distribution & Logistics Management* (2004).

[33] Yulan Wang et al. "Service supply chain management: A review of operational models". In: *European Journal of Operational Research* 247.3 (2015), pp. 685–698. ISSN: 03772217. DOI: 10.1016/j.ejor.2015.05.053. URL: http://dx.doi.org/10.1016/j.ejor.2015.05.053.

[34] Tuncdan Baltacioglu et al. "A new framework for service supply chains". In: *The Service Industries Journal* 27.2 (2007), pp. 105–124.

[35] Lisa M Ellram, Wendy L Tate, and Corey Billington. "Understanding and managing the services supply chain". In: *Journal of Supply Chain Management* 40.3 (2004), pp. 17–32.

[36] Scott E Sampson and Martin Spring. "Customer roles in service supply chains and opportunities for innovation". In: *Journal of Supply Chain Management* 48.4 (2012), pp. 30–50.

[37] Zahra Lotfi et al. "Information sharing in supply chain management". In: *Procedia Technology* 11 (2013), pp. 298–304.

[38] Claudia Colicchia, Alessandro Creazza, and David A. Menachof. "Managing cyber and information risks in supply chains: insights from an exploratory analysis". In: *Supply Chain Management* 24.2 (Mar. 2019), pp. 215–240. ISSN: 13598546. DOI: 10.1108/SCM-09-2017-0289.

[39] Umang Soni, Vipul Jain, and Sameer Kumar. "Measuring supply chain resilience using a deterministic modeling approach". In: *Computers & Industrial Engineering* 74 (2014), pp. 11–25.

[40] Yi Tao, Loo Hay Lee, and Ek Peng Chew. "Quantifying the effect of sharing information in a supply chain facing supply disruptions". In: *Asia-Pacific Journal of Operational Research* 33.04 (2016), p. 1650029.

[41] Mohd Nishat Faisal, DEVINDER KUMAR Banwet, and Ravi Shankar. "Information risks management in supply chains: an assessment and mitigation framework". In: *Journal of Enterprise Information Management* (2007).

[42] Irfan Ulhaq et al. "Information Security Risks in Supply Chain Management:" in: *International Journal of Information Systems and Engineering* 4.2 (2016), pp. 58–68. ISSN: 22893709. DOI: 10.24924/ijise/2016.11/v4.iss2/58.68.

[43] Mustufa Haider Abidi et al. "Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process". In: *International Journal of Intelligent Systems* 36.1 (2021), pp. 260–290.

[44] Bharat Bhargava, Rohit Ranchal, and Lotfi Ben Othmane. “Secure information sharing in digital supply chains”. In: *Proceedings of the 2013 3rd IEEE International Advance Computing Conference, IACC 2013* (2013), pp. 1636–1640. DOI: 10.1109/IAdCC.2013.6514473.

[45] Chen Zhang and Suhong Li. “Securing Information Sharing in Internet-Based Supply Chain Management Systems”. In: *Computer Information Systems Working Papers* 46 (June 2006).

[46] Prashant R Nair, Venkitaswamy Raju, and S P Anbudayashankar. “Overview of Information Technology tools for Supply Chain Management”. In: *CSI Comm* 33.9 (2009), pp. 20–27.

[47] Sari Uusipaavalniemi, Jari Juga, and Maqsood Sandhu. “Information Sharing in Service Supply Chain”. In: *Handbook On Business Information Systems*. World Scientific, 2010, pp. 717–735.

[48] Richard A Bettis and Vijay Mahajan. “Risk/return performance of diversified firms”. In: *Management Science* 31.7 (1985), pp. 785–799.

[49] Inga S Baird and Howard Thomas. “What is risk anyway? Using and measuring risk in strategic management”. In: *Risk, strategy, and management* 5 (1990), pp. 21–54.

[50] Pablo JG Guerra and DA Sepulveda Estay. “An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains”. In: *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE. 2018, pp. 61–65.

[51] Kaspersky. *What is Cyber Security? | Definition, Types, and User Protection | Kaspersky*. URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (visited on 12/29/2020).

[52] Symantec. “Internet Security Threat Report VOLUME 21, February 2019”. In: *Network Security* 21.February (2019), p. 61. ISSN: 13534858. URL: http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947.

[53] Jake Williams. *What You Need to Know About the SolarWinds Supply-Chain Attack*. 2020. URL: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/ (visited on 12/29/2020).

[54] US Department of Justice. *Department of Justice Statement on Solarwinds Update | OPA | Department of Justice*. URL: https://www.justice.gov/opa/pr/department-justice-statement-solarwinds-update (visited on 01/21/2021).

[55] Verizon. *Data Breach Investigations Report*. Tech. rep. 2020.

[56] Sudeep Tanwar, Karan Parekh, and Richard Evans. “Blockchain-based electronic healthcare record system for healthcare 4.0 applications”. In: *Journal of Information Security and Applications* 50 (2020), p. 102407.

[57] Yan Chen and Cristiano Bellavitis. “Blockchain disruption and decentralized finance: The rise of decentralized business models”. In: *Journal of Business Venturing Insights* 13 (2020), e00151.

[58] Elie Bouri et al. “Bitcoin, gold, and commodities as safe havens for stocks: New insight through wavelet analysis”. In: *The Quarterly Review of Economics and Finance* 77 (2020), pp. 156–164.

[59] By David Shorthouse and Michael Xie. “Blockchain Designed for Supply Chains : Guardtime Supply Chain Framework”. In: April (2020).

[60] “Blockchain Technology Overview - National Institute of Standards and Technology Internal Report 8202”. In: *NIST Interagency/Internal Report* (2018), pp. 1–57. URL: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

[61] Davor Dujak and Domagoj Sajter. *Blockchain Applications in Supply Chain*. Springer International Publishing, 2019, pp. 21–46. ISBN: 9783319916682. DOI: 10.1007/978-3-319-91668-2_2. URL: http://dx.doi.org/10.1007/978-3-319-91668-2%7B%5C_%7D2.

[62] S Cheng, B Zeng, and YZ Huang. “Research on application model of blockchain technology in distributed electricity market”. In: *IOP Conference Series: Earth and Environmental Science*. Vol. 93. 1. IOP Publishing. 2017, p. 012065.

[63] Yingli Wang, Jeong Hugh Han, and Paul Beynon-Davies. “Understanding blockchain technology for future supply chains: a systematic literature review and research agenda”. In: *Supply Chain Management* 24.1 (2019), pp. 62–84. ISSN: 13598546. DOI: 10.1108/SCM-03-2018-0148.

[64] Curtis Miles. *Blockchain security: What keeps your transaction data safe?* 2017. URL: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/ (visited on 12/29/2020).

[65] PricewaterhouseCoopers. “Blockchain – an opportunity for energy producers and consumers?” In: *Pwc.Com* (2016), pp. 1–45. URL: www.pwc.com/utilities.

[66] Zibin Zheng et al. “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”. In: *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017* (2017), pp. 557–564. DOI: 10.1109/BigDataCongress.2017.85.

[67] METI. “Survey on Blockchain Technologies and Related Services FY2015 Report”. In: *Nomura Research Institute* March (2016). URL: http://www.meti.go.jp/english/press/2016/pdf/0531%7B%5C_%7D01f.pdf.

[68] Manlu Liu, Kean Wu, and Jennifer Jie Xu. “How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain”. In: *Current Issues in Auditing* 13.2 (2019), A19–A29.

[69] Nick Szabo. “Smart contracts”. In: (1996). DOI: 10.4324/9780429029172-2. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[70] Yingli Wang et al. “Making sense of blockchain technology: How will it transform supply chains?” In: *International Journal of Production Economics* 211 (2019), pp. 221–236.

[71] Zainab Alhadhrami et al. “Introducing blockchains for healthcare”. In: *2017 international conference on electrical and computing technologies and applications (ICECTA)*. IEEE. 2017, pp. 1–4.

[72] Vitalik Buterin. *On Public and Private Blockchains | Ethereum Foundation Blog*. 2015. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (visited on 01/11/2021).

[73] Elli Androulaki et al. “Hyperledger fabric: a distributed operating system for permissioned blockchains”. In: *Proceedings of the thirteenth EuroSys conference*. 2018, pp. 1–15.

[74] Asma Khatoon et al. “Blockchain in energy efficiency: Potential applications and benefits”. In: *Energies* 12.17 (2019), p. 3317.

[75] Bhabendu Kumar Mohanta et al. “Blockchain technology: A survey on applications and security privacy challenges”. In: *Internet of Things* 8 (2019), p. 100107.

[76] Hyperledger Project. “Fabric whitepaper”. In: (2020), p. 2. URL: https://www.hyperledger.org/wp-content/uploads/2020/03/hyperledger%7B%5C_%7Dfabric%7B%5C_%7Dwhitepaper.pdf.

[77] Martin Valenta and Philipp Sandner. "Comparison of Ethereum, Hyperledger Fabric and Corda". In: *Frankfurt School Blockchain Center* June (2017), p. 8. URL: www.fs-blockchain.decontact@fs-blockchain.dewww.twitter.com/fsblockchainwww.facebook.de/fsblockchain%7B%5C%%7D0Ahttps://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6.

[78] Chinmay Saraf and Siddharth Sabadra. "Blockchain platforms: A compendium". In: *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*. IEEE. 2018, pp. 1–6.

[79] Richard Gendal Brown et al. "Corda: an introduction". In: *R3 CEV, August* 1 (2016), p. 15.

[80] Yunsen Wang and Alexander Kogan. "Designing confidentiality-preserving Blockchain-based transaction processing systems". In: *International Journal of Accounting Information Systems* 30 (2018), pp. 1–18.

[81] Marko Vukolić. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication". In: *International workshop on open problems in network security*. Springer. 2015, pp. 112–125.

[82] Visa. *Small Business Retail | Visa*. URL: https://africa.visa.com/visa-everywhere/small-business-tools/retail.html (visited on 04/21/2021).

[83] Murat Kuzlu et al. "Performance analysis of a hyperledger fabric blockchain framework: throughput, latency and scalability". In: *2019 IEEE international conference on blockchain (Blockchain)*. IEEE. 2019, pp. 536–540.

[84] Yue Hao et al. "Performance analysis of consensus algorithm in private blockchain". In: *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE. 2018, pp. 280–285.

[85] Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong. "Performance analysis of private blockchain platforms in varying workloads". In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE. 2017, pp. 1–6.

[86] Eosio. *#AskBlockone: What are the benefits of the EOSIO infrastructure? – EOSIO*. URL: https://eos.io/news/askblockone-what-are-the-benefits-of-the-eosio-infrastructure/ (visited on 04/21/2021).

[87] Digital Transaction Limited. *ParallelChain™ sets new blockchain speed record at over 144,000 transactions per second with no compromise | by Digital Transaction Team | Digital Transaction Blog | Medium*. URL: https://medium.com/digital-transaction-limited/parallelchain-sets-

new-blockchain-speed-record-at-over-144-000-tps-with-no-compromise-a900474218ba (visited on 04/21/2021).

[88] Johannes Sedlmeir et al. "The energy consumption of blockchain technology: beyond myth". In: *Business & Information Systems Engineering* 62.6 (2020), pp. 599–608.

[89] Eshani Ghosh and Baisakhi Das. "A study on the issue of blockchain's energy consumption". In: *International Ethical Hacking Conference*. Springer. 2019, pp. 63–75.

[90] Alex Hern. *Bitcoin mining consumes more electricity a year than Ireland | Bitcoin | The Guardian*. 2017. URL: https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland (visited on 01/19/2021).

[91] JD Bruce. "The mini-blockchain scheme". In: *White paper* (2014).

[92] Ittay Eyal et al. "Bitcoin-ng: A scalable blockchain protocol". In: *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*. 2016, pp. 45–59.

[93] Soohyeong Kim, Yongseok Kwon, and Sunghyun Cho. "A survey of scalability solutions on blockchain". In: *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE. 2018, pp. 1204–1207.

[94] Abdurrashid Ibrahim Sanka et al. "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research". In: *Computer Communications* (2021).

[95] Iuon-Chang Lin and Tzu-Chun Liao. "A survey of blockchain security issues and challenges." In: *IJ Network Security* 19.5 (2017), pp. 653–659.

[96] Dipankar Dasgupta, John M Shrein, and Kishor Datta Gupta. "A survey of blockchain from security perspective". In: *Journal of Banking and Financial Technology* 3.1 (2019), pp. 1–17.

[97] Huru Hasanova et al. "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures". In: *International Journal of Network Management* 29.2 (2019), pp. 1–36. ISSN: 10991190. DOI: 10.1002/nem.2060.

[98] Xiaoqi Li et al. "A survey on the security of blockchain systems". In: *Future Generation Computer Systems* 107 (2020), pp. 841–853.

[99] Nir Kshetri. "1 Blockchain's roles in meeting key supply chain management objectives". In: *International Journal of Information Management*. Vol. 39. Elsevier Ltd, Apr. 2018, pp. 80–89. DOI: 10.1016/j.ijinfomgt.2017.12.005.

[100] Michael Mylrea and Sri Nikhil Gupta Gourisetti. “Blockchain for supply chain cybersecurity, optimization and compliance”. In: *2018 Resilience Week (RWS)*. IEEE. 2018, pp. 70–76.

[101] Baidyanath Biswas and R. Gupta. “Analysis of barriers to implement blockchain in industry and service sectors”. In: *Computers and Industrial Engineering* 136.July (2019), pp. 225–241. ISSN: 03608352. DOI: `10.1016/j.cie.2019.07.005`. URL: `https://doi.org/10.1016/j.cie.2019.07.005`.

[102] Paul Michelman. “Seeing beyond the blockchain hype”. In: *MIT Sloan Management Review* 58.4 (2017), p. 17.

[103] Arthur Gervais et al. “On the security and performance of proof of work blockchains”. In: *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016, pp. 3–16.

[104] Shi-Syun Kuo and Wei-Tsung Su. “A Blockchain-Indexed Storage supporting Scalable Data Integrity in Supply Chain Traceability”. In: *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*. IEEE. 2020, pp. 348–349.

[105] Christian Beer and Beat Weber. “Bitcoin–the promise and limits of private innovation in monetary and payment systems”. In: *Monetary Policy and the Economy. Q* 4 (2015), pp. 53–66.

[106] Aviv Zohar. “Bitcoin: under the hood”. In: *Communications of the ACM* 58.9 (2015), pp. 104–113.

[107] Stefan Seebacher and Maria Maleshkova. “A model-driven approach for the description of blockchain business networks”. In: *Proceedings of the 51st Hawaii International Conference on System Sciences*. 2018.

[108] Dhiren Patel, Jay Bothra, and Vasudev Patel. “Blockchain exhumed”. In: *2017 ISEA Asia Security and Privacy (ISEASP)*. IEEE. 2017, pp. 1–12.

[109] Nir Kshetri. “Will blockchain emerge as a tool to break the poverty chain in the Global South?” In: *Third World Quarterly* 38.8 (2017), pp. 1710–1732.

[110] Ryan Henry, Amir Herzberg, and Aniket Kate. “Blockchain access privacy: Challenges and directions”. In: *IEEE Security & Privacy* 16.4 (2018), pp. 38–45.

[111] Pritesh Shah et al. “Blockchain Technology : Data Privacy Issues and Potential Mitigation Strategies”. In: *Practical Law* (2019).

[112] Francesco Longo et al. “Blockchain-enabled supply chain: An experimental study”. In: *Computers and Industrial Engineering* 136.July (2019), pp. 57–69. ISSN: 03608352. DOI: `10.1016/j.cie.2019.07.026`. URL: `https://doi.org/10.1016/j.cie.2019.07.026`.

[113] Robert K Yin et al. “Design and methods”. In: *Case study research* 3 (2003).

[114] Izak Benbasat, David K Goldstein, and Melissa Mead. “The case research strategy in studies of information systems”. In: *MIS quarterly* (1987), pp. 369–386.

[115] Per Runeson et al. *Case Study Research In Software Engineering*. John Wiley & Sons, 2012, pp. 1–241. ISBN: 9781118104354. URL: http://www.worldcat.org/title/case-study-research-in-software-engineering-guidelines-and-examples/oclc/828789615%7B%5C&%7Dreferer=brief%7B%5C_%7Dresults.

[116] Johanna Gustafsson. *Single case studies vs. multiple case studies: A comparative study*. 2017.

[117] Pamela Baxter, Susan Jack, et al. “Qualitative case study methodology: Study design and implementation for novice researchers”. In: *The qualitative report* 13.4 (2008), pp. 544–559.

[118] Syed Muhammad. “Methods of data collection”. In: *Basic Guidelines for Research: An Introductory Approach for All Disciplines*. Vol. 1. Mohammad Javed Rahim Book Zone Publication, 2016. Chap. 9, pp. 202–276. ISBN: 978-984-33-9565-8.

[119] Paul Gill et al. “Methods of data collection in qualitative research: interviews and focus groups”. In: *British dental journal* 204.6 (2008), pp. 291–295.

[120] Carol Grbich. *Qualitative research in health: An introduction*. sage, 1998.

[121] Sherree Decovny. “Benchmark Survey : Blockchain In Supply Chain: Edging Toward Higher Visibility”. In: *Chain Business Insights* May (2017), pp. 1–10.

[122] Gareth Terry et al. “Thematic analysis”. In: *The Sage handbook of qualitative research in psychology* (2017), pp. 17–37.

[123] Andrew K Shenton. “Strategies for ensuring trustworthiness in qualitative research projects”. In: *Education for information* 22.2 (2004), pp. 63–75.

# Appendices

# Appendix 1 - Interviewee list

1. Chibuzor Udokwu is a PhD student at Taltech, he is a member of the blockchain group and has done extensive research on the subject, at the same time he works in Logistikum retail, an organization investigating possible blockchain uses.
2. Gabriel Silva is the coordinator of the cybersecurity specialization in a University in Costa Rica with ample knowledge in Blockchain and cybersecurity with 10 years of experience in the subject.
3. Alexandr Kormiltsyn is a PhD student at Taltech, has published several papers on the uses of Blockchain, has worked 5 years in Arvato, organization that also investigates uses of Blockchain technology.
4. Silver Kelk has worked 2 years for Guardtime a leading company who has implemented blockchain solutions in multiple public and private organizations, including companies in supply chain.
5. Alexander Norta has 7 years of experience being an associate professor, lecturer, Phd students' supervisor, Blockchain group manager in Taltech, and has countless of publications dealing with blockchain.
6. Shabahat M. Ayubi has years of experience working at organizations which implement Blockchain, currently has his own startup called Coalescense Technologies which has Blockchain implementations as part of their revenue model.
7. Otto Mora has worked for 2 years at EY, organization that investigates and implements Blockchain solutions to all sorts of customers around the globe. He has 2 years in this organization and has been part and coordinator in several Blockchain projects, some of which have been in supply chain environments.
8. Xavier Fernandez is co-founder of EOS Costa Rica, an organization that has experimented with different use cases for EOSIO blockchain technology, especially for enterprise use, among such cases are supply chain implementations. Xavier is the tech lead of blockchain implementations.
9. Andres Gomez has worked for almost 2 years as security researcher at EOS Costa Rica, he has a PhD from Frankfurt University in cybersecurity and extensively re-

searches the security aspects behind Blockchain. Andres has been part of blockchain implementations in supply chain environments in EOS CR.

10. Edwin Iraheta works in the Research and Development department in GBM dealing directly with blockchain implementations for their customers. He has vast experience as an IT administrator, providing an important perspective on how information is stored and shared in organizations.
11. Peeter Sepp work as a Supply Delivery Manager in Ericsson, he has over 4 years of experience in logistics and supply chain.
12. Riivo Pilvik is co-founder and CIO of SkillBill.io a company that focuses on building digital solutions for businesses, as such Riivo has been involved in the investigation of blockchain applications for supply chain environments.

# Appendix 2 - Interview Questions

General Questions

1. What is your name?
2. In which company do you currently work at?
3. How long have you worked in the previously mentioned company?
4. How well you know about the below topics: Cryptography, Blockchain,Cybersecurity, Blockchain applied to finances, Blockchain applied to services?
5. What is your company's stance towards blockchain?

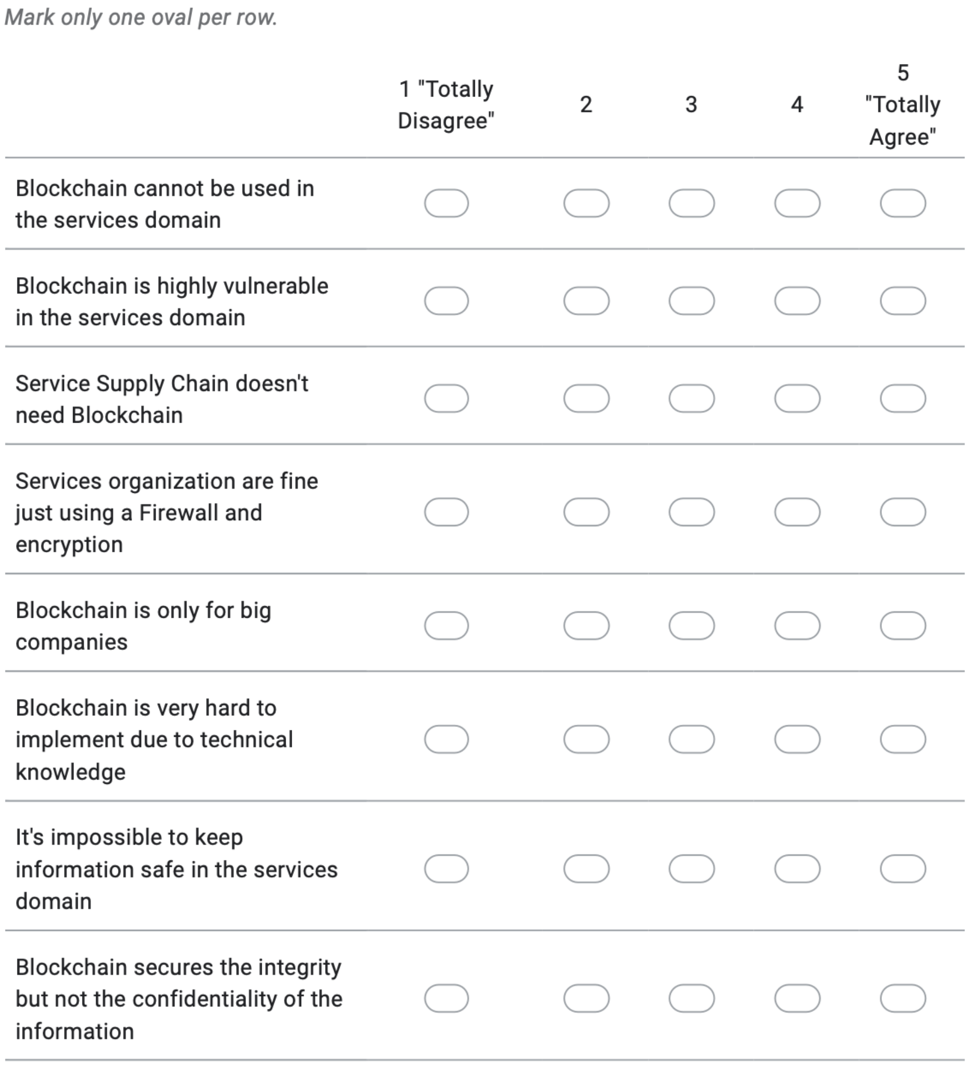
Understanding Current used tools for information sharing

1. Based on your experience, which tools or platforms are used in service industry to share information with stakeholders and customers?
2. How trustworthy do you think these tools or platforms are to safe keep the privacy and confidentiality of the shared information?
3. What tools or platforms would you recommend a services organization to use to safe keep the confidentiality and privacy of the shared information?
4. In your opinion, which are the main problems that the current used methods to share information have?
5. Please rank from 1 to 6 which of the following is more important to you or your organization in terms of information handling:Data Privacy,Data confidentiality, Fast access to information, Auditable trail of information, Availability of information, Integrity of the information

Blockchain Knowledge

1. Do you know what is Blockchain?
2. Can you explain in your own words what Blockchain is?
3. Do you know in which industries is Blockchain being applied?
4. What are the main benefits of using Blockchain in an organization?
5. What are the main advantages of Blockchain in a services organization?
6. What are the two most important advantages of Blockchain to Service Supply Chain?

7. For which activities would you use Blockchain the most?
8. Do you think that Blockchain is secure enough to maintain the confidentiality of information?
9. In your opinion what are the biggest obstacles to implementing Blockchain in Service Supply domain?
10. Do you think that Blockchain can be used in Service Supply Chain?
11. Can you give the reason of why your previous answer?
12. What are the main benefits of using Blockchain in a Service Supply Chain?
13. What are the main obstacles of using Blockchain in a Service Supply Chain?
14. Are you aware of any organization providing services that uses Blockchain?
15. Would you recommend a services organization to use Blockchain to share information?
16. What are the main requirements for this organization to implement Blockchain?
17. Can you please indicate your level of agreement with the below phrases using a scale of 1 to 5 where 1 is "Totally Disagree" and 5 is "Totally Agree"?



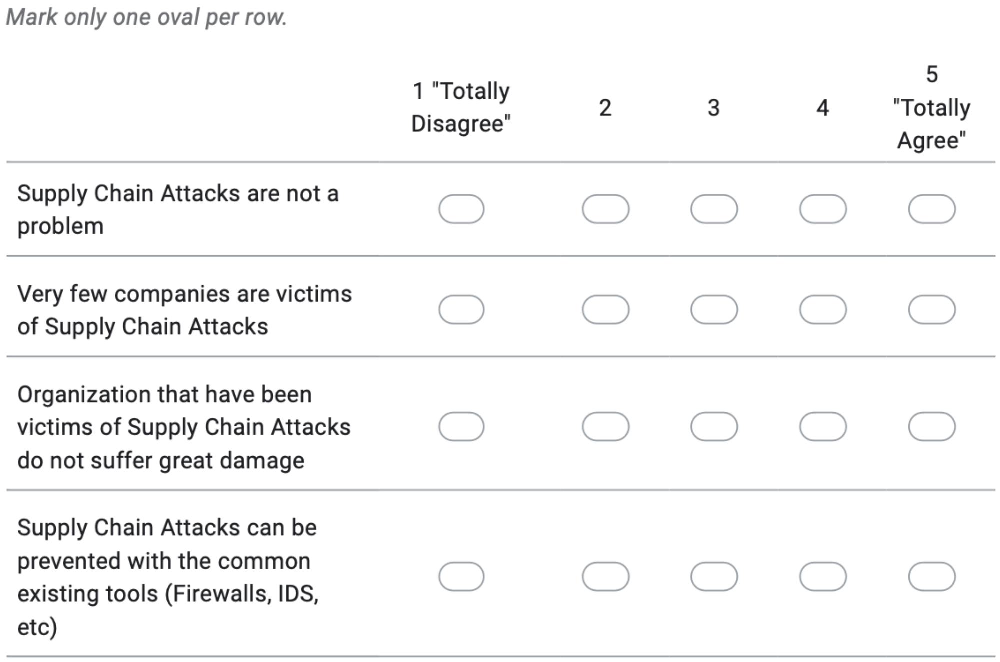
*Mark only one oval per row.*

| | 1 "Totally Disagree" | 2 | 3 | 4 | 5 "Totally Agree" |
|---|---|---|---|---|---|
| Blockchain cannot be used in the services domain | ○ | ○ | ○ | ○ | ○ |
| Blockchain is highly vulnerable in the services domain | ○ | ○ | ○ | ○ | ○ |
| Service Supply Chain doesn't need Blockchain | ○ | ○ | ○ | ○ | ○ |
| Services organization are fine just using a Firewall and encryption | ○ | ○ | ○ | ○ | ○ |
| Blockchain is only for big companies | ○ | ○ | ○ | ○ | ○ |
| Blockchain is very hard to implement due to technical knowledge | ○ | ○ | ○ | ○ | ○ |
| It's impossible to keep information safe in the services domain | ○ | ○ | ○ | ○ | ○ |
| Blockchain secures the integrity but not the confidentiality of the information | ○ | ○ | ○ | ○ | ○ |

18. Which type of Blockchain do you think suits better a services environment?
19. Can you please explain why the previous choice?
20. Which consensus method would you use with the previous type of blockchain and why?
21. Do you think that the cryptography model used in Blockchain is safe enough for information sharing?

Understanding Risks

1. In your opinion, what are the biggest cyber risks that services organizations face?
2. Are you aware of any services organization that suffered a cyber attack?
3. What happened to that organization? What kind of attack was it?
4. Which controls should that organization implement to prevent the mentioned attack?
5. Do you think Blockchain could've prevented or helped against the attack? Why?
6. Can you please indicate your level of agreement with the below phrases using a scale of 1 to 5 where 1 is "Totally Disagree" and 5 is "Totally Agree".



*Mark only one oval per row.*

| | 1 "Totally Disagree" | 2 | 3 | 4 | 5 "Totally Agree" |
|---|---|---|---|---|---|
| Supply Chain Attacks are not a problem | ○ | ○ | ○ | ○ | ○ |
| Very few companies are victims of Supply Chain Attacks | ○ | ○ | ○ | ○ | ○ |
| Organization that have been victims of Supply Chain Attacks do not suffer great damage | ○ | ○ | ○ | ○ | ○ |
| Supply Chain Attacks can be prevented with the common existing tools (Firewalls, IDS, etc) | ○ | ○ | ○ | ○ | ○ |

# Appendix 3 - Links to Transcriptions and Interview Recordings

- Interview Riivo video record https://web.microsoftstream.com/video/df935356-7d2b-4b55-a16a-5b6f76cb8dc3
- Interview Peeter video record https://web.microsoftstream.com/video/dc9e7c81-be46-42e8-8b0e-76518107669d
- Interview Edwin video record https://web.microsoftstream.com/video/420ac3f6-679c-45c0-8b4d-f6f7b04947ae
- Interview Andres video record https://web.microsoftstream.com/video/de376a32-d0fa-4bfa-bec0-3416a77e3eae
- Interview Xavier video record https://web.microsoftstream.com/video/9f9a8752-8d7d-448d-92b8-938bb8d0a69c
- Interview Aleksander video record https://web.microsoftstream.com/video/57177440-41fe-4167-bd3e-5e100f573017
- Interview Chibuzor video record https://web.microsoftstream.com/video/4fe7d753-78ba-416b-9e70-34c025948df2
- Interview Shabahat video record https://web.microsoftstream.com/video/a10484c9-b84e-421d-881b-6aefd38cf669
- Interview Alexander video record https://web.microsoftstream.com/video/5880d2ec-a83a-4570-834b-fa8da1dd849b
- Interview Otto video record https://web.microsoftstream.com/video/4191b9f4-1829-44ae-adf0-527461af42d9
- Interview Silver video record https://web.microsoftstream.com/video/63353ce5-4cb2-49d2-b13b-a4e3a579356a
- Due to technical issues it was not possible to record Gabriel's Silva interview

Link to transcripts:

https://drive.google.com/drive/folders/1dZTC6uVX-QMdjqGhNrJfVpWwYoJLK5b
usp=sharing