Spring | 18

UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

Master Degree Project in Innovation and Industrial Management

Blockchains, the New Fashion in Supply Chains?

- The compatibility of blockchain configurations in supply chain management in the fast fashion industry

Ida Lönnfält & Josefine Sandqvist

Graduate School
Master of Science in Innovation and Industrial Management
Supervisor: Rick Middel

Blockchains, the New Fashion in Supply Chains?
- *The compatibility of blockchain configurations in supply chain management in the fast fashion industry*

By Ida Lönnfält and Josefine Sandqvist

School of Business, Economics and Law, University of Gothenburg, Vasagatan 1, P.O. Box 600, SE 405 30 Gothenburg, Sweden
Institute of Innovation and Entrepreneurship

Contact: Ida.Lonnfalt@gmail.com; Sandqvist.Josefine@gmail.com

Abstract

Background and Purpose: Blockchain Technology has recently, with its disruptive force and revolutionising ways of improving security and data sharing, gotten a lot of attention in both academics and business. Blockchains can be separated into several configurations of blockchains, which all have different benefits and drawbacks. There is, however, a lack of consensus about these different configurations and the existing literature does not provide any comprehensive compilation. Moreover, blockchains are said to have an especially benefiting value in supply chain management. Despite this, the diffusion of the technology and use cases in the fast fashion industry, which is highly reliant on an efficient supply chain, are still near to non-existent. One of the most important factors affecting the diffusion of new technologies has been said to be compatibility. Hence, this study aims to investigate how compatible the different configurations of blockchains are in the supply chain management in the fast fashion industry.

Methodology: The research builds on an extensive literature review of blockchain technology and its different configurations, resulting in a compilation of the characteristics distinguishing the configurations. The literature is then extended and built upon by conducting qualitative semi-structured interviews with blockchain experts about the different configurations. In addition to this, fast fashion companies are interviewed, also by semi-structured interviews, about their perception based on each of the characteristics identified in the literature review.

Findings and Conclusions: One of the main findings is that the different configurations of blockchains can be distinguished by four clusters of characteristics and that there are trade-offs evident between them that affect the compatibility of the different configurations. Based on this, a model has been constructed that was used to assess the compatibility of the blockchains configurations in supply chain management in the fast fashion industry. This resulted in the second main finding of the study, which is that even though it has been discussed that there is a lot of benefits achievable by blockchains, the result indicates that no configuration is fully compatible in this aspect studied. However, each configuration can be compatible to a certain extent and can consequently provide value in different settings. It is also identified that a consortium blockchain is adaptable and has the potential to overcome some of the trade-offs. Furthermore, the study provides four recommendations regarding the adoption of the different configurations of blockchains in supply chain management in the fast fashion industry.

Keywords: *Blockchain Technology, Configurations of Blockchains, Public Blockchain, Consortium Blockchain, Private Blockchain, Compatibility, Supply Chain Management, Fast Fashion Industry*

Acknowledgements

We would like to express our appreciation to everyone that in any way has contributed to this study. In particular, we would like to thank Rick Middel and Daniel Hemberg for valuable feedback and guidance during this this project. Further, we would like to thank additional staff at the Institution for Innovation and Entrepreneurship at Gothenburg School of Business, Economic and Law for your support.

Our gratitude also goes to the Sten A. Olsson Foundation for granting us a scholarship, which enabled us to travel to the relevant place for data collection. We would further like to thank our contact persons at the technology company that helped us to identify the knowledge gap that this study examines and further provided us with the right contacts. Lastly, we would also like to express our sincerest gratitude to all of the interviewees that allocated both time and effort to participate in interviews and provided us with the information that this thesis is built upon.

Gothenburg, May 31, 2018

Ida Lönnfält

Josefine Sandqvist

Table of Contents:

List of Figures:

List of Tables:

1. Introduction

This chapter initially describes the background and problem setting of the topic to be studied in this thesis, which then leads to the research question that the study aims to answer. This is followed by a description of the delimitations of the study. Lastly, the disposition of the thesis is presented.

1.1 Background

Every now and then, new paradigm shifts fundamentally change the world and how business is performed. These paradigm shifts can be traced back to industrial shifts such as the steam engine, electric power and information technology (Swan, 2015; Qian, 2017). Researchers, enthusiasts and the business world are now discussing Blockchain Technology as the next big industrial shift due to its potential to fundamentally change the value exchange and trust between actors in business (Etwaru, 2017; Warburg, 2016). Its disruptive force has been compared to the upbringing of the Internet and many argue that blockchains have the potential to solve problems of lack of trust and need of intermediaries similar to how Internet solved the problems of distance and information exchange (Etwaru, 2017; Warburg, 2016). Blockchains have a great disruptive and revolutionary potential in many industries, and it has been estimated by World Economic Forum that 10 % of the world's GDP will be stored in blockchain technology by 2025 (Bauman, Lindblom & Olsson, 2016). The interest in blockchains has increased both in academics and in business in recent years (Zalan, 2018).

Blockchain technology was first introduced in 2008 when the alias of Satoshi Nakamoto released the white paper explaining the technology of an electronic payment solution, which was the foundation of the cryptocurrency Bitcoin (Nakamoto, 2008; Bauman et al., 2016). A common misconception is that blockchain technology equals cryptocurrency, but it is actually only one of many possible applications of blockchains (Nowiński & Kozma, 2017). ResearchBriefs (2018) has identified 36 areas of business where blockchain technology is likely to drastically affect the business, such as financial services, insurance industry and supply chain management. Another misconception is that blockchain technology consists of one big blockchain, similar to the Internet. This is according to Laurence (2017) not true, who rather argues that there are and will be many different blockchains that can be designed and created for different purposes.

Although the blockchain technology is very complex, it can, in short, be described as a data-sharing platform that uses cryptography, a technique that enables secure communication by concealing data into a string of numbers. It is described as a peer-to-peer network, a distributed network of equally powerful nodes (network actors), which validate transactions and store data in a more secure way. (Walport, 2016; Bauman et al., 2016; Etwaru, 2017) It ensures transparency, traceability, security, and irreversibility of transactions by creating a network of trust amongst peers and thereby eliminating the need of middlemen (Walport, 2016; Bauman et al., 2016; Etwaru, 2017). The original and most well known type of blockchain, presented by Nakamoto, is a fully public blockchain that is distributed and accessible for everyone (Bauman et al., 2016). However, the open source characteristics behind the technology have enabled several other types, where the power and access are restricted, to emerge as well. The complete opposite of a fully public blockchain is a fully private blockchain where the power is completely centralised (Zheng, Xie, Dai, & Wang, 2016). Further, a hybrid between the fully public and the fully private blockchain with distributed power, but restricted to a specific number of actors, has emerged under many names (Brennan & Lunn, 2016; Walport, 2016; O'Leary, 2017; Bauman et al. 2016; Zheng et al., 2016). This hybrid version will in this study be referred to as a consortium blockchain and the different ways in which a blockchain can be designed will hereafter be referred to as different configurations of blockchains. Important to note is that, compared to the Internet that has a set standard (Maxwell & Salmon, 2017), the variety of configurations that can be created within the main categories, private, public, and consortium, is near to unlimited (Provenance, 2016; Arvsov, 2017). The literature generally speaks of the three configurations discussed above and this division will be used in this study. However, there seems to be a lack of a comprehensive compilation of the different configurations in the literature.

One benefit of blockchains is its characteristic of being immutable, which enables anyone to check the transactions and ensure that its information has not been tampered with (Xu, 2016). In relation to this, the technology enables a transparent and traceable register of assets and their owners, which makes many argue that blockchain has a specific benefiting value in supply chain management (SCM) (Loop, 2017; Nowiński & Kozma, 2017). SCM refers to the management the flow of information, transactions and activities involved in the very first to the very last step of the production process (Lopes de Sousa Jabbour, Gomes Alves Filho, Backx Noronha Viana, & José Chiappetta Jabbour, 2011; Masteika & Čepinskis, 2015). A supply chain usually consists of both upstream activities, with suppliers, and downstream activities, with customers (Porter, 1985; Galbraith & Kazanjian, 1986; Nicovich and Dibrell, 2007). As the blockchain technology has a distinct focus on networks (Walport, 2016; Bauman et al., 2016) it could be figured that the technology could be of particular benefit to the upstream part of SCM that is highly concerned with networks (Chang, Chiang, & Pai, 2012).

Blockchain technology and its potential within SCM have recently been widely discussed (Foerstl, Schleper & Henke, 2017). It has been pointed out that the use of blockchains in SCM create a comprehensive ledger shared by all actors in the supply chain (Walport, 2016) and thereto enable the actors to trace the origin, point of production, precise location and end destination of an asset in real time. (Loop, 2017; Lu & Xu, 2017). There have been a number of use cases of blockchains in supply chains, e.g. a seafood company that used blockchains to trace origin or their fish, which was reported to increase their sales by $22 million, and a diamond producer that used blockchains to trace and identify diamonds to prevent the circulation of fake diamonds in the market. (Loop, 2017) Another example is a Danish fashion premium brand using blockchain by enabling the customer to trace back where the garment is made and with what material, all the way to the exact alpaca, to create a product journey (Provenance, 2018).

As the fashion industry is an industry with high reliance on an efficient supply chain (Christopher, Lowson & Peck, 2004; Chan, Ngai & Moon, 2017), it can be argued to be a suitable setting for using of blockchain as a way for creating more secure, transparent and traceable supply chain. The supply chains in the fashion industry are often long and contain a lot of steps, thus including a lot of actors (Bruce, Daly & Towers, 2004). This in combination with often having very short production cycles makes the SCM in the fashion industry quite complex (Bruce & Daly, 2011). The fashion industry is, in general, facing increased demands in terms of sustainability, where the supply chain is the most affected area (Khurana & Richetti, 2016). In the business world, the fashion industry's supply chains have been discussed to be to benefiting from blockchain technology from a reputational perspective as a way of dealing with the increasing criticism of ethical and sustainability issues (Burbidge, 2017).

One part of the fashion industry that has gotten especially much criticism regarding these kinds of issues recent years is the fast fashion industry (Perry, 2018; Buchanan, 2017; Kaur, 2016; Siegle, 2013; Buchanan, 2017; Hendriksz, 2017). Fast fashion is commonly referred to as companies with strategies to create efficient supply chains in order to produce low cost fashionable clothes rapidly while quickly respond to consumer demands (Zarley Watson & Yan, 2013; Levy & Weitz, 2008). Thus, based on above discussion, blockchain technology could potentially help and solve many of the concerns present in the fast fashion industry. However, although the interest in the use of blockchain technology is increasing, the use cases existing today are still near to non-existent in the supply chains in the fast fashion industry. Hence, the lack of adoption of all types of blockchains, despite the discussed benefits, indicates that more knowledge is needed in this regard.

The reasons to why some new technologies become diffused and adopted while others do not, and the factors affecting the rate of adoption, are both topics that have been widely discussed by both academics and practitioners (Sherif, Zmud & Browne, 2006; Schilling, 2013). The compatibility has been pointed out as one of the most important attributes that can affect an innovation's adoption (Rogers, 2003). The compatibility of a new technology can be defined as how well it is perceived to be consistent with the values, past experiences and needs of a potential adopter (Rogers, 1983). Due to the lack of use cases in the fast fashion industry, the compatibility of different configurations of blockchains has not yet been determined. Examining the compatibility is important to do in order to work against the perceived unfamiliarity of an innovation and can facilitate the prediction of its future rate of adoption (Rogers, 2003). It can also facilitate the future adoption rate by highlighting potential discrepancies between the technology and the perception of the potential adopters and thereby providing a sense of what actions that have to be taken in order to increase the future compatibility (Agarwal & Karahanna, 1998). Thus, due to the so far limited diffusion of blockchain technology in supply chain management, and in the fast fashion industry in particular, looking closer on the compatibility could increase both the understanding and the likelihood of a potential future adoption.

Overall, little research can be found about the different configurations of blockchains and whether they are compatible with SCM in the fast fashion industry. This, in combination with the lack of practical cases, implies that there is a need for further research on the topic.

1.2 Purpose and Research Question

The purpose of the thesis is to examine the potential use of blockchain technology in supply chain management by applying it to the fast fashion industry. More specifically, to examine how compatible the different configurations of blockchains are with supply chain management in the fast fashion industry. Further, the aim is to provide a deeper understanding and expanding the research area of blockchain technology by a comprehensive compilation of its different configurations.

Based on the background and this purpose, the following research question has been formulated:

- *How compatible are the different configurations of blockchains with supply chain management in the fast fashion industry?*

By answering the research question, the study will contribute theoretically by providing a comprehensive compilation of blockchain configurations, since this is lacking in current research. Moreover, the study provides a model that can be used in order to assess the compatibility of the blockchain configurations, thereby building on existing literature of blockchain technology. As blockchain technology is still found in a very early stage of diffusion, especially as it comes to supply chain management in the fast fashion industry, studying the compatibility can contribute to the understanding of its future adoption.

In addition to this, it will provide a practical contribution by mapping the industry and giving insight in what configuration of blockchain that may be compatible in a future adoption of blockchains in the supply chain management. By examining this, companies in the industry might get a deeper understanding of the technology and how compatible it is for their SCM. Furthermore, in discussion with a large technology company, it was expressed an interest in, and lack of knowledge of, which configuration of blockchains that would be suitable to use in the supply chain management in the fast fashion industry. Thereby, by examining this topic, the practical implication will be to fill a gap of knowledge that exists today.

1.3 Delimitations

As already mentioned, blockchain technology has many applications where cryptocurrency is the most well known. However, for the scope of this study, the use of Bitcoin and other cryptocurrencies and paying methods will be excluded from the focus. It will merely be used as a way of explaining the technology of blockchain since most of the existing literature is covering these topics. Further, characteristics that can be accomplished through all of the different blockchain configurations with similar results will be excluded.

As the focus in the study lies on the fast fashion industry, other industries will not be analysed. Moreover, only companies with their headquarters in Sweden or the United Kingdom will be included. These two countries are included because of the fact that the fast fashion industry is considered to be prominent and developed in both of these countries. The reason for not including companies from additional countries was due to the time and access constraint. The study will also focus on the upstream activities in the SCM, and will thereby not cover the downstream activities. In addition to this, the term compatibility will merely be used to denote how suitable a technology is with a company's characteristics. The study does not aim to extend or build upon the theoretical framework of compatibility but will rather use it as a concept to examine the compatibility of the different configurations of blockchains. Finally, the thesis will take an organisational perspective and will not study the subject from a societal or consumer perspective.

1.4 Disposition

The thesis will consist of the parts specified below and will be presented in the following order.

Figure 1.1: Disposition of the Research Process. Compiled by authors.

2. Literature Review

The following chapter will present the literature review. The chapter will be initiated with a brief presentation of new technology adoption and compatibility. This will be followed by a section about blockchain technology that initially will explain the technology, followed by the different configurations of blockchains and finally the use of blockchains in supply chain management. The literature review of blockchains will then be summarised in a compilation of the different configurations and their characteristics.

2.1 Compatibility of New Technologies

Although the benefits that blockchain can bring into business have been widely discussed, and the technology has undergone substantial growth and development during the previous years (Loop, 2017; Nowiński & Kozma, 2017; Zalan, 2018), there are still few companies that have actually implemented blockchains in their operations and in particular in their supply chain management. In order for a technological innovation to become adopted, several factors come into play (Rogers, 2003; Schilling, 2013). Many researchers and practitioners have studied the diffusion of innovations with the aim of identifying what factors that enables an innovation to become adopted (Sherif, Zmud & Browne, 2006; Schilling, 2013). A general tendency is that the initial adoption rate is slow as the innovation enters the market, but increases as the market gets familiar with it and realises its value. The rate of adoption then declines again when the market has been saturated. (Schilling, 2013)

The fact that the rate of adoption tends to be slow in the beginning can have crucial effects on the mere survival of technological innovations as some innovations simply get replaced by alternatives perceived as superior. There is a tendency for so-called dominant designs to emerge and become the standard technology. This means that a specific design of a technology spreads and becomes adopted by the majority of users, and thereby becomes the industry standard. This usually happens some time after a technology has been introduced to the market and has been developed, adjusted and improved by multiple actors. (Utterback & Abernathy, 1975; Suárez & Utterback, 1995; Schilling, 2013) The reason that some innovations get adopted and others do not, can have multiple explanations (Schilling, 2013).

One of the factors affecting an innovation's rate of adoption is the compatibility (Rogers, 1962; Moore & Benbasat, 1991; Agarwal & Karahanna, 1998). Compatibility was initially defined by Rogers as *"the degree to which an innovation is consistent with existing values and past experiences of the adopters"* (Rogers, 1962 p. 126). This definition has been slightly altered, and was in 1983 reformulated as "*the degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters"* (Rogers, 1983 p. 223). Agarwal and Karahanna (1998) separate the constructs of compatibility, based on Rogers definition, into four parts that an innovation needs to be compatible with, namely existing work practices, preferred work style, prior experiences, and values. Due to the fact that blockchain technology has just recently started to become adopted, especially within the supply chain management in the fast fashion industry, looking closer on its compatibility could contribute to the understanding of its future adoption.

2.2 Blockchain Technology

The sections below will present a description of what blockchain technology is, an explanation of the different configurations of blockchain and of the use of blockchains in supply chain management. It will then be concluded by a summary of the blockchain characteristics that have been identified.

2.2.1 What is Blockchain Technology?

The technology was originally developed by Satoshi Nakamoto, a to this day unknown person, and released in 2008 as a white paper as a solution to the peer-to-peer electronic cash system, today known as Bitcoin (Nakamoto, 2008; Lin, Shen, Maio & Liu, 2018; Bauman et al. 2016). Trust between actors is believed to be essential in order to exchange value where actors today usually use middlemen in order to exchange value when there is no or little trust (Etwaru, 2017; Warburg, 2016). Trust is the centre of blockchain technology and the technology was in fact developed in order to increase trust between unknown untrusting actors, reducing the need of middlemen such as banks (Warburg, 2016; Etwaru, 2017). The technology is thereby creating what Mattila (2016) refers to as digital trust. Since the technology is open source, meaning that it is free for all to build, adapt and develop their own blockchain, many argue that blockchains can be used in many more ways than solely in financial assets, which are the first application of blockchains (Bauman, et al., 2016).

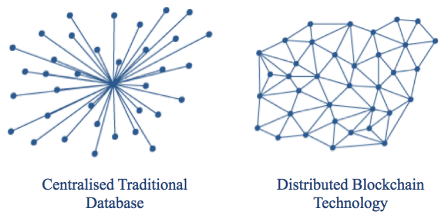

Figure 2.1: Blockchain Distribution of Actors and Copy of the Ledger. Compiled by authors based on Warburg (2016), Etwaru (2017), Brennan & Lunn

Blockchain technology is in short a peer-to-peer network that stores data on a ledger in a decentralised and distributed way (Walport, 2016; Bauman et al., 2016; Etwaru, 2017). This means that the data infrastructure is not owned or controlled by one single entity, such as the tax registry that is owned and controlled by governments. Instead, everyone that is part of the network is jointly responsible for that the network is working, which means that it is decentralised. Further, everyone is responsible that the information that is stored is correct by all participants owning a copy of the ledger, in so-called nodes, meaning that it is distributed. (Bauman et al., 2016; Warburg, 2016; Etwaru, 2017) The technology is enabling a fully transparent history of transactions and thereby granting traceability through the blockchain (Bauman et al., 2016). Walport (2016) describes that all the copies are identical, shared and constantly updated to one another in a more secure way than traditional databases. By having the data stored and shared across a network, the risk of cyber attacks is low due to that the network is not dependent on one storage place or a single one point of failure as in a traditional centralised system (IBM, 2017a). If one of the ledgers gets attacked or failed, the network will detect this since the majority of the network has another copy and will continue to operate, maintaining the system's availability (Fanning & Centers, 2016). This is one of the arguments why the blockchain technology is more secure than traditional data storage.

Another advantage is believed to be its immutability, meaning that once the data is stored on the ledger, i.e. the blockchain, it is nearly impossible for someone to tamper or change the record (Xu, 2016). This is due to the blockchain technology's network characteristics and use of cryptography to encrypt and secure transactions. Blockchains store the transaction by that all transactions performed in the network within a certain time frame are bundled up and gets verified, cleared and stored into a block that is interchanged with the earlier block (Tapscott & Tapscott, 2016), creating an interdependency (Etwaru, 2017). For example, the Bitcoin blockchain has a time frame of ten minutes (Tapscott & Tapscott, 2016). The foundation is that all transactions are broadcasted for the network to verify and reach consensus before they gets stored (Lipton, 2018.)

Berke (2017) describes that all actors commit computing power, e.g. software and hardware resources, to follow an algorithm that verifies transactions by solving a cryptographic puzzle, in the Bitcoin blockchain called mining (Xu, 2016). Thereby, the actors' computers power the system and the one that reaches the solution first is usually rewarded in some sort of fee while the rest of the actors in the network verify the puzzle's authenticity (Berke, 2017: Xu, 2016). Only after a collective verification of authenticity, reached by all actors with consensus power, can the transaction be transformed into a block (Xu, 2016) and this forms the basis for the next cryptographic puzzle (Burke, 2017). Thereby, the blockchain is a ledger based on blocks in a chronological order (Fanning & Centers, 2016). What makes it immutable is that the blocks are all interchanged, meaning that the next block is dependent on the content of the earlier block and, thereby, all the blocks earlier in the chain (Etwaru, 2017; Burke, 2017). This is significantly different from how data is stored in a traditional database (Etwaru, 2017). Thereby, changing anything in an earlier sequenced block or trying to tamper with the data will be detected and the network will automatically replace the tampered and, thereby, false ledger (Etwaru, 2017).

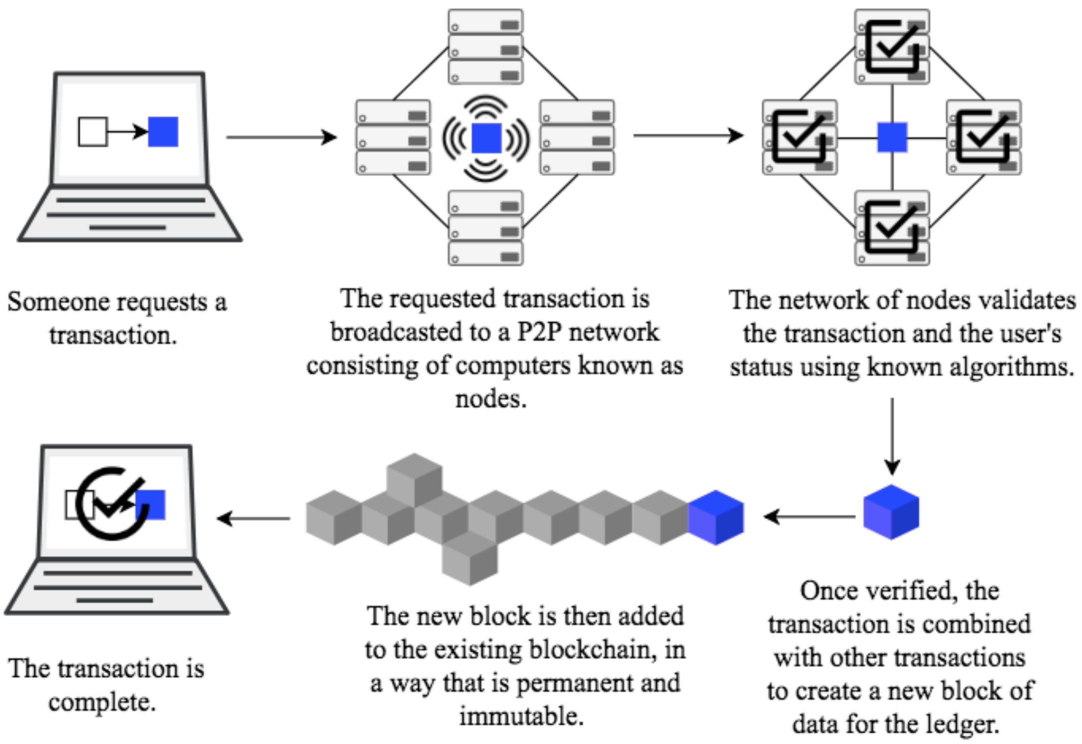

Figure 2.2: Blockchain Transaction Process. Compiled by authors inspired by PWC (2016a)

To hack or tamper with the information would require massive computing power in order to alter all the earlier blocks on the majority of the actors (nodes), in the network's ledger (Lin, Shen, Maio & Liu, 2018). The blockchain is thereby considered to be more secure the more actors there are in the network, i.e. the more the technology gets adopted (Xu, 2016). Further, in many blockchains, in order in ensure this security, there is a built-in incentive system where the actors in the network that is validating the transactions are gaining a small fee since they use computer power to run the network (Zalan, 2018; Walport, 2016).

Security is what many argue is the real novelty of the new technology compared to a traditional system. It enforces trust between the actors in the network without the need of a central authority or a middleman such as a bank, company or government. (Walport, 2016; Warburg, 2016) Advantages of blockchain technology are said to be full distribution, transparency, traceability, security and immutability (Christidis & Devetsikiotis, 2016; Bauman et al., 2016; Ross 2017). According to Dinh, Wang, Chen, Liu, Ooi, and Tan (2017), the blockchain's immutability and transparency further help reduce human errors and the need for manual intervention due to conflicting data. Swan (2015) has described that blockchain technology enables records to be*:*

"Shared by all network nodes, updated by miners, monitored by everyone, and owned and controlled by no one"

- Swan 2015, p. 1

2.2.2 Different Configurations of Blockchain Technology

The version of a blockchain that Nakamoto suggested as a revolutionising paying method is what many call the original and truly distributed version of the technology. This version is built to be permissionless, meaning that there is no limitation or restriction for the actors to take part or see the information in the system, and is called a public blockchain (Nakamoto, 2008; Ross 2017; Lin et al., 2017; Dinh et al., 2017). Today, ten years after the first introduction of blockchains, different configurations of blockchains with different characteristics have been developed. From the original permissionless public blockchain, there have emerged other kinds of blockchains that are referred to as being permissioned, meaning that there is a restriction of who can take part of and see information on the ledger. (Walport, 2016; Ross, 2017; IBM, 2017b) Further, compared to a public, these permissioned blockchains have actors that are responsible and in control of the blockchain, either a single entity, so-called private, or a collaboration group, so-called consortium (Walport, 2016; Zheng et al., 2016; Bauman et al., 2016; Dinh et al., 2017). Lin and Liao (2017) argue for that even though the blockchain configurations are different, they all have their advantages. Even though the varieties of blockchains that could be created within these blockchain configurations are infinite due to that the technology is programmable (Maxwell & Salmon, 2017), the study will focus upon the three main configurations that have been identified. The three main configurations identified are divided into the two categories permissionless and permissioned and are illustrated in Figure 2.3 below.

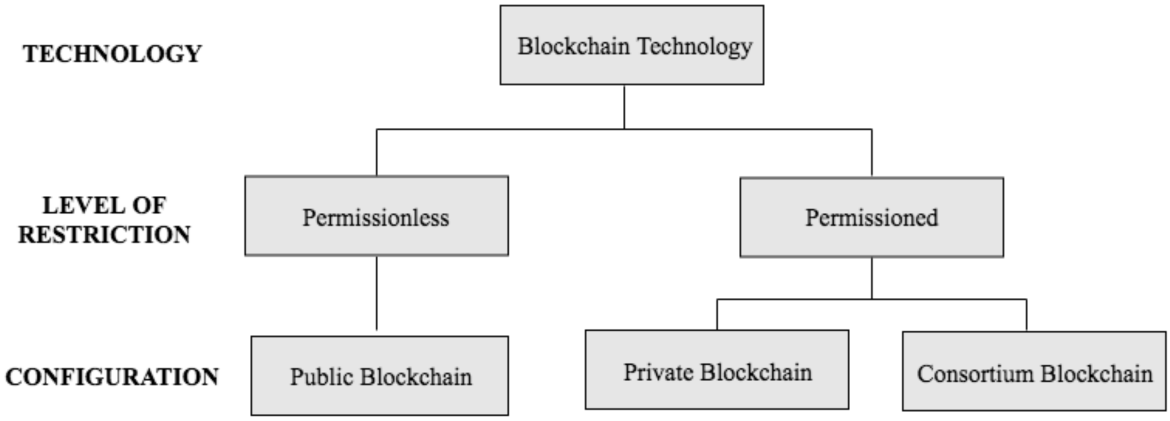

Figure 2.3: Outline of Blockchain Configurations. Compiled by authors based on literature review.

2.2.3 Permissionless Blockchain

There is a consensus among practitioners and researchers that the original blockchain is permissionless and is commonly referred to as a public blockchain (Walport, 2016; Bauman et al. 2016; PWC, 2016b; Ross, 2017). This configuration of blockchain will be presented in more detail in the following section.

2.2.3.1 Public Blockchain

A public blockchain is a blockchain that is open source, which means that anyone can build a public blockchain. Even if anyone can build and start the blockchain, nobody can control or own a public blockchain. (Bauman et al. 2016; Walport, 2016; IBM, 2017b) The literature and many practitioners agree that the fully public and uncontrolled blockchain is the purest of the blockchains, which implies that it achieves the full advantages of the technology, such as full distribution, transparency, traceability, cyber security and immutability (Buterin, 2015; Brennan & Lunn, 2016; Christidis & Devetsikiotis, 2016; Arsov, 2017; Ross, 2017). The characteristics of the permissionless blockchain imply that anyone can join, take part, validate or see information and transactions on the blockchain (Christidis & Devetsikiotis, 2016; Zheng et al., 2016). Zheng et al. (2016) describe that a public blockchain in regarding the consensus power, e.g. the power to take part and decide in the network and its transactions, all actors can take part and no one can be restricted. There is thereby a distributed power to reach consensus (Zheng et al., 2016). However, even though everyone can see everything that is happening on the ledger and perform transactions, no single actor can alone decide what is written on the blockchain, i.e. the ledger cannot be owned (Walport, 2016; Bauman et al., 2016; Arsov, 2017). Thus, the system does not allow differentiation between the creator and the other users (Moyano & Ross, 2017).

One of the main benefits of the public blockchain is that it is immutable, meaning that once information is stored, it is nearly impossible to be tampered with or being deleted (Ross, 2017; Bauman et al. 2016; Bano, Sonnino, Al-Bassam, Azouvi, McCorry, Meiklejohn & Danezis, 2017). One other main benefit is mentioned to be the public blockchains' ability to protect against cyber attacks (Kshetri, 2017; Bauman et al. 2016; Priya; 2018; IBM, 2017a). A high level of both immutability and protection against cyber attacks are referred to as security features of a public blockchain (Bauman et al., 2016; IBM, 2017a; Kshetri, 2017). Due to the increasing need of computing power and electricity as the blockchain increases in length and users, one challenge that many agree upon is that it is not scalable enough to handle the increasing transactions (Brennan & Lunn, 2016; Bauman et al., 2017; Lemieux, 2016; Buterin, 2016). For example, Bitcoin can handle seven transactions per second, which can be compared Visa's 2000 transactions per second (Lipton, 2018; Yli-Huumo et al. 2016; Swan, 2015; Croman et al. 2016).

Further, Lipton (2018) mentions that in a public blockchain, at least six subsequent blocks need to be created in order to be sure of full security. Thereby, secure data cannot be collected in real time. Berke (2017) mentions that to ensure and consider the data fully verified and secure, this can take up to one or two hours in a public blockchain. This might be considered vulnerability for the public blockchain since the delay might lead to that one transaction that seems to be verified later loses it status (Berke, 2017). Oh and Shong (2017) argue that due to this, it is difficult to expand the network and the transaction speed. Similarly, Conoscenti, Vetro and De Martin (2016) report that a public blockchain cannot scale to deal with many complex transactions. However, it is discussed that the scalability challenges actually is the mechanism that ensures the security of the system due to increasing computing power needed (Berke, 2017; Croman et al. 2016) Since Xu (2016) mentions that the blockchain is more secure the more actors there are, a permissionless blockchain is considered to be more secure than a permissioned since there are unlimited actors that can hold a copy that is needed to be hacked. Thereto, the more actors there are, the more difficult it is to tamper with information since the majority of the network needs to be altered (Lin, Shen, Maio & Liu, 2018).

The high security further comes with a higher cost to run the system. Brennan and Lunn (2016) explain that the cost to run the system is high on a public blockchain because of the extensive computer power that is needed to run the network. This cost gets higher as more actors join, compared to a permissioned blockchain where the total amount of actors and the consensus power are limited, reducing the need of computing power (IBM, 2017b; Bauman et al., 2017). A monetary reward is usually needed to create an incentive for the trustless actors to use their computer power to take part and run the network, such as on the Bitcoin blockchain where miners collect the token Bitcoin to run the system (Brennan & Lunn, 2016; Walport, 2016). IBM (2017b) argues that this incentivising mechanism is put in place to encourage more actors into to join the network. A further limitation of the fully public blockchain is its lack of flexibility, meaning that once it is developed it is very difficult to change rules that have been made (Oh & Shong, 2017). This is due to that in order to change rules, at least 51 % of the unknown actors in the network that all have different incentives must accept the changes (Lin & Liao, 2017).

Because of the security feature in place, there is no need of trust between the actors, the trust needed is in the system itself (Xu, 2016; Warburg, 2016; Mattila, 2016). Xu (2016) refers to that the technology facilitates trust-free transactions. The system is thereby built on unknown actors reaching consensus by computers and does not require a central authority in order to be trusted (Zalan, 2018). Xu (2016) explains that one of the reasons for the decreasing of the need of trust is that all transactions are laid out for the whole network to control and see. The actors do thereby not need to know the identity of the actors since trust is not needed (Bauman et al., 2016). Further, there is no need of a third party such as a bank or government (Nakamoto, 2008).

Oh and Shong (2017) argues for that anybody can access the data in a fully public blockchain. In regards to identity of the actors, Oh and Shong (2017) refer to this as pseudo-anonymous, which means that even though the data can be accessed, the identities of the actors are concealed on a public blockchain. This is achieved by the fact that the users have a sort of digital identity by using a public key, which Ross (2017) calls public address, that is visible for everyone since it is shared on the network. Ross (2017) further compares this to a public social media page, but in blockchains, the key is a set of random numbers that is not identifying the users true identity. Ross (2017) further compares the use of a private key, which the actors use to identify themselves in order to unlock their personal information, to a password. Even though information can be concealed, due to that there is no restriction of who can join, add or see information on a public blockchain, the privacy level of the information is considered to be low (Maxwell & Salmon, 2017). Zheng et al. (2016) explains that evidence has been shown that even though the users have been using its private and public keys, privacy leakage can happen. Even though the identity is hidden, all the transactions and other information shared between the actors are broadcasted to the whole network (Xu, 2016). Maxwell and Salmon (2017) explains that due the re-use of the public key, which is constantly broadcasted on the network, it is possible to obtain information that enables individuals and companies to be singled out and identified by being referenced to their public key. Kosba, Miller, Shi, Wen and Papmanthou (2016) refer to this as the lack of transaction privacy and argue for that the lack of privacy is the major hindrance for broad adoption for public blockchains.

2.2.4 Permissioned Blockchain

As soon as any restriction is put into place regarding which actor that is able to join, which information that can be seen or what can be written the blockchain is referred to as a permissioned blockchain (O'Leary, 2016; Bauman et al. 2016; Christidis & Devetsikiotis, 2016). Kshetri (2017) claims that by only trusted actors having the controlling access, the problems faced by permissionless blockchains will be avoided. The literature and practitioners have further identified two categories of blockchain that are permissioned. One that is called private blockchains, which refers to a permissioned blockchain that is controlled by one single entity, and one that is called consortium blockchain, which is described as a hybrid of the public and private blockchain, consisting of a trusted network (Oh & Shong, 2017; Buterin, 2015; Zheng et al., 2016; Swan, 2017). Some call it permissioned private and permissioned public (Walport, 2016; Brennan & Lunn, 2016) while other call it private and consortium (O'Leary, 2017; Zheng et al., 2016; Bauman et al., 2016; Buterin, 2015; Oh & Shong, 2017). The two configurations of blockchains will be described separately in the sections below.

2.2.4.1 Private Blockchain

In a fully private blockchain the owner, as a single central authority, has control over the network and whom that can participate (Zheng et al., 2016; Brennan & Lunn, 2016). Thereby, all the actors in the network are trusted and identified (Bano et al., 2017; Oh and Shong, 2017). Dinh et al. (2017) mention that all identities are authenticated. Further, the consensus process of validating transactions is fully owned by this central authority that can determine the final consensus, thereby one actor has all the consensus power (Zheng et al., 2016). Some argue for that a fully private blockchain do not give the advantages of the original characteristics in fully public blockchain since the main characteristics of distributed power have disappeared (Bauman et al., 2016). For example, the security of the immutability and cyber attacks are reduced compared to a public blockchain since the number of copies of the ledger is reduced, and the dominant actors have the power to tamper with the record (Zheng et al., 2016). This restricted number of actors and restricted consensus process to one single entity results in that the resources and energy consumption, and thereby transactions cost, of the system are lower than a public (Bauman et al., 2017; Brennan & Lunn, 2016; Buterin, 2015; Lipton, 2018).

This consensus process also increases the speed of transactions (Berke, 2017) and the scalability of the throughput is greater in a private blockchain (Christidis & Devetsikiotis, 2016; IBM, 2017b). Oh and Shong (2017) also mentions a cost reduction of using a private blockchain compared to a public blockchain and further argue that there is a higher transaction speed enabling real time data and that networks expansion in scalability is very easy to achieve, which is not possible with a public. Incentives to maintain the network are not based on monetary reward as in a public blockchain. The incentive system is instead based on what Brennan and Lunn (2016) call stake, which means that the actor has a stake in keeping the integrity of the ledger intact.

Compared to a fully public blockchain, the private blockchain is more flexible because the owner has the ability to fix errors created in the network and reverse transactions since a majority of many actors is not needed (Berke, 2017). Oh and Shong (2017) also mention a high flexibility and mentions that a private blockchain could be modified to fit the user. Regarding the privacy issues of a public blockchain, many argue that a private gives higher privacy (IBM, 2017b; Maxwell & Salmon, 2017). Oh and Shong (2017) claims that the data is only accessible to authorised users. Because of this restriction of which actors that can access the data, public key are not broadcasted over an unrestricted network (Oh & Shong, 2017). Thus, what Maxwell and Salmon (2017) describe as a problem for privacy in a public blockchain, is considered to be lower in a private blockchain. Christidis and Devetsikiotis (2016) mention that this is since the owner is controlling the rules and the participants. Ross (2017) argues that with a private blockchain, sensitive information will never be published to the public. In the light of this, Christidis and Devetsikiotis (2016) say that private networks make more sense for stakeholders who wish to operate in a controlled regulated environment where sensitive information is important. Bauman et al. (2016) describe the private blockchain as being suitable in a controlled environment such as financial market and government services (Bauman et al., 2016).

2.2.4.2 Consortium Blockchain

As the public and private blockchain may be seen as two extremes, a consortium is often referred to as a hybrid in the middle and thereby many of characteristics found between public and private where they have the opposite relation, a consortium is usually placed in the middle (Oh & Shong, 2017). There seems to be a lack of agreement regarding which name to use. Some call the blockchain a permissioned public blockchain (Brennan & Lunn, 2016; Walport, 2016) while others call it a consortium blockchain (O'Leary, 2017; Zheng et al., 2016; Bauman et al., 2016; Buterin, 2015; Oh & Shong, 2017). Some researchers define it as a mix of the public blockchain and private blockchain since it is a permissioned blockchain in the number of actors in the blockchain, but has the network effect is similar to a public blockchain (Brennan & Lunn, 2016; Provenance, 2016; Zheng et al., 2016). Despite all these different names, the main distinction of a consortium is mainly the same. It is mainly described as a blockchain where distributed consensus is reached by a set of closed and predetermined of actors (nodes) with collaborative authority, which are chosen as validators with consensus power (O'Leary, 2017; Oh & Shong, 2017; Provenance, 2016; Arvsov, 2017). Arsov (2017) is thereby defining this form of blockchain as partially decentralised in comparison with a public blockchain. This is compared with the private blockchain in which the owner has the authority or the public blockchain where all participants have authority (O'Leary, 2017; Oh & Shong, 2017; Arvsov, 2017)

In a consortium blockchain, a large degree of trust is needed between the actors since the distribution of the validation process is smaller than in a public and the predetermined set of trusted users validate the transaction rather than the large mass of unidentified actors (Brennan & Lunn, 2016; Provenance, 2016; Zheng et al., 2016; Bano et al., 2017). Oh and Shong (2017) argue that this maintains a distributed structure which strengthens security, compared to a private, while solving some of the scalability, flexibility and privacy problem in the public blockchain. They further argue that it is easy to expand the network and transaction speed is fast. Dinh et al. (2017) mention that even though the actors might not necessarily fully trust each other, although higher trust than in a public blockchain is needed, their identities are authenticated amongst the network. The right to read the blockchain may be public or restricted, depending on the programming (Arsov, 2017).

Advantages with a consortium is said to be, while wanting to establish a single record of consensus about facts, information and processes across collaborating entities in a distributed more secure way since no single entity has all the authority and being able to independently make changes (Bauman et al., 2016; Oh & Shong, 2017). Further, according to Bauman et al. (2016) when using the blockchain in a shared network with agreed protocol, the advantages such as data integrity and record of history will be similarly beneficial as in a public blockchain, although not as high, but with higher scalability and privacy. Although the security of immutability and cyber security in a consortium blockchain are higher than in a private blockchain, these characteristics are not described to be as high as in a public blockchain due to the lower of the number of copies of the ledger as well as numbers of actors needed to gain the majority in order to tamper with the information. (Zheng et al., 2016; Oh &

Shong, 2017) Even though a majority of a pre-set number of actors are to be considered more secure than only one dominant as with a private (Zheng et al., 2016).

Oh and Shong (2017) mention that the security and transaction speed can be increased compared to a public. This results in lower resources and energy consumption in the consensus process than in the case of a public blockchain because the consensus process is divided amongst fewer actors (Buterin, 2015), which results in a lower transaction cost than a public, but still higher cost than a private blockchain (Bauman et al. 2016; Brennan & Lunn, 2016; Provenance, 2017; Oh & Shong, 2017). The incentives to maintain the network can be referred to, as in a private blockchain, as being based on co-called stake. This incentive is off-chain and the actors have a stake in keeping the integrity of the ledger intact rather than by receiving a monetary reward. (Brennan & Lunn, 2016)

Privacy in a consortium blockchain can be considered to be similar to that in a private blockchain since the data access, such as the public keys that Maxwell and Salmon (2017) describe as a privacy problem in public blockchains, are restricted to authorised actors of the system (Oh & Shong, 2017). However, there is higher risk with more actors than it is with a fully private blockchain. Lu and Xu (2017) claim that a consortium blockchain performs better in privacy than a public blockchain. Casey and Wong (2017) claim that for example commercial data and production activities would be cryptographically recorded in open ledgers. They thereby imply that a consortium blockchain, where the information is shared only with the collaborating parties, will be beneficial for companies seeking to protect market share and profit.

2.2.5 Blockchains in Supply Chain Management

The recent development and growth of research about blockchain technology have provided several publications and studies pointing out SCM as one of the areas that can come to experience radical changes by the integration of blockchains (Nowiński & Kozma, 2017; Abeyratne & Monfared, 2016; Mattila, 2016; Lu & Xu, 2017; Loop, 2017; Apte & Petrovsky, 2016). SCM is a term describing the management of the supply chain, which can also be described as the flow, of materials, information and activities involved in the production process from start to end (Lopes de Sousa Jabbour et al., 2011; Masteika & Čepinskis, 2015). Supply chains involve multiple activities and multiple actors and thereby creates a complexity that has to be managed to some extent (Chou, Tan & Yen, 2004). A supply chain tends to have both upstream activities, taking place between the lead firm and its suppliers, and downstream activities, taking place between the lead firm and its customers (Porter, 1985; Galbraith & Kazanjian, 1986; Nicovich & Dibrell, 2007). Upstream activities, that will be the focus in this study, typically refers to the supply of material and components, but can also refer to activities such as design, manufacturing and assembly, depending on which activities that are performed by suppliers and not in-house (Chan & Qi, 2003). Recent development has been more towards extended supply chains, i.e. the inclusion of all actors involved in the supply chain all the way to components suppliers (Mouritsen, Skjøtt-Larsen & Kotzab, 2003; Masteika & Čepinskis, 2015).

The integration of supply chains is increasing as information becomes more accessible. Hence, the use of information technology has increased the possibilities and decreased the time and costs of sharing data between the parties in a supply chain, and thereby increasing the integration of supply chains. (Chan & Qi 2003; Power, 2005; Masteika & Čepinskis, 2015) According to Loop (2017) SCM can profit from further digital transformation since there is an increased need for efficient systems, increased expectations on sustainability from society and consumers, an enhanced need for security, transparency and authenticity in the supply chain process etc. In similarity with the way Internet affected SCM, blockchain technology and its potential in the field of SCM has recently been discussed (Foerstl et al., 2017). Blockchains have been stated to provide benefits within SCM such as improved possibilities to prevent counterfeit, strengthen the proof for insurance protection, decrease the risk of fraud and for goods being stolen (Loop, 2017). Abeyratne and Monfared (2016) are explaining immutability as an advantage for supply chains and Priya (2018) explains that protection against cyber attacks will be strengthened by the use of blockchains. Abeyratne and Monfared (2016) further advocated that more increasingly global and complex supply chains are vulnerable for a single point of failure when using a centralised system, leaving the network at risk for cyber attacks, which is something that they claim blockchain can help with. They further claim that types of data that can be added manually or automatically could be ownership, time stamping, location, product specifics and environmental impact data. By adding this kind of data, the literature mentions advantages such as increasing the traceability and enabling the tracking of products in time, location and point of production, and by increasing the transparency within the supply chain (Lu & Xu, 2017; Abeyratne & Monfared, 2016). These two characteristics will be described further in the two following paragraphs.

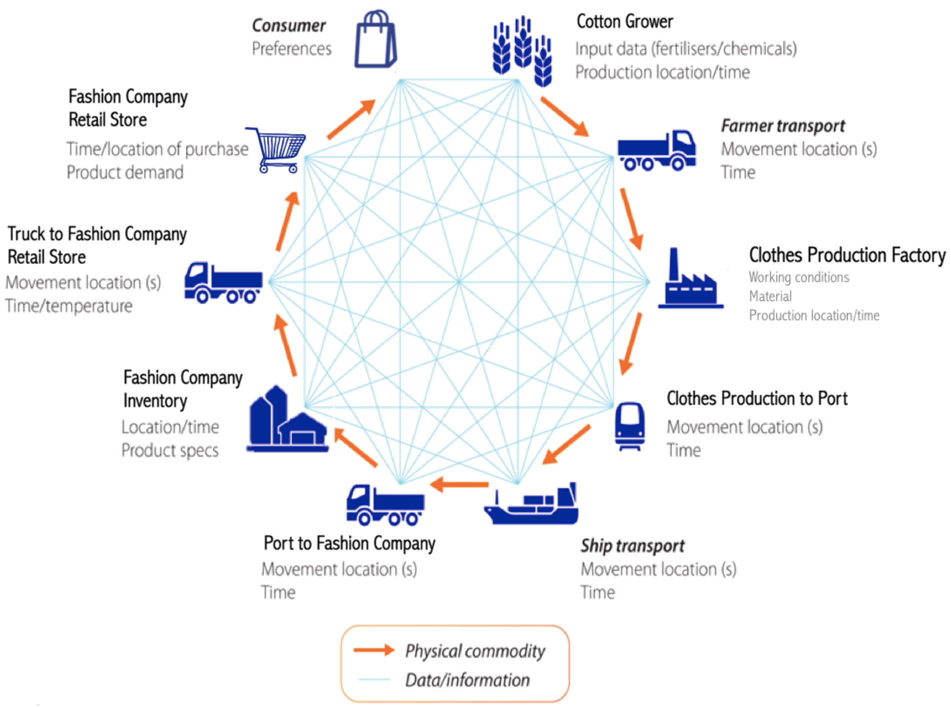

Figure 2.4: Traceability and Transparency of Information in Global Supply Chains. Compiled by authors based on Lefroy (2017).

Apte and Petrovsky (2016) claim that blockchain technology advocates transparency in the supply chain. Abeyratne and Monfared (2016) agree and argue that blockchain could enhance transparency within supply chains because of its unchangeable and immutable track record of data where the same information is distributed to every participant (Abeyratne & Monfared, 2016). By having a distributed database, the blockchain increases the value in the network by increasing the transparency of information that otherwise would have been in centralised silos (Loop, 2017). Deloitte (2017) also mentions this and further describe that for example in the automotive industry's supply chains, there is limited visibility beyond the second tier of suppliers, meaning that there is a lack of insight particularly regarding the raw material. The enhanced transparency of blockchains by providing customer access to information could further bridge the gap between the firm and their customers (Abeyratne & Monfared, 2016). This increased transparency is also believed to empower the customer to exclude actors that do not follow society's norms and values (Loop, 2017). The higher amount of identical copies of nodes, the higher security there is of the transparency, which means that the public blockchain has the highest transparency (Apte & Petrovsky, 2016).

Deloitte (2017) argues for an increasing traceability by using blockchain in supply chain. This is argued by Deloitte (2017) to be done by the blockchains tracking capabilities, including time stamping that provides a full audit trail, which gives business confidence in the authenticity in the goods. A traceable system in the supply chain enables the network of tracking the products from by providing information such as origin, components and exact locations at any point in time (Lu & Xu, 2017). Blockchain technology is claimed to be good in order to increase traceability in supply chains and reduce the need for the existing traceability intermediaries (Lu & Xu, 2017). To be able to trace and verify material in a supply chain setting could potentially help avoid sustainability scandals (Foerstl et al., 2017). Moreover, blockchains could enable companies to receive secure and correct information from suppliers, thus leading to enhanced access to information concerning delays and potential accidents (Loop, 2017). Abeyratne and Monfared (2016) mean that an increasing immutability is significantly improving traceability due to the detection of false data. Lu and Xu (2017) agree and mean that having a higher degree of certainty that the pre-sequenced blocks have not been deleted or tampered with increases the certainty of the traceability characteristics, which mean that a public blockchain has the most secure traceability and a private blockchain has the lowest. Further, a blockchain could be used to decrease the extent of human error and costs, which thereby ensures traceability (Abeyratne & Monfared, 2016).

2.2.6 Summary of the Characteristics of Blockchains Configurations

By examining and compiling the literature regarding different configurations of blockchains, and the literature specifically covering blockchains in supply chains, it can be derived that several characteristics distinguish the three configurations of blockchains from each other. All such characteristics identified in the above literature review have been compiled and summarised in Table 2.1 in a similar order that they have been presented in the text.

	Private Blockchain	***Consortium Blockchain***	***Public Blockchain***	***Discussed by***
Consensus Power *The distribution of consensus power.*	Single Authority	Consortium of Authority	Fully Distributed Authority	Zheng et al., 2016; Zalan, 2018; O'Leary, 2017; Oh & Shong, 2017; Lin et al., 2018; Walport, 2016; Lemieux, 2016; Dinh et al., 2017; Arsov, 2017
Immutability *Being sure that information has not been tampered with.*	Low	Medium	High	Xu, 2016; Dinh et al., 2017; Ross, 2017; Bauman et al. 2016; Bano et al, 2017; Berke, 2017; Xu, 2016; Lin et al., 2018; Oh & Shong, 2017
Protection against cyber attacks *Being protected against external cyber attacks and hacking.*	Low	Medium	High	Fanning & Centers, 2016; Kshetri, 2017; Bauman et al. 2016; Priya; 2018; IBM, 2017a; Xu, 2016; Oh & Shong, 2017
Scalability *The ability to perform a high amount of transactions.*	High	Medium	Low	Lipton, 2018; Berke, 2017 Lemieux, 2016; Buterin, 2016: Brennan & Lunn, 2016; Bauman et al., 2017; Oh & Shong, 2017; Conoscenti et al., 2016; Christidis & Devetsikiotis, 2016
Cost *The level of transaction cost.*	Low	Medium	High	Lipton, 2018; Brennan and Lunn, 2016; IBM, 2017b; Bauman et al., 2017; Oh and Shong, 2017
Existing trust *The existing level of trust between actors.*	High	Medium	Low	Mattila, 2016; Xu, 2016; Ross, 2017; Bauman et al., 2016; Kshetri; 2017; Dinh et al., 2017; Bano et al., 2017
Flexibility *Being able to change rules and settings about the sharing of information and transactions.*	High	Medium	Low	Oh & Shong, 2017; Lin & Liao, 2017; Berke, 2017; Oh and Shong, 2017
Privacy *Being sure that confidential information is concealed.*	High	Medium	Low	Oh & Shong, 2017; Ross, 2017; Maxwell & Salmon, 2017; Zheng et al., 2016; Lu and Xu, 2017
Incentives *The incentives for actors to run the network.*	Stake	Stake	Monetary Reward	Brennan & Lunn, 2016; Walport, 2016; IBM, 2017b
Transparency *Having access to information that is shared between the actors in the supply chain.*	Low	Medium	High	Abeyratne & Monfared, 2016; Apte & Petrovsky, 2016; Deloitte, 2017
Traceability *Being able to trace products back in the supply chain.*	Low	Medium	High	Lu & Xu, 2017; Foerstl et al., 2017; Deloitte, 2017; Abeyratne & Monfared, 2016

Table 2.1: Summary of Characteristics of the Blockchain Configurations. Compiled by authors.

3. Methodology

The following chapter will go through the methodology used for the study, starting with the research strategy and research design. This will be followed by a description of the methods used for collecting data and for the process of analysing the data. Finally, an assessment of the quality of the research will be presented.

3.1 Research Strategy

The study will take an exploratory approach as the subject is new and, so far, relatively unexplored. A qualitative strategy is chosen due to the need to explore the subject in depth and to analyse the perceptions of the actors in a subjective way, rather than the objective way that is usually connected with a quantitative approach. It is a suitable strategy when uncertainty is high due to a lack of existing knowledge (Bryman & Bell, 2011). In order to examine the compatibility of the different configurations of blockchains in supply chain management in fast fashion companies, it is necessary to examine the topic from the organisation's perspective and how they actually experience it themselves. Conducting qualitative interviews provides an opportunity to take part of the interviewees' point of view and opens up for detailed descriptions of the issue. The nature of the qualitative data collection in form of interviews opens up for exploring novel information, which is in line with the exploratory approach of the thesis (Bryman & Bell, 2011). It also provides opportunities such as asking complementary questions when clarification is needed, which is not possible with a quantitative strategy to the same extent (Bryman & Bell, 2011).

Further, the approach to theory in this study is abductive. This means that the study has both a deductive approach, a theory testing approach, and an inductive approach, a theory generating approach (Eriksson & Kovalainen, 2008; Bryman & Bell, 2011), in different parts of the study. More specifically, the study initially takes a deductive approach by reviewing literature and based on this compiling the characteristics distinguishing the configurations of blockchains. This compilation is used as the basis for collecting the empirical findings. Themes identified in the empirical findings are then combined with the literature to build upon and extend the initial compilation, creating an analysis model used to answer the research question of this study. This constitutes the more inductive part of the study.

The study has a qualitative strategy with an abductive approach towards theory as it aims to fill a gap in existing research in a novel subject. Although some research exists, there is a gap regarding the different configurations of blockchains technology and whether they are compatible with the supply chain management among fast fashion companies. Existing research and literature about different configurations of blockchains are connected to information about this obtained from experts within the field, and about the perception from fast fashion companies, to extend the knowledge base. Thus, the study extends and builds upon the existing literature regarding the different configurations of blockchains in the context of supply chain management in the fast fashion industry. The overall approach of the study is a linear approach, although the data collection followed a more iterative approach by conducting the majority interviews with experts and companies in parallel. The iterative process will be explained in further details in section 3.3.2.2.

An overview of the research process is illustrated in Figure 3.1. The steps will be described further in the subsequent sections.

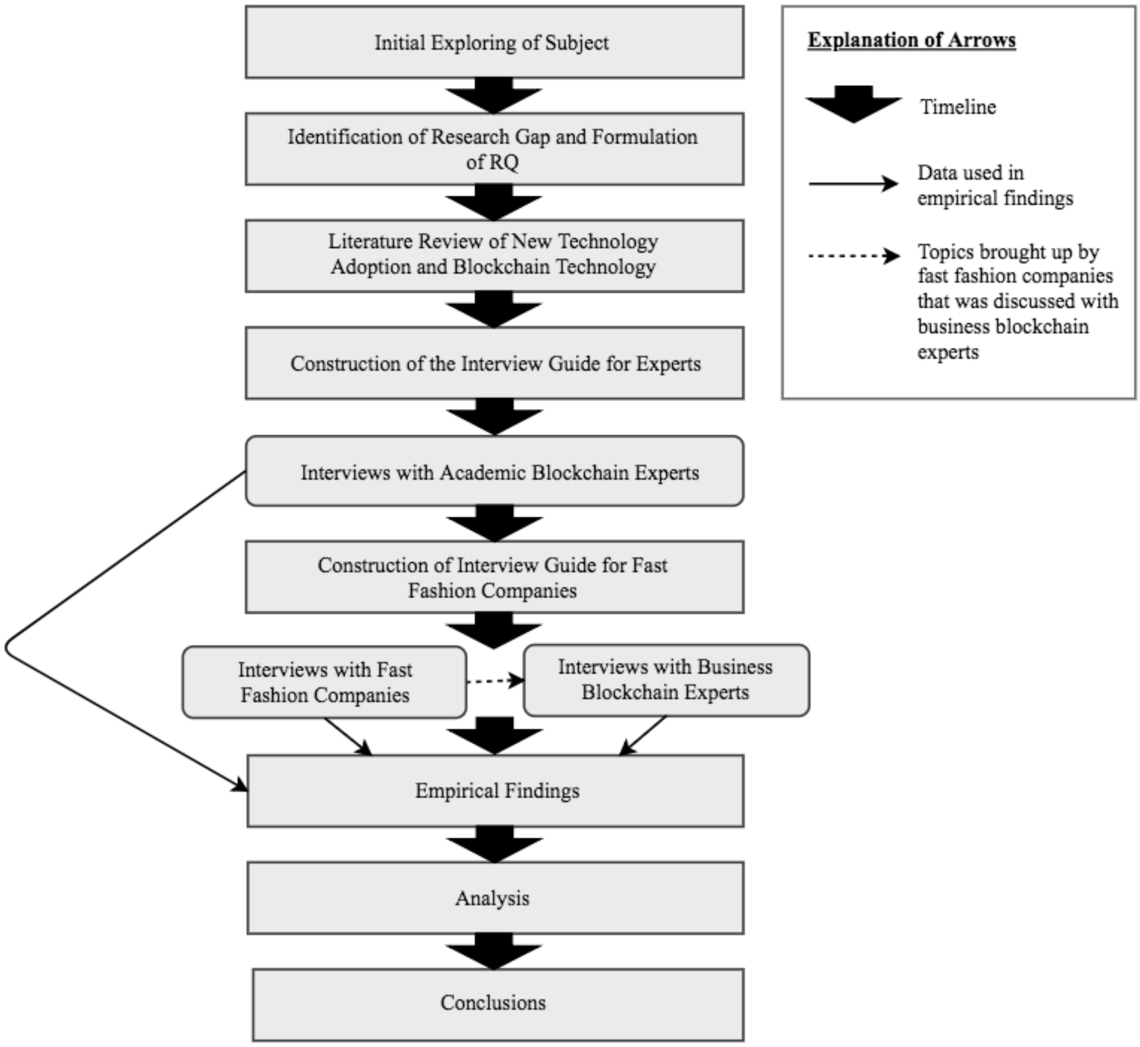

Figure 3.1: Summary of the Research Process. Compiled by authors.

3.2 Research Design

The research design of this study has an exploratory approach. In line with the abductive approach, different types of data were collected for its deductive and inductive elements. By performing a literature review, the study aimed to map and account for existing research and publications about new technology adoption as well as blockchain technology and its different configurations. This created ground for the subsequent qualitative interviews used to collect empirical data about the issue. The data collected from experts was then used as a complement to the literature and to extend the knowledge base of different configurations of blockchains. The data collected from fast fashion companies was used as a way to map the SCM in fast fashion companies.

An analysis model was created by extending literature review with identified themes from interviews conducted with experts and with fast fashion companies. The collected data from the fast fashion companies was discussed based on the analysis model in order to assess the compatibility of different configurations of blockchains. This assessment was made for each individual company, in an organisational level of analysis, as well as for identifying themes between the companies that could indicate the compatibility of different configurations in SCM in the fast fashion industry overall.

3.3 Research Method

The research method used for collecting data is based on a secondary and a primary data collection process. The initial data was gathered through a literature review based on secondary data. This data was collected by performing a systematic literature review and searching for information about the subject. After this, the primary data was collected by conducting qualitative interviews with experts and companies within the fast fashion industry.

3.3.1 Secondary Data Collection

The secondary data collection was initiated by searching for information about the subject before the focus of the thesis was completely determined. The authors started to search for information on the web with the aim to find the most relevant subjects to examine into more detail. After this search, the purpose and research question of the thesis were formulated, which thereafter were followed by a systematic literature review. This is a method for reviewing literature in an organised and predetermined way, which allows for a thorough and comprehensive review of the literature of a specified subject. (Bryman & Bell, 2011) A systematic literature review can be made in various ways, but was in this case performed by systematically going through material published in specified databases about the research fields relevant for the study, i.e. 'New Technology Adoption' and 'Blockchain Technology'.

3.3.1.1 Databases

Multiple databases were used in order to make sure that a sufficient number of relevant articles were found. However, a restriction of the number of databases used was made by assessing the trade-off between the limitation of time and the value of finding additional articles. The utilised databases were Emerald, Business Source Premier, Scopus and Google Scholar, which were chosen based on their field, range and quality of content.

3.3.1.2 New Technology Adoption

The systematic literature review of new technology adoption was made by searching for diffusion and adoption of innovation in different forms. The keywords included in this search can be found in Appendix A. As the focus on compatibility was determined, a new round of search focusing specifically on compatibility was performed.

The inclusion criteria were to include articles found in this search that was peer reviewed, published in established academic journals and that had a focus in line with the subject of the study. Some exceptions were made when articles were especially relevant for the study but not published in an academic journal. However, in such cases, only articles that had been cited in peer reviewed articles were included. The exclusion criteria comprised of articles written in other languages than English or Swedish, and articles that had a specific focus outside the scope of this thesis.

3.3.1.3 Blockchain Technology

The systematic literature review of blockchain technology was performed by searching for the keywords in phase 1 separately (Appendix A). After this search, a second search of keywords was performed in phase 2 (Appendix A), which were added to the initial keywords from phase 1. Articles were examined based on headings, abstracts and overall topics and were chosen by the authors based on the inclusion and exclusion criteria.

Inclusion criteria for the study were articles that were focused on general descriptions of the technology, different configurations or types of blockchains and blockchains in supply chains. Even though the firstly ever-published white paper about blockchain technology was published in 2008, it was not until 2015 that the technology became a subject of broad and current interest (Bauman et al., 2015). With this in mind, in addition to that the topic is new and quickly changing, the study has mainly focused on articles that are published the year 2015 or later, with exception of the first white paper written by Nakamoto in 2008. Inclusion criteria were further to focus on peer reviewed articles the extent it was possible. However, because of the newness and constant change in the research topic, other sources have been included in the literature review. These sources were most usually found by a snowballing approach through other academic articles.

By strictly focusing on information relevant for the research question, an exclusion criterion was that all articles with the main focus of cryptocurrencies were excluded with the exception of articles that mainly focus on explaining the public configuration of a cryptocurrency blockchain. Further, articles about blockchains as a paying method or financial services were excluded. Rather, as the focus of the study is the use of blockchain in SCM and different configurations of blockchains, articles regarding other opportunities within blockchain such as Internet of Things, Intellectual Property Rights and service development were excluded as well as articles with a focus on other sectors or industries. Exceptions from this were made when articles contained specific information about the different configurations or blockchains in supply chain management. Articles with the main focus on technical aspect, explaining the coding and programming of the technology was excluded due to that the study has a business perspective rather than pure technical perspective. A final exclusion criterion was that all articles that were not written in English or Swedish were excluded.

3.3.2 Primary Data Collection

Primary data was collected based on semi-structured interviews with both with experts about the blockchains technology and blockchain in supply chains and with companies in the fast fashion industry. Semi-structured interviews were performed by asking relatively open questions that were prepared in advance in a so-called interview guide. Unlike an unstructured interview, the semi-structured nature of the interview meant that there was a focus on the order and on asking the questions in a systematic way, but that room was still left for flexibility and for the interviewees to speak freely and elaborate as they wanted, which is not possible in a structured interview (Bryman & Bell, 2011). This type of interviewing was considered appropriate due to the exploratory and abductive approach of the study, where the different configurations of blockchains in the SCM is an unexplored subject that requires a possibility for new information be brought up. However, as the study aims to examine the compatibility of the different configurations, the interviews needed to have some structure in order to collect the necessary information for answering the research question.

3.3.2.1 Selection of Interviewees

To achieve a sufficient level of data gathered and to increase the external validity (Bryman & Bell, 2011), six companies within the fast fashion were interviewed. Fast fashion companies were chosen by using criteria based on the definition of fast fashion presented in section 1.1. Thus, the criteria were that the company should have a high focus on having an efficient supply chain, be in the lower segment of price range and have a high turnover of collections. Another criterion when selecting interview companies was that their headquarters should be located in Sweden or the UK, due to both time and space constraint of the researchers. In addition to this, eight experts within the field were interviewed, two from the academic and six from the business world. The business blockchain experts consisted of three blockchain consultants and three blockchain startup companies.

This distribution was made to include experts will different perspectives and experiences. An expert is defined as someone who is active in the topic of blockchain technology, e.g. by working with it, writing articles, participating in events or in other ways is especially knowing in the subject. This provided insights from several perspectives and thereby created a more nuanced portrait of the issue. Further, it enabled the findings from the companies to be compared and matched with the experts' views. The sample size of both fast fashion companies and experts were selected due to the limited time constraint of the study and to some extent also the access of interviewees.

The two academic experts were interviewed before conducting the interviews with the fast fashion companies as a complement to the literature review. As the literature about blockchain technology has just still started to emerge, this was done as a way to ensure that relevant issues of the configurations of blockchains were taken into account even if they have not yet been discussed in academic journals or other used sources. The six business experts were then interviewed in parallel with the fast fashion companies to create a possibility to discuss issues and topics that were brought up by the fast fashion companies.

The fast fashion companies were identified by searching the Internet, asking experts for referrals, and by calling out to the researchers' personal network. When companies had been identified, the aim was to identify and contact people with positions such as Supply Chain Manager, Chief Information Officer and similar. Regardless of role, it was important that the interviewee had an active role and insight in the supply chain management of the company. All companies of interest were contacted by email, either directly from the researchers or indirectly in cases where companies were first contacted by experts or personal contacts. The email described the researchers, the topic and in what way the companies could contribute to the thesis (Appendix B). To ensure that the potential interviewees possessed the appropriate knowledge, the email also described the purpose of the study and what type of knowledge that was desired from the interviewee. The companies that expressed interest to participate in the study then recommended a suitable person within the organisation to set up an interview with.

Identification of experts was made in the same ways as the companies, but also by the use of a so-called snowball sampling. This means that relevant persons from the initial search were asked to further suggest persons with expertise that could be of relevance for the study (Bryman & Bell, 2011). These persons were then contacted, and this process was continued until the sufficient number of experts had been found to interview based on the scope of the study.

3.3.2.2 Interview Guides

Two different types of interview guides were created, one for the experts and one for the fast fashion companies. The interview guide for the experts was created first because the interviews with academic experts took place at an earlier point in time. This interview guide (Appendix C) was based on the literature review regarding different configurations of blockchains. The interviews with the two academic experts and the literature review together then created the foundation for constructing the interview guide made for the fast fashion companies (Appendix C). This approach was followed to ensure that all relevant topics would be covered in the interviews with the fast fashion companies even if everything has not yet been discussed in the literature, which was important due to the novelty of the topic and the lack of existing research. Both interview guides were based on characteristics distinguishing the different configurations of blockchains, which had been identified in the literature review of blockchain technology.

Since the interviews with business blockchain experts were conducted in parallel with the fast fashion companies, topics that came up with companies could be further discussed with the business experts. Taking part of the knowledge and experience of the business experts about topics related to the configurations of blockchain technology gave the possibility of gaining a deeper knowledge about the subject. This was done in line with the exploratory and iterative approach of the data collection that was chosen due to the unexplored topic of the study. An iterative approach is advantageous in the sense that it enables the researcher to go back and forth to increase the understanding of the issue (Bryman & Bell, 2011). However, in order to ensure the comparability of the companies, the main questions for the fast fashion companies were not changed as the data collection progressed. Thereby, the iterative approach was used as a way to discover and discuss interesting topics brought up by companies rather than altering the interview guide.

Common for both interview guides was that the questions were carefully formulated to make sure that they incorporated an organisational focus, and were as simple and direct as possible so that they would be understood correctly and in a similar way by all interviewees. This was done to reduce the risk of receiving answers that would be difficult or even impossible to compare and analyse. When a first draft of the interview guides had been formulated, it was sent out to a test person with the purpose of getting feedback about the clarity and the relevance of the questions. Changes were then made based on the feedback that was given.

The finalised versions of the interview guides begin with general questions about the interviewee and about the subject, and then go over to more specific questions. The interview guide for experts consisted both of a general part about the configurations of blockchains, and the use of blockchain in SCM, and of a more specific part covering the eleven characteristics. Similarly, the fast fashion companies were first asked about general information about their supply chains in order to put their information into the right context, and then specific questions regarding the characteristics. In addition to this, the fast fashion companies were asked about their perception of each characteristic based on the way it is distinguished in the different configurations. This was done in order to reduce the influence of the researchers own perception of the companies' answers, giving them a chance to rank themselves, creating more neutral findings. Thus, the companies got to rank or describe each characteristic based on how they perceive its importance in their SCM. To exemplify, low is referred to a perceived importance of low or non-existent, and high is referred to high to unlimited importance.

Apart from the main questions, which are visible in the interview guides, room was also left in the interviews for asking follow up questions and discussing additional topics that were brought up. An overview of the topics from the interview guides was sent out to the interviewees one week in advance of the interviews in order to give them an opportunity to prepare for the interview. The reason for not sending the complete list of questions was to not affect the answers as the study aims to capture the topic from the interviewees' perspectives and how they actually experience it themselves.

3.3.2.3 Conducting the Interviews

Interviews performed face to face were preferred since it allows for more nuanced conversations and is considered to increase both the understanding and the personal engagement from the interviewee (Bryman & Bell, 2011). In the cases where the interviewees were located outside of Sweden, they were visited for face-to-face interviews. However, other communication channels such as telephone and video were was used as a second option when face-to-face interviews were not possible. Details about the interviews are presented in Table 3.1 and 3.2.

Due to confidentiality, all interviews have been kept anonymous in terms of the names of the people and the companies. The identities of the interviewees are not needed to fulfil the purpose of the research. Rather, the information obtained in the interviews was analysed based on the experts' knowledge about blockchains and on the companies' experience in the fast fashion industry.

BLOCKCHAIN EXPERTS					
Interviewee	**Referred to as**	**Title/Experience**	**Date & Duration**	**Location**	**Language**
Academic Expert 1	A1	*PhD, Associate Professor*, Head of Division of Department of Applied IT at one of the biggest Technological University in Sweden.	2018.02.27 60 min	Sweden	Swedish
Academic Expert 2	A2	*PhD, Associate Senior Lecturer* at the Department of Applied IT.	2018.02.28 45 min	Sweden	English
Blockchain Consultant 1	BC1	*Blockchain Consultant* at a management consulting company. Founded and worked as a business developer for blockchain companies since 2011.	2018.03.08 30 min	*	Swedish
Blockchain Startup Company 1	BSC1	*Manager* of blockchain startup creating a platform for freeing up capital in global supply chains.	2018.03.14 30 min	United Kingdom	English
Blockchain Startup Company 2	BSC2	*Co-founder & Chief Operating Officer* of a blockchain startup creating a platform based on blockchain for cross-border trade.	2018.03.20 30 min	United Kingdom	English
Blockchain Consultant 2	BC2	*Consultant* for supply chain solutions and blockchain technology.	2018.03.21 60 min	United Kingdom	English
Blockchain Startup Company 3	BSC3	*Co-founder* of a startup creating a technical interface for digital assets on the blockchain with goods in supply chains.	2018.03.23 60 min	United Kingdom	English
Blockchain Consultant 3	BC3	*Senior Strategy Consultant* within global trade digitisation in a technical company.	2018.04.16 45 min	*	English

* Interview was conducted via Video Call

Table 3.1: List of Interviews Blockchain Experts

FAST FASHION COMPANIES					
Interviewee	**Referred to as**	**Title**	**Date & Duration**	**Location**	**Language**
Fast Fashion Company 1	FFC1	*- Supply Chain Manager*	2018.03.12 45 min	Sweden	Swedish
Fast Fashion Company 2	FFC2	*- Logistics Coordinator*	13/03/2018 60 min	Sweden	Swedish
Fast Fashion Company 3	FFC3	*- Group IT Director* *- Enterprise Architect*	2018.03.15 60 min	United Kingdom	English
Fast Fashion Company 4	FFC4	*- Senior Vice President*	2018.03.22 60 min	*	English
Fast Fashion Company 5	FFC5	*- Business IT Solutions*	2018.03.22 45 min	*	English
Fast Fashion Company 6	FFC6	*- Chief Information Officer*	2018.04.06 45 min	Sweden	Swedish

* Interview was conducted via Video Call

Table 3.2: List of Interviews Fast Fashion Companies

During the interview with Fast Fashion Company 3, an additional interviewee joined. It needs to be taken into consideration that the two interviewees might have affected each other in their responses. However, one of the interviewees (Group IT Director) was the one mainly answering the questions while the second interviewee (Enterprise Architect) was filling in only when the first interviewee had already answered. Thus, as the Group IT Director provided the majority of the answers and always spoke first, the answers were not considered to have been influenced to large extent.

All interviews were recorded to avoid the risk that information would be lost. All interviewees were asked for consent before the interviews were started. In addition to this, some notes were taken to facilitate to follow up and referring back to especially interesting topics during the interviews, but also to be used as a complement in the transcription process that took place after the interviews. Apart from recording and taking notes during the interviews, constant record keeping was held during the whole research process to keep track and enable peers to act as audits of the process. This goes in line with what Bryman and Bell (2011) define as an auditing approach, which increases the dependability of the study.

When the interviews had been performed, the recordings, and to some extent the notes, were used to transcribe the interviews. The interviews were transcribed to allow the information obtained to be coded and analysed. The transcription process started as soon as the first interview had been conducted and continued in parallel with the on-going interviews. When all of the interviews had been performed and fully transcribed, a respondent validation was made, meaning that a summary of the interview was sent to the interviewee for check control. In accordance to Bryman and Bell (2011), this decreases the risk that the author's own perspective, subjective views and interpretation mislead the data by enabling the interviewees to control and confirm that all data was correctly interpreted, thereby increasing the authenticity and credibility of the data. In case of discrepancies between the transcribed interview material and the perceptions of the interviewees, corresponding changes were made.

The majority of the interviews were conducted in English. However, in cases where all participants in the interview had Swedish as mother tongue, the interview was performed in Swedish instead. This because it enables the interviewee to be more comfortable, speak more freely and for the researchers to capture more nuances of what is said (Andrews, 1995; Tsang, 1998). These interviews were transcribed and translated into English and the translation was then sent to the interviewee for respondent validation to make sure that no content was lost or substantially changed in the translation.

3.4 Data Analysis

The main analysis tool used was thematic analysis, which is a qualitative analysis tool (Bryman & Bell, 2011). As the aim of the interviews were to discuss and take part of the interviewees perspective on the different configurations and the characteristics distinguishing them, the interviews were colour coded after the characteristics identified in the literature review of blockchain technology. Both authors coded the transcriptions on their own, compared the results and then discussed the differences, when such occurred, before jointly deciding on the final coding. This was done in order to increase the quality and to reduce the risk of the authors' personal views to affect the result. When all interviews had been coded, they were compiled and presented in the empirical findings (chapter 4). The empirical findings were then analysed and presented in chapter 5 of the study by comparing the findings from the experts and from the fast fashion companies to each other, and to the literature. In order to do this, an analysis model was constructed (section 5.1.2). The model was constructed based on the compilation of characteristics distinguishing the configurations of blockchains that were summarised in the literature review and identified themes from the empirical findings from blockchain experts and fast fashion companies. The characteristics were divided into clusters based on the way the characteristics were described in the interviews. It was also identified that there are trade-offs evident between these clusters (see section 5.1.2). The model was then used as a way to discuss and assess the compatibility of the different configurations of blockchains in the SCM in the fast fashion industry.

3.5 Research Quality

The quality of the research is affected by the research criteria validity, reliability and replicability (Bryman & Bell, 2011). Hence, in order to assess the research quality of this study, these criteria will be discussed in the following sections.

3.5.1 Validity

The validity of research refers to the quality of the conclusions and can be divided into internal and external validity. The internal validity is concerned with the causality in the study and how well the conclusions that are drawn match the empirical findings (Bryman & Bell, 2011). In this study, the internal validity was enhanced by the fact that the all interviews were transcribed and sent to the interviewees for validation. Further, it was also enhanced by the fact that the fast fashion companies were asked to rank the characteristics themselves. All of this decreases the risk of findings becoming misinterpreted and leading to questionable conclusions. The external validity is instead concerned with the generalisation of the findings, i.e. if the findings from this study are viable in another setting (Bryman & Bell, 2011). In order to increase the external validity in this study, multiple blockchain experts and fast fashion companies were interviewed. However, the sample of experts and companies used in this study is still limited and it can therefore be questioned to what degree it can be generalised to the whole industry. This is a common difficulty in qualitative research since it often has small samples (Bryman & Bell, 2011). However, the limited number of interviewees was due to the time and access constraints. The authors dealt with this issue by providing a thick description of the data collected and the setting it was collected in. According to Bryman and Bell (2011), this increases the possibilities for the readers to assess the generalisation themselves. Furthermore, the findings from the fast fashion companies, with the exception of one company, showed similar patterns, which strengthens the external validity.

3.5.2 Reliability

The reliability of the study measures how repeatable the study is, i.e. if the results would be consistent if a similar study would be made (Bryman & Bell, 2011). More specifically, if another researcher would come to the same conclusions (Lecompte & Goetz, 1982). The reliability of research refers to the quality of the conclusions and can be divided into internal and external reliability. The external reliability is referring to in what degree the study can be replicated (Bryman & Bell, 2011). Due to that the topic of the study concerns a newly emerged technology that is constantly under change in a research field that is fast moving, the results may differ in the future as the adoption of blockchain technology might be further developed. Hence, the observations and conclusions made in this study are running the risk of being obsolete in a short time. However, since this research can lay the foundation for the future adoption, it still considered being relevant to study.

Internal reliability is referring to if the researchers agree on the interpretation of the data collected in cases when there is more than one researcher participating in the study (Bryman & Bell, 2011). As a way to strengthen the internal reliability in this study, both authors participated in all interviews, coded the transcribed interviews separately and performed the subsequent analysis collaboratively. Further, the researchers took, as mentioned above, an auditing approach, which according to Bryman and Bell (2011) increases the dependability.

3.5.3 Replicability

The replicability of the study refers to the degree to which the study can be replicated. A necessary condition for having replicability is that a lot of details about the study are included. (Bryman & Bell, 2011) The procedure of this study, from compiling the literature review, the setting of the interviews, coding the data, building the analysis model and conducting the analysis, have therefore been described in detail in order to increase the possibility for a future researcher to replicate the study. Also, the rationale behind all decisions was described. In order to clarify further, a model of the overall process is presented in section 3.1.

4. Empirical Findings

This chapter will present the empirical findings from the experts and the fast fashion companies. The first part will present the findings from the experts in the same order as was done in the interviews, i.e. beginning with the general part of blockchains, and then continuing to the characteristic distinguishing the configurations from each other. The second part will present the findings from the fast fashion companies, also in the same order as was done in the interviews, i.e. beginning with general information about their supply chains and then the perceptions of the characteristics.

4.1 Blockchain Experts

The following section will present the empirical findings from the blockchain experts. A list of abbreviations of the respondents is found in section 3.3.2.3.

4.1.1 General View of Blockchains

The sections below will present the blockchain experts' general view of blockchains and of blockchains in supply chain management.

4.1.1.1 Different Configurations of Blockchains

When asked about their views of the main configurations of different blockchains, the experts' answers were divided. According to Academic 1 (A1), there are only two different blockchains, "real blockchains", which he refers to as public blockchains, and "fake blockchains", which he refers to as blockchains that are owned and controlled by a central authority. Academic 2 (A2) refers to blockchains as either being public, meaning the open source and original type of blockchain, or permissioned, where the control is limited to a selected network that is not open for everyone. In permissioned blockchains, he describes that there are the private blockchain that is run by one actor and the consortium blockchain, which includes multiple actors. However, although A2 refers to all these as blockchains, he mentions that many claim that permissioned blockchains are not even blockchains and that these blockchains are argued to lose the original idea of blockchain as a concept.

The business experts generally distinguish the types as public blockchains and more restricted blockchains. Blockchain Consultant 2 (BC2) explains that in a restricted permissioned blockchain, you cannot join the network if you are not invited and all parties involved are trusted and identified, while in a public, all can join and all actors are anonymous. Blockchain Consultant 1 (BC1) describes it in a similar way and defines the two different blockchain configurations as a fully public blockchain and a consortium blockchain. BC1 explains that this second version is limited to a certain group of actors of who can write, see and validate transactions. BC1 and A2 explain that due to that the number of actors can be restricted, the consortium is very adaptable, meaning that it can be coded to achieve different traits, not necessarily laying exactly in between a private and a public blockchain.

The private blockchain with one central authority is not commonly mentioned by the experts. Both BC1 and BC2 question why you would like to build a blockchain if you are alone. A1, who refers to private blockchains as "fake blockchains", explains that the window of opportunity for these blockchains is very slim. He further argues that compared to a traditional database, the lower efficiency and higher environmental cost make this type obsolete and very ineffective if the company trust the central authority. A1 is further sceptical to the hybrid version of a consortium blockchain and claims that the idea of restricting participation results in losing the concept of blockchain technology.

"I usually say that if you are working alone, then you might just have a traditional database"

- BC1

BC1 does not really see a big difference between a fully private blockchain and a traditional database since one single actor controls it. He suggests that would be a poor choice as it brings a lot of the negative aspects of a blockchain but not as much of the benefits. A2 also mentions that there might be a lack of point in choosing a fully private, but mentions that it depends on what you are after. He mentions that a distributed database would be an alternative for increased security while BC1 suggests an open database as an alternative to using a private blockchain if the benefit of transparency is desired as only the central authority has the power to make changes and verify transactions anyway. A1 claims that private blockchains rather will be used for reputational purposes and as a way for companies to market themselves. A2 argues that companies use permissioned blockchains in order to create attraction and publicity but also because they are perceived as less risky as fewer actors are involved. Both A2 and BC2 argue that the permissioned blockchains are more suitable to use in a business environment. A2 further mentions that companies can build an internal pilot with a private blockchain as a way to learn.

"I think all types will be used in parallel, but for different purposes."

- A2

The quote above refers to the need of looking closer at the purpose of the blockchain. When deciding on which blockchain to choose, both A2 and BC1 both stress the importance of looking into the exact reason and aim of using the blockchain, due to that there are different trade-offs between them. They argue that finding the configuration that is the best suited is much dependent on what the company does, needs and wants.

4.1.1.2 Challenges of Blockchains in Supply Chains

All respondents mention that supply chains could benefit from blockchain technology. When asked and answering about specific challenges that might occur, three main subjects were discussed that will be described below.

Data Input & Human Error

A few of the respondents (BC3, BSC2, BSC3) mention that even though blockchain technology enables immutability, there is still a risk that the entered data might be wrong to begin with. For example, Blockchain Consultant 3 (BC3) mentions that there is still a risk of human error when the data is put onto the blockchain or when controlling the ID. Blockchain Startup Company 2 (BSC2) and Blockchain Startup Company 3 (BSC3) mention the expression "garbage in, garbage out" as a way of explaining that if the data that is entered onto the blockchain is not correct, it is irrelevant whether the data is immutable. Blockchain Startup Company 1 (BSC1) and BSC3 say that even though blockchains help to reduce human error, there will be a risk of human error until everything gets fully automated, e.g. by the use of IoT and for example robots scanning the container and all garments. In similar, BSC3 argues that IoT and the use of sensors as a way to trace clothes can help and describes that some companies already use sensors in combination with blockchain, but not yet in mass-scale. Several of the respondents (BC1, BC2, BSC2, BSC3) agree that the use of IoT and other technologies in combination with blockchains will improve its potential performance.

Physical Assets to Digital Record

When discussing the immutability of the blockchain and the potential human error, all business experts expresses that a difficulty in supply chain management could be to transfer the physical data to the digital record in a secure way. BC1 mentions that finding a proper digital ID without a failure point is something that might be difficult to do with goods where it is difficult to define something unique. BC2 and BSC3 give examples of new technologies that currently are being developed that potentially could solve the problem of transferring physical assets to a digital record. They describes two different kinds of technologies that are under development where the main function is to create a register of the substance of a material, creating a sort of digital ID that anyone in the supply chain can scan to verify the physical asset to the digital record, thereby helping with the problem. BSC3 describe it with the following quote:

"This solves so many problems of 'what happens if bad data gets on the blockchain'. It won't stop people from doing mistakes, but it provides enough verification there that we can check if it's actually correct."

- BSC3

IT Capacity at Suppliers

BC3 and BSC2 express that not all suppliers down the supply chain might be able to run the network (be nodes) due to their lack of IT capacity. BC3 further argues for that the smallest suppliers might not have to be nodes in order participate. BC2 mentions that fast fashion companies probably will work with different types of suppliers, where some of the suppliers will not invest in mature IT. He continues to explain that he does not really see this as a problem since he claims that it is not very expensive to upload information on the blockchain and that only a smartphone and Internet connection are needed. Another solution that BC2 sees becoming possible in the future is that external certification organisations will collect the data and upload it on the suppliers' behalf, driving down the cost. Similarly, BSC2 mentions that a solution to ease the hurdle could be that a bigger organisation helps to input the data for the supplier.

4.1.2 Characteristics of Different Configurations of Blockchains

The section below will describe the view of the experts regarding each of the eleven characteristics identified in the literature.

4.1.2.1 Consensus power

In regards of consensus process and participants in the network, A2 mentions that the owner has full consensus power in a private blockchain. A1 explains that the consensus power in a public blockchain is distributed. BC1 explains that in public blockchain, it is usually a question of computing power, rather than votes like it is in the consortium blockchain, to reach consensus in the validating process. A1 explains that in public and consortium blockchain, the consensus is reached when over 50 % of the network reaches consensus rather than that you trust the central authority. BSC2 says that a consortium blockchain is useful due to that trusted users have the consensus power to verify each other's transactions. BC1 explains that instead of a central point having the only copy, the selected network each has a copy and validate transactions if changes are made. He further says that the majority of the selected network needs to reach consensus when validating transactions. BC2 explains that you cannot join the network in a consortium blockchain if you are not invited and that all parties involved are trusted and identified, while in a public all can join and all actors are anonymous. BC1 further mentions that consensus power and number of actors are choices that need to be made in the implementation of blockchains since the different types have different number of actors.

4.1.2.2 Immutability

Almost all respondents (A1, A2, BC1, BC2, BSC2, BSC3) bring up security, in terms of immutability, as a benefit of using blockchain technology. BC2 explains the benefit of immutability as follows:

"I am seeing the data at the same time you are seeing it and I know you cannot change it and I cannot change it, so it is immutable, it is final. ... Even if we try to change it, your version might change but our collective version would not change."

- BC2

BSC3 explains that in a private blockchain, there is less certainty of full immutability than in a consortium blockchain or public blockchain due to that there is an increased probability to rewrite the history. A1 describes that in terms of immutability, the public blockchain is the best in both security issues, as you need to breach the majority of the network.

"The fewer nodes the less secure. If you restrict the numbers of nodes then the security risk of data manipulation will increase."

- A1

BC2 mentions when discussing immutability that he is not aware of that security would increase with increasing numbers of nodes. He questions why it would be more secure to rely on thousands of unknown and not trusted individuals rather than a trusted network in a consortium. BC2 mentions that in a consortium blockchain, somewhere between 10 and 20 trusted actors being nodes would be enough to make it secure in terms of immutability. Everyone else could instead be participants. When discussing immutability, BSC3 argues for that in a permissioned blockchain, the exact number of nodes might be less important than in a public blockchain since you trust the actors taking part of the network.

4.1.2.3 Protection Against Cyber Attacks

Almost all respondents (A1, A2, BC1, BC2, BC3, BSC2, BSC3) bring up security, in terms of protection of cyber attacks, as a benefit of using blockchain technology. BSC2 and BSC3 mention that there is a high risk of problems occurring in a supply chain if it is not secure. Many of the respondents (A1, A2, BC1, BSC3) mention an increasing security as more actors join the network. This means that a public blockchain, which has the possibility of unlimited actors, is the most secure and the private blockchain has the lowest security. This is explained to be because of the increased copies of the ledger that needs to be hacked to corrupt the system. BC1 explain this with the following quote:

"Public blockchains are more secure since there are more actors that have copies and validate the blockchain."
- BC1

A1 and BC1 mention that you can technically break the encrypted chain but that it is very expensive as the network grows larger and mentions that the security is higher with a fully public blockchain. BC1 explains that it is much harder to breach a public blockchain compared to one or a few points of failure since there is less security the fewer nodes there are. A1 argues that each node increases the value of the total network, but states that there is likely to be an upper limit of the value it can provide. BC1 mentions the security is higher in blockchain technology than in a traditional database since there is no single point of failure because all actors have a copy of the leger.

4.1.2.4 Scalability

Many of the experts (BC1, BC2, A1, A2, BSC3) expressed that a public blockchain is slow and scale quite bad compared to a permissioned blockchain. For example, BC1 mentions that a private and a consortium blockchain can handle many more transactions per second than a public. A1 explains that this lack of scalability usually is a design choice made by the developers in order to make the system more secure. When deciding on what type of blockchain to use, A2 describes scalability as a trade-off choice between scalability and security, both in terms of protection against cyber attacks and immutability, due to that the mechanism that makes the public secure also slows down the process. He further explains that in order to have high performance in scalability, you need to compromise with other benefits related to the blockchain. A2 states that if a company wants high scalability, a private would be the best choice.

BSC2 explains that they are currently building their platform on a public blockchain but are aiming to change to a consortium version because the public blockchain transactions are slow. She explains that a consortium offers an increased speed compared to the public blockchain and is cheaper. BSC3 argues for that a public blockchain is too slow for a global supply chain system. BC1 refers to that because of the scaling problem, and the fact that it is expensive to put information onto a blockchain, companies might only want to put information that they want to be secure onto a blockchain. BC3 is stressing the importance of not overusing the blockchain by putting too much information on to the blockchain since more transactions will make the system slow. He describes it as follows:

"I think it's very important to not put everything on blockchain. So I would say if you use blockchain in a correct manner, you could enhance supply chain visibility and supply chain communication. But if you overuse blockchain you could also kill it by slowing up all the processes and make it cumbersome. It's very important to find the right balance."
- BC3

4.1.2.5 Cost

Many of the respondents (A1, A2, BC1, BSC2, BSC3) mention that in a private and consortium blockchain, transactions are much cheaper than in a public blockchain due to the lower amount of actors. A1, BC1 and BSC3 argue that a public blockchain is very expensive in terms of the computing and energy power needed to run the network with many actors. A1 explains that new technologies have usually decreased the transaction costs in the past but that blockchain technology is instead increasing the transaction cost. He continues to describe that you pay a higher price in a public blockchain in order to not be reliant on trusting the central authority and to get higher security. BC1 mentions that it is very difficult to define the exact cost since the projects so far mainly have been pilots and that this is something important to look into when choosing to implement. BSC1 explains that it is probably quite expensive to build a blockchain. A1 states that blockchain technology likely will lower the integration cost for the company compared to more developed traditional integrated systems.

4.1.2.6 Existing Trust

Many of the experts (BC3, BSC1, BSC2, BSC3) agree that there seems to be a general lack of trust between all the involved actors in a supply chain, resulting in the use of one or many middlemen. BSC3 explains that actors usually trust each other within their closest trading relationship, but that actors usually do not have trust beyond those relationships. BC2 claims that companies trust these middlemen only because they have to and that companies probably would want to avoid them if they could. A common mentioned possibility when using blockchain in supply chain is exchanging value without having existing trust between the actors, which reduces the need of middlemen. When discussing this, A2 says that trust is managed by computers rather than humans, meaning that the required level of trust is low. BC2 claims that blockchains build trust by the fact that everyone sees the same information.

A1, A2 and BC1 claim that public blockchains are the most efficient when there is low trust in the system or in the central authority. BC1 further mentions that in a public blockchain, you do not need to trust the other parties since the technology will economically incentivise the actors to behave. A2 explains that when in a situation with no trust, the public blockchain is the only one that currently lives up to the minimal level of trust created in a network. A1 mentions that in a permissioned blockchain, on the other hand, you trust the actors involved. Thereto, BC1 describes that you have to trust every participant in a traditional database and a private blockchain, especially the central authority, while in a consortium, the actors only have to trust that the majority of the identified and trusted actors act in good faith. BSC3 mentions that heavily regulated industries probably would prefer permissioned blockchains as they have a high value of being able to identify all participants and have high trust in knowing that they behave according to rules or otherwise can be excluded. BC2 claims that permissioned blockchain works for businesses due to that companies generally want to know and trust whom they are working with. It is commonly mentioned that the level of existing trust is an important factor in blockchains. A2 states that when deciding if and what blockchain is necessary, it is important to look into how serious the trust problem is in the network.

4.1.2.7 Flexibility

When discussing the flexibility of the different configurations, A2 and BSC3 describe the private blockchain as being more flexible since the central authority have more control, while nobody has that much power on their own in a public blockchain, which makes it less flexible to change rules. A1, BC3, BSC1, BSC2 do not mention or do not know much about the level of flexibility in the different blockchain configurations. BSC3 refers to, what he calls, a governance problem in how to control and change rules regarding the actors' behaviour on the public blockchain. As an example, he mentions that sometimes information needs to be deleted, such as when encoded illegal documents get stored on one of the blocks in a public blockchain. BSC3 explains that it is nearly impossible to delete these documents or punish such behaviour in a public blockchain. BSC3 further explains that he sees a lot of advantages of the consortium and private blockchains comes from being governed and flexible. BSC3 believes that some kind of control and flexibility probably is needed in a business setting but also mentions that some people like the inflexibility of the public blockchains since it sets clear rules. BC2 explains that flexibility is important in the fashion industry because of the fact that trading patterns change all the time, meaning that it is very dynamic.

"In public blockchains you need consensus - everyone needs to agree on the rules. So, for a change in the rules, everyone needs to update their client to make the changes, and this is very hard and difficult to do. So generally, if you want a more flexible system, then more a permissioned blockchain is better."

- BC1

In regards to the quote above, BC1 expresses that a public blockchain is quite inflexible and that it is difficult to change rules once the blockchain has been designed. BC1 continues telling that this could both be an advantage or a disadvantage depending on what you want and that it is a question of trade-offs between the benefits. BSC3 also mentions that there is a trade-off between flexibility and security in form of immutability. The private blockchain is more flexible but it is less certain that the ledger represents the accurate record. BC1 also mentions a trade-off and explains it as follows:

"I usually call it a trade-off between public blockchain that is more secure since it is more actors that validates this type of blockchain. In the meantime, private is more flexible and is able to handle more transactions per second, thereby it scales better. So it depends on what functionalities someone wants."

- BC1

When discussing this trade-off, BC1 suggest to use a consortium blockchain for the day-to-day transactions and that, for example at the end of the day, a timestamped checkpoint of the ledger gets transferred to an existing public blockchain. This is something BC1 would recommend for the supply chain management in the fashion industry since it will bring scalability, flexibility and privacy while ensuring high security and certainty to the end-of-the-day timestamped ledger. This option is not mentioned by any of the other respondents.

4.1.2.8 Privacy

A1, A2, BC1 explains that you can control and encrypt the data so that the information that is visible on the blockchain can be controlled and different information can be shown for different actors. A1 and A2 say that this is decided when the blockchain is built. BC2 explains that the use of, what he calls, channels in a consortium blockchain could enable one supplier to supply to several competitors and still conceal confidential information for them, meaning that only the actors that need to see the information will be able to do that. BC2 and BSC3 mention that in theory, encrypted information could be distributed to parties but mentions that companies probably would feel safer to only send important confidential information to involved parties, even if encrypted. BC1 explains that all information that the actors want to be validated and secure must be made public, while metadata such as identity could be encrypted and hidden to all except certain actors but then the data will not be validated and secured.

One solution mentioned by BC1 is to create a digital fingerprint (hash) of the data to be validated without the network actually receiving the information behind the fingerprint. BSC1 also says that personal information can be concealed by a private key, even though all transactions between the public keys are broadcasted over a whole network, enabling the information behind is concealed. He continues to explain that you for example can conceal exactly what content that is inside the container that is being transported. BSC1 says that a company needs to find a balance of how much it wants to reveal and how much you want keep private and confidential. One problem for fashion companies could be the new privacy legislation GDPR saying that personal information needs to be protected, which according to BSC3 is impossible to assure on a public blockchain.

4.1.2.9 Incentives

When implementing a blockchain, A2 explains that the design choice that needs to be decided is how to incentivise the actors running the network. BC2 explains that the blockchain needs to have some sort of value for every participant, which for example in a consortium is based on being part of the network. A2, BC1 and BC2 explain that in a public blockchain, a monetary reward, for some blockchains called mining, is usually used in order to incentivise people to participate and maintain the infrastructure due to that all actors are unknown and do not trust each other. A1 explains that this logic is due to the participants takes on a financial burden by using computing power to maintain the network and an incentive is thereby needed in order to run the system. In a private blockchain or consortium blockchain, A2 and BC1 explain that there is usually no need of incentives based on monetary rewards since the actors that are running the network have a stake in the network. Thereby, the incentives for these blockchain configurations are referred to as stake in the network. BC2 believes that in a consortium blockchain, participants run the network because they see a value being part of the network and not because an authority is forcing them.

4.1.2.10 Transparency

Many of the respondents (A2, BC1, BC3, BSC1, BSC2, BSC3) bring up transparency as a benefit of using blockchain in supply chains. For example, BSC2 explains that with blockchain technology, the network has one single truth that all have agreed upon instead of all parties having different. A1 mentions that there is higher transparency in a public blockchain since the information is fully distributed, secure and not controlled by one or a few actors, which enable a flow of information rather than having information in many unreachable centralised places. BSC3 explains that in order to be certain of that the cotton is organic, the companies normally need to go back many tiers in the supply chain, which something that is not very common or easy since not many actors want to disclose information about their suppliers. According to BSC3, blockchain would make this an easier process due to the immutability of the data it creates, which in turn increases traceability.

4.1.2.11 Traceability

Many of the respondents (A2, BC1, BC3, BSC1, BSC2, BSC3) also bring up traceability as a benefit of using blockchain in supply chains. BSC1 describes the possibility to track a package or shipment from one place to another and once it has arrived the possibility to scan to receive information of the origin as very beneficial. BC2 also mentions that it enables to be able to track for example exactly where a truck is and when it is planned to arrive.

"And depending on if they are internally willing to identify where stuff comes from or if the company want to independently prove that"

- A1

In relation to the quote above, A1 explains that if a company internally wants to be sure about a product's origin, a private blockchain might suffice. On the other hand, A1 explains that if the traceability is to be used to market out to customers rather than to ensure immutability, a public blockchain could be an option due to increase the security of traceability. BSC3 mentions that even though a brand is trusted, it could still be valuable for the customer to be certain of the traceability, as it becomes a way of strengthening the brand. He explains that one possibility would be for a customer to scan a barcode to be able to see all the input data and the origin of the product. BSC2 explains that by increasing transparency and traceability, brands can market themselves as sustainable and ethical with the blockchain as proof.

4.2 Fast Fashion Companies

The following section will present the empirical findings from the fast fashion companies. A list of abbreviations of the respondents is found in section 3.3.2.3.

4.2.1 General Information about the Supply Chains

Fast Fashion Company 1 (FFC1)

As a fairly new company, FFC1 explains that its supply chain is not very advanced. Currently, one single supplier accounts for 30 to 40 per cent of the supplied products. The remaining suppliers are more dispersed and consist of both large and small actors. The majority of suppliers are located in China, Turkey and a smaller number in Bangladesh and India. One challenge brought up by FFC1 in regards to the SCM is the vast amount of documents needed throughout the supply chain. An important part of the SCM is also said to be their sample process, which FFC1 describes as a way for the company to control and get insight into the production. FFC1 states that it has a positive view of innovation. However, the company says that it would prefer to implement innovations as early as possible in the chain as the investments become greater the later in the chain that changes are made since the value of the product increases as it goes down the chain. When discussing the potential use of blockchains, the company thinks that an advanced technology such as blockchain technology might be beneficial first in a few years when the company has grown and developed its supply chain.

Fast Fashion Company 2 (FFC2)
FFC2 describes that the company has a vision of being simple. It started out as a small company, and this view has remained despite the fact that the company has grown substantially over the years. The suppliers are based in Asia and Turkey. However, basically, all purchases are made through intermediary agents, which means that the company has little direct contact with the suppliers. FFC2 describes one challenge being the IT capacity. The company has an old IT system, lacks IT resources and a lot of activities are still performed manually. IT is mentioned as something that could solve many of the problems the company is facing, such as keeping track of products and logistics in general. When talking about innovations in the SCM, FFC2 says that its current work practices are sufficient, but that they could be significantly improved. Therefore, FFC2 says that it could be beneficial for the company to take the next step. The company has little prior experience of implementing innovations, but do think that the company has a positive view of innovations. FFC2 states that the company has no direct experience of blockchain technology and did not have any specific view of the technology.

Fast Fashion Company 3 (FFC3)
The SCM of FFC3 is described as being fairly traditional. Most suppliers are concentrated in China and Bangladesh, but it also has some local suppliers in the UK. The company owns some of their suppliers. FFC3 mentions that one of its biggest challenges is to manage the demand of the market and the capacity of its suppliers. An especially important part is the samples going back and forth, which requires close communication, information flow and seamless management of the physical goods. FFC3 says that the physical parts need to be able to be checked and controlled at any part of the supply chain. When talking about innovations in the SCM, FFC3 says that it depends on the type of innovation. The company sees more innovation coming into the sample process where the physical samples are manually handled and are argued as being difficult to register in the IT system. It also pointed out that the company would like to see more innovation in the part of the supply chain focused on manufacturing and shipping. When discussing blockchain technology, FFC3 argues that it is important to translate a technology into use cases. The company hopes that blockchains can provide improvements, but thinks that it will come to compete with a lot of other innovations.

Fast Fashion Company 4 (FFC4)
FFC4 says that it owns the production of some product categories, but not all. The production that is outsourced to external suppliers is spread across the globe. In many cases, these suppliers are reached through intermediary agents or buying houses. The suppliers are spread to Asia, and to some extent also Europe. FFC4 describes a problem related to changes in demand as demand patterns are not always evident at the time where you have to make the decisions about the supply. The company would also like to see a more accessible information flow. When talking about innovation, FFC4 describes that it is practical, focusing more on increasing the information flow and visibility in the supply chain, rather than on new, advanced, technologies. FFC4 considers blockchain to provide different benefits depending on the type of fast fashion company. FFC4 says that blockchain can work as a way to showcase the authenticity and provenance of a good, to provide transparency and efficiency

and thereby having better visibility of where the goods are and an ability to trace back and identify work practices to ensure that the company pursues fair labour protections, or to simply determine that you are actually getting the product you were promised.

Fast Fashion Company 5 (FFC5)

FFC5 begins with explaining that it has a lot of different tiers of suppliers, meaning that there are a lot of steps going from the company and through all processing steps all the way back to the cotton farmers. The company also has a large number of suppliers with whom it has direct contact. The company operates across a lot of different geographical regions, where the biggest regions are China and Bangladesh. The company sees one of its biggest challenges related to managing the diversity of its supply chain. As many suppliers work with multiple factories at once, it quickly becomes a lot of actors to keep track of. The company currently does not see further back than to tier one and two but would like to see that change. When talking about innovations in the SCM, FFC5 says that it sees possibilities in going from paper-based solutions to more digital alternatives and making data collection more efficient. The company also says that they want to collaborate with others in order to find solutions and move things forward. The company has no prior experience of blockchains but sees the technology as a way to increase traceability in the supply chain. It is currently looking at a blockchain pilot to be introduced next year. The company sees a benefit of blockchain by ensuring that data is correct and enabling sharing of data in a sensitive way.

Fast Fashion Company 6 (FFC6)

FFC6 describes that the company has some primary suppliers that it works with. The majority of its suppliers are located in Asia and Turkey and it has relationships directly with the suppliers. The company mentions its biggest challenge being the management of its samples. The company wants to get more information about the arrival time of the samples and also to make sure that they arrive at the right time. When talking about innovations in the SCM, FFC6 explains that the company has implemented a number of innovation projects to improve processes and systems. However, the company is more concentrated on innovating in the part of the supply chain that is aimed to the customers than to the suppliers. It says that it would like to see collaboration between different actors as it is difficult for a single actor to change things, especially as it comes to sustainability issues. The company describes that it feels unsure of the benefits blockchain can provide in its SCM. It states that it is important that the benefits are clear enough if it is going to consider an implementation. FFC6 also says that it is crucial that the benefits are clear enough for the suppliers in order to get them to want to participate.

4.2.2 Characteristics of Different Configurations of Blockchains

The section below will describe the companies' view of the eleven characteristics identified in the literature one by one. After presenting the findings from the discussion of each characteristic, the result of the companies' stated perception based on the alternatives distinguishing the different configurations will be presented.

4.2.2.1 Consensus Power

When discussing the design of the validation process and how the consensus power would look time in a potential implementation of blockchain, no company states that it knows how they would want it to be. FFC2 states that it could consider collaborating with both competitors and suppliers but are more positive towards partnering up with suppliers. In comparison, FFC3 does not know whether the company would like to collaborate with others or not. The company says that they think that this is something they would discuss with their extended supply chain before initiating a project like this. FFC4 describes that it would most likely buy into an existing blockchain provided by an external company.

When asked to describe their perceptions of the importance of consensus power, the companies stated that they did not have a specific view and that this would be something that would be decided at the point of implementation.

	Single Authority	**Consortium of Authority**	**Fully Distributed Authority**
Consensus Power *The distribution of consensus power.*	n/a	n/a	n/a

Table 4.1: Consensus Power. Compiled by authors.

4.2.2.2 Immutability

When discussing the ability to be sure that information has not been tampered with, FFC1 says that the information they get today is not completely trustworthy, e.g. the company has experienced that the products do not come from the place as is stated on the documents. This is something the company wants to improve in the future. FFC2 mentions that they often have to correct incorrect data in their information system. It points out the inadequate IT infrastructure among some of its suppliers as an obstacle to accessing correct data. FFC3 has not experienced any problems with not being able to trust the data provided, but regard immutability as important. FFC4 says that the company has not had any problems with data being tampered, but argue that this might be a problem in the industry in general. FFC4 further argues that immutability can be important in business-to-business settings as a way of determining the source of truth. FFC5 says that it is becoming increasingly important in the future. FFC6 does currently not feel any significant concern that data has been tampered with, but see a bigger challenge of security further back in the supply chain.

A majority of the companies (FFC2, FFC3, FFC4, FFC5, FFC6) brought up that even though the data has not been tampered with, it might not be correct from the beginning. More specifically, the human interaction means that the provided data can be inaccurate. When discussing the human interaction, FFC3 says that it is important that the company has the ability to track a product back down the chain and double check that the information is correct. FFC2 says that the human factor can cause a lot of problems in the supply chain in the fashion industry. Similarly, FFC4 argues that due to the fact that the information is manually entered, potential errors are introduced and you can therefore not always trust the data. According to FFC5, this problem could be avoided by transferring technology electronically.

When the companies were asked to rank the importance of immutability in their SCM, they gave the following answers:

	Low	Medium	High
Immutability *Being sure that information has not been tampered with.*		FFC4	FFC1, FFC2, FFC3, FFC5, FFC6

Table 4.2: Immutability. Compiled by authors.

4.2.2.3 Protection Against Cyber Attacks

Having high security is considered to be important by all interviewed fast fashion companies. FFC1 says that being protected against cyber attacks is crucial for them and that the company has experienced problems of cyber attacks in the supply chain, which caused a lot of problems. FFC2 has also experienced some problems related to suppliers being exposed to cyber attacks and says that it is important for them to feel secure. Despite this, the company does not feel that their supply chain is especially threatened since a lot of the activities are being handled manually. FFC3 argues that it is important to be protected against cyber attacks and thinks that this is something everyone needs to be concerned about.

> *"I don't think anyone out there, any retailer, can sit there and say that they are totally secure."*
> *- Group IT Director, FFC3*

FFC4 says that everyone are in need of protection and that it is important, but that bigger companies are more exposed than smaller companies. In accordance, FFC6 describes that being protected against cyber attacks is a big issue for the company as it regards the company as a public actor that needs to take the issue seriously. According to FFC5, you have to be careful in the state of the existing business environment and that it is becoming increasingly important. The company puts a lot of resources in its IT department and maintaining a high security is a priority. It discusses the sensitivity of customers' private data and that it is important that this information remains secure.

When the companies were asked about the importance of protection against cyber attacks in their SCM, they ranked it as follows:

	Low	Medium	High
Protection against cyber attacks *Being protected against external cyber attacks and hacking.*	FFC2	FFC4, FFC5	FFC1, FFC3, FFC6

Table 4.3: Protection Against Cyber Attacks. Compiled by authors.

4.2.2.4 Scalability

When discussing the need of scalability in the operations, FFC1 says that the current information flow is not updated very often and that the company wishes to get more real time updates in the future. However, one update per day is said to be enough based on their needs. FFC2 and FFC4 say that they will always want information faster and would like to receive it as early as possible. At the same time, FFC4 describes that its business is not very fast moving and therefore means that if a shipment would be missed by one or two weeks, it is not a big deal. FFC2 says the need for fast information varies over time. When the company has campaigns or new product lines to introduce, the need for fast information becomes greater. FFC2 further explain the need fast and many transactions as follows:

"It is not a fast industry if you think about how the whole chain looks like. It does not require precision in terms of seconds."

- Logistics Coordinator, FFC2

FFC3 says that the company gets the information straight away, without any delays. Therefore, the company does not feel that they need the information faster. At the same time, they express that the ability to react once a problem has occurred is important. FFC4 says that although there might be spikes with many transactions, it will not be a high number of transactions per second. FFC5 describes that it sometimes receive real time data, but that it is not across all platforms. The company explains that the company wants more information to be shared automatically. FFC6 explains that predictability is one of the most important characteristics. The company has not experienced any problems of not receiving information fast enough and does therefore not feel like this is an area that needs to be improved. To conclude, all the companies interviewed argue that the fast fashion industry is not very complex and is thereby not dependent on a high amount of transactions in the SCM.

"I do not think that you have a great need of handling a large number of transactions in the textile industry. It is not that complex, it is just clothes."

- Supply Chain Manager, FFC1

When asked to rank the importance of scalability in their SCM, the companies answered as follows:

	Low	Medium	High
Scalability *The ability to perform a high amount of transactions.*	FFC1, FFC2, FFC4, FFC5, FFC6	FFC3	

Table 4.4: Scalability. Compiled by authors.

4.2.2.5 Cost

A majority of the fast fashion companies (FFC1, FFC3, FFC4, FFC5, FFC6) state that they would accept increased costs as long as the benefits it can provide is clear enough. At the same time, the companies did not have a clear perception of what transaction cost that would be acceptable if blockchain would be implemented and stated that it would be decided closer to potential implementation and in relations to the benefit. FFC3 says that it currently does not see what kind of problem that blockchain will solve in the SCM in the fast fashion industry. FFC2 and FFC6 have so far prioritised investments in the downstream activities, towards customers, and do therefore not think that it would be likely that a lot of investments will be put in the upstream activities. In contrast, as mentioned by FFC1, it prefers investments early in the supply chain, as this is where the information flow is the most lacking. Further, FFC3 says that retailers in the fast fashion industry, in general, might want to wait to invest in new technologies until another industry has successfully implemented it in their extended supply chain.

When asked to describe their perception of the level of cost in a potential implementation of blockchains, the companies said that this would simply depend on the benefits it would provide, and could not specify a certain level.

	Low	Medium	High
Cost *The level of transaction cost.*	n/a	n/a	n/a

Table 4.5: Cost. Compiled by authors.

4.2.2.6 Existing Trust

All the interviewed companies describe the trust with their suppliers to be quite high. Some of the companies say that the trust is based on long-term relationships and on having clearly defined working routines (FFC1, FFC2, FFC5). FFC5 says that trust is built by investing time and resources. However, no company describe the trust they have to their suppliers to be completely perfect. FFC6 says that even though the trust is high, you can never be sure exactly what the suppliers are doing every day. FFC4 describes the trust by using the following words:

"I feel like complete trust is something you have with your best friends"

- Senior Vice President, FFC4

FFC1 describes that it has a close relationship with its biggest supplier. FFC2 says that the relationships are good with the suppliers that they have worked with for a long time. Similarly, FFC3 says that they have worked with some of their suppliers for a long time, which has enabled them to build strong relationships. FFC4 describes that the company has good relationships with all suppliers and argues that having fewer suppliers enables building stronger and deeper relationships, and thus, increase the level of trust. FFC5 says that it has the most trust with its closest suppliers and states that the relationships should be like a partnership with the equal commitment from both sides. However, FFC5 describes that the influence it has over its suppliers becomes less the more you move up the supply chain and that it has the most influence over tier one and two suppliers. Finally, FFC6 describes that the trust to suppliers is high in general and also defines trust as being one of the most important characteristics in its SCM.

When asked to rank their existing level of trust between actors in their supply chain, the companies answered the following:

	Low	Medium	High
Existing Trust *The existing level of trust between actors.*		FFC2, FFC4, FFC6	FFC1, FFC3, FFC5

Table 5.6: Existing Trust. Compiled by authors.

4.2.2.7 Flexibility

FFC1 describes that the fashion industry in general has a lack of flexibility and that implementing changes usually is a slow process. In line with this, FFC3 expresses that there is a need of seeing more of flexibility in the fashion industry. The company also argues that the fashion industry is less trade focused and more focused on building relationships, which means that it does not require as much change as other industries might. FFC4 thinks that it should be easy to be able to change terms and settings with suppliers and to set up contracts easily. Further, FFC4 said that a system has to match the needs that the company has. In similarity with this, FFC5 describe flexibility as something important to have, both in terms of systems and processes. FFC5 describes that its operations vary much, meaning that the systems need to be able to handle this. FFC1 describes that it has shipping manuals that are followed by everyone, which means that the practices look quite the same for all suppliers. Still, since the fashion industry is dependent on trends, it is important for them to able to take quick decisions. FFC6 says that it is important that new suppliers can be connected to the information system in an easy way. FFC2 explains that it does not need flexibility in its current situation but might need to do some changes, as they grow bigger.

When being asked to rank the importance of having flexibility in their supply chain, the companies answered in the following way:

	Low	Medium	High
Flexibility *Being able to change rules and settings about the sharing of information and transactions.*	FFC2		FFC1, FFC3, FFC4, FFC5, FFC6

Table 4.7: Flexibility. Compiled by authors.

4.2.2.8 Privacy

Common between all fast fashion companies interviewed is that they regard privacy, the ability to conceal confidential information, to be a somewhat important need. FFC1 says that the company has not experienced any problems related to privacy so far, but that it might be a risk in the future. FFC4 makes a distinction between confidential data related to business and data about customers, but think that it is important to be able to conceal both. A lot of the companies (FFC1, FFC3, FFC4, FFC6) say that confidential information such as the name of the suppliers and prices is important to keep concealed for competitive reasons. Moreover, FFC2 says that they do not see prices as particularly sensitive as they think the price levels are somewhat similar for all companies, but that they would not want to share it with the customers. When discussing privacy specifically related to blockchains, the Enterprise Architect from FFC3 described this in the following way.

"You can't let any commercially sensitive information loose on the blockchain."
- Enterprise Architect, FFC3

Similarly, FFC4 expresses some concern with having a fully distributed database where every actor can see all the information. FFC5 speaks of the importance to conceal confidential information related to its customers. FFC6 says that it does not want the quantity of orders to be spread. It does neither want its purchase prices to be public, even though it does not think that the prices are very different from competitors. Several of the companies explain that if information about the clothes and the designs are spread, it is usually already too late in the process to be a risk. Related to this, FFC3 describes that once the clothes or designs have reached the factory, it is usually too late for being a competitive risk. It is however considered to be sensitive information and should not be spread to the wrong parties.

When being asked to rank the importance of having privacy in their SCM, the fast fashion companies answered the following:

	Low	Medium	High
Privacy *Being sure that confidential information is concealed.*		FFC1, FFC2	FFC3, FFC4, FFC5, FFC6

Table 4.8: Privacy. Compiled by authors.

4.2.2.9 Incentives

Regarding the incentives for actors to participate in a potential blockchain, no company states that it has any specific perception of what it would prefer. FFC1 argues that the relationships between a fashion company and its suppliers are buyer-seller relationships. If you are a significant buyer for a supplier, this means that you have the ability demand certain things. In comparison, FFC2 thinks that a monetary reward could be beneficial for engaging actors to participate and to make sure that they store correct data on the blockchain. FFC3 and FFC5 are unsure whether monetary rewards would be necessary. According to FFC4, it is crucial that the suppliers see a value of participating in a potential blockchain network. It should not just be beneficial for the lead firm, but also for the suppliers. FFC6 is not sure if suppliers should get a monetary reward or not, but argues that someone will need to bear the cost if the technology requires an increased effort from the people working in the supply chain.

"It is important that our suppliers see the benefit of adding data onto a blockchain. For example by being able to show us that exactly what they have done."

- Chief Information Officer, FFC6

However, FFC1, FFC3, and FFC4 express some concern that some suppliers might not have the adequate IT capacity to add data onto a blockchain. As expressed by FFC4, there are varying levels of sophistication of the IT infrastructure and this is dependent on where the suppliers are located. FFC3 sees that a lot of the smaller suppliers are paper-based and argue that it might be difficult to get these kinds of suppliers on board a project like a blockchain implementation. The company therefore sees this as a barrier of entry for blockchains.

Since none of the companies stated that it had any specific view of the incentives, they did not prefer any of the alternatives stake or monetary reward.

	Stake	Stake	Monetary Reward
Incentives *Being sure that confidential information is concealed.*	n/a	n/a	n/a

Table 4.9: Incentives. Compiled by authors.

4.2.2.10 Transparency

All fast fashion companies describe transparency as a crucial characteristic to have in the supply chain management. The majority of the companies also express a need of having more information and increased transparency. FFC1 says that you can never have too much information and FFC3 says that they will always want more. At the same time, some of the companies clarify that you should be careful not to be overloaded with information and that you need the right type information. FFC1 means that even though it is not necessary, information is always nice to have. Similarly, FFC2 and FFC6 say that although the companies only need a certain amount of transparency, it is important.

FFC1 says that the visibility is better with their largest supplier than with suppliers they buy from more rarely. FFC1 mentions that its visibility tends to be low before the goods are loaded onto the shipping boat. The company explains that it would like to get more information automatically. FFC2 describes that they have had problems related to lacking information, which has made the company realise that they need to set higher demands on their suppliers. FFC5 mentions that the company has the most visibility with the tier one suppliers and the visibility becomes less as you move up the supply chain. FFC6 explains that it is important to have a precise information flow. Further, FFC6 explains that it does not see further back in the chain than to the suppliers they order from.

FFC1, FFC2 and FFC6 all mention that they do not have integrated systems with their suppliers. In comparison, FFC3, FFC4 and FFC5 say that they are moderately integrated with its suppliers. FFC3 and FFC4 say that most information from the suppliers is received electronically. However, FFC4 says that since some of their suppliers are very small, they do not always have IT systems that are sophisticated enough to transfer data electronically. Similarly, FFC1 mentions that the quality of information differs depending on the IT capacity of the suppliers, where suppliers from more technically developed countries tend to provide better information than those with a less developed technical capacity. FFC3 also see a problem with smaller suppliers not having sufficient IT systems, making it difficult to integrate. According to FFC6, the company has not experienced any problems with its suppliers having inadequate IT systems but does agree that the IT level differs depending on the country where the supplier operates.

When the companies were asked about their perception of the importance of having transparency in their SCM, they answered as follows:

	Low	Medium	High
Transparency *Having access to information that is shared between the actors in the supply chain.*		FFC1, FFC2	FFC3, FFC4, FFC5, FFC6

Table 4.10: Transparency. Compiled by authors.

4.2.2.11 Traceability

As mentioned by several of the companies, managing their samples as they go back and forth between the company and its suppliers is an important part of the SCM. FFC1 describes that keeping track of the samples is a way for them to keep track of its production. This is also described by FFC3, FFC2 and FFC6 as an important part of managing the production. Unlike the rest of the interviewed fast fashion companies, FFC4 describes that they at some points have visibility all the way back to the cotton growers. In order to showcase this to the customers, as part of the company's marketing strategy, FFC4 says that it is important to have the ability to keep track of the origin of the cotton used in the garments. FFC2 says that it is important for them to track the products and getting information about the estimated time of arrival. FFC3 says that they do not see as far back in the supply chain as they would have wanted to and that it would like to have more accuracy and availability of data in order to improve stock optimisation. FFC6 describes that there are some parts of the supply chain where it has limited visibility of what is happening and that the company is in need of more predictability.

When discussing the emerging demand from consumers to get more information about the clothes, FFC1 says that it is becoming increasingly important to know that products are made in a sustainable manner and that the company's requirements increase all the time. FFC2 does not feel a lot of pressure from customers to be able to trace products since the agents stand for this responsibility. FFC3 mentions that in relation to CSR, it has a need to source where a garment comes from and how it has been produced. The company experiences an increasing demand from customers of being able to showcase more details from the supply chain. FFC3 further explains that the consumers want to know which country a garment comes from, but also want information about the specific material, e.g. if the cotton is organic or not. FFC4 overall defines traceability as highly important. FFC5 says that the company wants to increase traceability due to sustainability issues.

"We produce quite a lot of products that are made from sustainable materials. For us to develop those products and then market them to consumers, we need to be able to identify where they come from, that they come from sustainable sources. To do that we really need to be able to trace the clothes, products, all the way from the early life cycle all the way through until it's arriving on the shelf. "

- Business IT Solutions, FFC5

The company is interested to track a product all the way from early life cycle all the way to end of life recycling. Moreover, FFC5 express that the company has identified a need to be able to trace the source of their products on its own, without simply trusting the garment manufacturer. Also, FFC6 feels that it is important for customers to have information about where the clothes are from and what materials they are made from.

When the fast fashion companies were asked about the importance of having traceability in their SCM, they ranked it in the following way:

	Low	Medium	High
Traceability *Being able to trace products back in the supply chain.*	FFC2	FFC1, FFC6	FFC3, FFC4, FFC5

Table 4.11: Traceability. Compiled by authors.

4.2.3 Summary of the Fast Fashion Companies' Perception of the Characteristics

	Low	Medium	High
Consensus Power *The distribution of consensus power.*	n/a	n/a	n/a
Immutability *Being sure that information has not been tampered with.*		FFC4	FFC1, FFC2, FFC3, FFC5, FFC6
Protection against Cyber attacks *Being protected against external cyber attacks and hacking.*	FFC2	FFC4, FFC5	FFC1, FFC3, FFC6
Scalability *The ability to perform a high amount of transactions.*	FFC1, FFC2, FFC4, FFC5, FFC6	FFC3	
Cost *The level of transaction cost.*	n/a	n/a	n/a
Existing Trust *The existing level of trust between actors*		FFC2, FFC4, FFC6	FFC1, FFC3, FFC5,
Flexibility *Being able to change rules and settings about the sharing of information and transactions*	FFC2		FFC1, FFC3, FFC4, FFC5, FFC6
Privacy *Being sure that confidential information is concealed.*		FFC1, FFC2	FFC3, FFC4, FFC5, FFC6
Incentives *Being sure that confidential information is concealed*	n/a	n/a	n/a
Transparency *Having access to information that is shared between the actors in the supply chain.*		FFC1, FFC2	FFC3, FFC4, FFC5, FFC6
Traceability *Being able to trace products back in the supply chain.*	FFC2	FFFC1, FFC6	FFC3, FFC4, FFC5

Table 4.12: Summary of the Fast Fashion Companies' Perception of the Characteristics. Compiled by authors based on empirical findings.

5. Analysis

In the following chapter, the empirical findings will be analysed by comparing the empirical findings from blockchain experts and fast fashion companies to each other and to the literature. The chapter begins by presenting the analysis process, which is partly done by constructing an analysis model. Each characteristic distinguishing the configurations of blockchains will then be discussed, which will be followed by an assessment of the coherency of the characteristics for each fast fashion company. This discussion will form the basis for determining the compatibility of the different configurations. Finally, the chapter will end by presenting additional factors affecting the compatibility.

5.1 The Analysis Model

The following analysis aims to determine how compatible the different configurations are with SCM in the fast fashion industry. However, due to some identified discrepancies between the literature and the empirical findings from the experts about the definition of blockchain overall and of the configurations in particular, this will first be discussed.

5.1.1 Definition of the Configurations of Blockchains

In order to extend and build upon the literature review about blockchains and the different configurations, eight experts about blockchains were interviewed. The definitions and the blockchain characteristics were generally described in the same way by the experts as in the literature, using the same characteristics, but were called different names. It is when the blockchain gets restricted, i.e. permissioned, that the main differences between empirical findings and the literature can be found. For example, A1 states that permissioned blockchains are “fake blockchains”. In accordance with this, A2 describes that some do not define permissioned as blockchains at all. This view is not identifiable in the literature.

Another discrepancy is that even though the literature mentions that there are many different versions of consortium blockchains, it describes that the consortium blockchain provides the middle of the benefits and needs of the private and public blockchain. The experts (BC1, A2), however, rather emphasise the adaptability of the consortium blockchain. Thus, they argue that the ability to choose the number of actors and what they can do means that the achievable level of the characteristics in a consortium does not necessarily have to be in the exact middle between a private and a public blockchain at all times. Both BC2 and Bauman et al. (2016) describes the permissioned, as especially good in business environments. This is in line with what A2 explains that it might be good to use a private blockchain for internal learning process in businesses. On the other hand Al, A2 and BC1 are questioning the benefit of using a fully private blockchain in large scale compared to simply using other alternatives of traditional databases since it gives little of the advantages but a lot of disadvantages, which Bauman et al. (2016) also mentions, but a lot of the negative aspects of blockchains.

To sum up, these discrepancies can thereby both be found in the literature, amongst the expert respondents as well as between the literature and the expert. Thus, it can be concluded that there is a lack of coherency amongst researcher and the business world of exactly what to call a blockchain and the different configurations, which mirrors how new, uncertain and fast-moving the technology is today. However, the characteristics and main differences of the three different configurations seems to be described in similar ways but under different names, indicating that the division chosen in this study is still relevant to examine.

5.1.2 Constructing the Analysis Model

In order to assess how compatible the configurations of blockchains are with the SCM in the fast fashion industry, it has to, according to the definition of compatibility (Rogers, 1983; Agarwal & Karahanna 1998), be assessed how consistent these configurations are within the SCM in fast fashion companies. Based on the way the characteristics are described by the experts and by the fast fashion companies, it has been identified that the characteristics are connected to a company in different ways, creating distinguishable clusters of characteristics. This can also, to a certain extent, be confirmed by the way the characteristics were discussed in the literature, although it does not explicitly mention the clusters.

Cluster	Explanation of Division of Characteristics
CURRENT STATE OF RELATIONS - Existing trust	Trust is, as described in the literature, a core concept in blockchain technology as the technology was first created due to low trust in existing networks (Warburg, 2016; Etwaru, 2017). The experts agree and also mention that the existing level of trust is an important factor when first looking into blockchain. For example, A2 argues that trust is important to examine first when assessing what blockchain that is necessary. Based on what is mentioned above, and that trust is something the companies also describe as very important, the existing level of trust in the network will be examined as the first part of the analysis model.
BENEFITS OF BLOCKCHAINS - Protection against cyber attacks - Immutability - Transparency - Traceability	Protection against cyber attacks, immutability, transparency and traceability are all described as benefits achievable by using blockchain technology by both the experts and literature (Christidis & Devetsikiotis, 2016; Bauman et al., 2016; Ross, 2017). Similarly, all of the fast fashion companies discuss these characteristics as something that can improve their current operations. Thereby, these characteristics will be analysed as blockchain benefits.
OPERATION NEEDS - Scalability - Flexibility - Privacy	Scalability, flexibility and privacy are characteristics that experts describe as something that must be dealt with when using blockchain technology. The three characteristics, scalability, flexibility and privacy, will thereby be clustered as the operations needs as they are described as something that are depending on what a company requires in its operations rather than benefits that can be achieved. This is strengthened by the way the companies talk about these characteristics, e.g. FFC4 explain that the system must match the need the company has of flexibility and FFC2 explains that the need of fast information is high in some periods.
BLOCKCHAIN IMPLEMENTATION DESIGN - Cost - Consensus Power - Incentives	The experts mention cost, consensus power and incentives as being more of design choices that are made when blockchain technology is being implemented. For example, BC1 explains that it is difficult to determine the exact cost due that there are only pilot studies, which is not mentioned in the literature. Further BC1 mention that the consensus power and number of actors are choices that need to be made in the implementing process. A2 argues for how the actors are going to be incentivised is a design choice that needs to be made. Further, the companies found these characteristics as something they would think about and discuss first when they would choose to implement blockchains and did not have any specific opinion about which to choose. This cluster will thereby be described as an implementation design of the different configuration and will in the analysis be used more as an outcome of the other characteristics.

Table 5.1: Explanation of Division of Characteristics. Compiled by authors.

Based on the above discussion, the characteristics distinguishing the configurations of blockchains can be divided into four clusters, current state of relations, benefits of blockchains, operation needs and blockchain implementation design.

	Private Blockchain	Consortium Blockchain	Public Blockchain
CURRENT STATE OF RELATIONS			
Existing Trust *The current level of trust between the actors.*	High	Medium	Low
BENEFITS OF BLOCKCHAINS			
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*	Low	Medium	High
Immutability *The degree of wanting to be sure that information has not been tampered with.*	Low	Medium	High
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*	Low	Medium	High
Traceability *The degree of wanting to be able to trace products back in the supply chain.*	Low	Medium	High
OPERATION NEEDS			
Need of Scalability *The degree of needing to perform a high amount of transactions.*	High	Medium	Low
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	High	Medium	Low
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*	High	Medium	Low
BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$$ Medium	$$$ High
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	∞ Fully Distributed Authority
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward

Figure 5.1: Analysis model. Compiled by authors base on literature review and empirical findings.

The characteristics in the first column of the model illustrate the characteristics previously discussed in the study. The way the characteristics distinguish the configurations from each other can be seen in the three alternatives presented horizontally after each characteristic. The model can be used to identify an appropriate configuration of blockchain for a company by assessing each characteristic based on how a company perceives them in terms of their current state, wanted benefits and operation needs. According to several experts, assessing what configuration of blockchain that is suitable is much dependent on what a company wants and needs. This is also in line with the definition of compatibility, stating that an innovation needs to be perceived to be consistent with the values, past experiences and needs of potential adopters (Rogers, 1983).

The experts also discussed that there are some trade-offs that can be connected to the clusters. More specifically, the characteristics in operation needs are discussed by the experts as being trade-offs to the benefits of blockchains. Where the public blockchain gives a high degree of the benefits but a low degree of scalability, flexibility and privacy, the private blockchain has the opposite relation. This relationship is also to some degree mentioned in the literature, especially between security and scalability (Berke, 2017; Croman et al. 2016). Thus, due to the trade-offs present between the current state, wanted benefits and operation needs, this also needs to be considered when assessing the compatibility. By mapping out the ways these clusters are perceived in the SCM in the fast fashion industry, it can be assessed how coherent these configurations are. As none of the companies expresses that they have any specific perception of what level of cost, type of consensus process or type of incentives they would prefer if implementing blockchains, there is no trade-off evident for this cluster. These characteristics will thereby not be included when assessing the coherency between the clusters, but rather interpreted as if the design characteristics would simply be a result of the blockchain that potentially would be chosen. Thus, if a company's perception of these characteristics is not fully matched with any of the configurations, this indicates that none of the configurations can be considered to be fully compatible.

5.1.3 Summary of the Analysis Process

In order to determine how compatible the configurations are, it firstly needs to be assessed how consistent the characteristics are with the SCM in the interviewed companies. Since the findings from the blockchain experts at some points differ from the literature also concerning the specific characteristics, these differences will be discussed in relation to the findings from the fast fashion companies. Due to the identified trade-offs between the configurations of blockchains, it also needs to be assessed if there is a match, a coherency, between the current state, wanted benefits and operation needs of the interviewed companies. The findings from the fast fashion companies will be compared to the clusters of characteristics to assess whether these match with any of the configurations.

When the fast fashion companies' perception of the characteristics have been compared to the literature and to the experts, and when the coherency between the clusters of characteristics based on the companies' assessment has been assessed, this will be used as the basis for determining the compatibility of each of the different configurations of blockchains. The final part of this section will consist of a discussion of the overall compatibility.

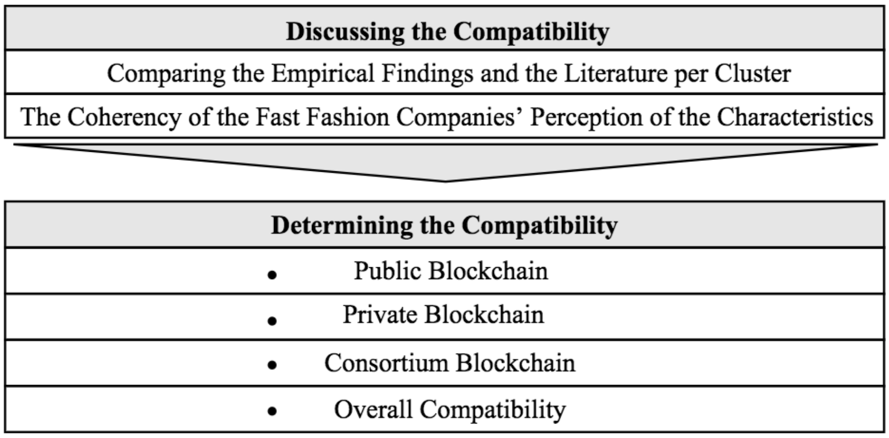

Figure 5.2: Summary of the Analysis Process. Compiled by authors.

5.2 Discussing Compatibility

The following section will add to the discussion of compatibility of the different configurations by examining the findings for each of the clusters individually. This discussion will then be used to examine the coherency of how the companies perceive the characteristics and how they are distributed in regards to the blockchain configurations. The result of the fast fashion companies' stated perception of each characteristic, as illustrated in the empirical findings, have been compiled into the analysis model and can be found in Appendix D.

During the following analysis, it was identified that the clusters of characteristics from the framework have different relationships to compatibility. From the discussion about the current state of relations, it can be read that the more trust there is between the actors, the more configurations are suitable, while less trust means that fewer configurations are possible. Moreover, based on what the companies discussed in the interviews, it was evident that even though some companies ranked the benefits of blockchains as medium or low, it was repeatedly mentioned that this is only a minimum requirement and that they would the always like more of it. Similarly with the operation needs, the companies described that their ranking was in fact what they need, but that they would not be negatively affected by achieving more of it. If assuming that this reasoning is valid for all companies, more configurations than the one corresponding with what a company ranked can be compatible.

When discussing the results, this will be illustrated by marking the alternative that the company specifically chose with dark green, and the alternatives that can are compatible based on the previous discussion will be marked with light green. The alternatives that are not compatible at all will be marked with red. Moreover, a number of experts point out some issues related to the characteristics that indicate that more alternatives can be compatible than what initially could be read from the literature. When the experts have expressed views that differ from the literature, adjustments will be made in the table showing the result by marking the additional compatible alternative with yellow. A summary of the colours is presented in Table 5.2. This is also described and illustrated in further detail in Appendix E.

(dark green)	Compatible, based on the alternative chosen by the fast fashion company.
(light green)	Compatible, based on the discussion from the fast fashion companies.
(yellow)	Compatible, based on the findings from the blockchain experts.
(red)	Not compatible.

Table 5.2: Explanation of Colours Used When Discussing Compatibility. Complied by authors.

5.2.1 Comparing the Empirical Findings and the Literature per Cluster

This section of the analysis will be performed by discussing each characteristic describing the configurations one by one. The fast fashion companies' perception of each characteristic will be discussed by comparing it to the empirical findings from the experts and to the literature. See Appendix D for an overview of the fast fashion companies' stated perception of each characteristic inserted in the analysis model.

5.2.1.1 Current State of Relations

Level of Trust

Half of the fast fashion companies ranks its level of trust as medium and the other half rank it as high, which according to the literature are suitable with a private or consortium blockchain. The literature mentions that trust-free transactions require an open system where the transactions can be controlled and verified by everyone, such as is the case in a public blockchain (Xu, 2016). Thus, if the trust among the actors in the companies' supply chains is very low, a public blockchain could be suitable. This is agreed by the experts, where A2 describes that when trust is completely absent or very low, a public blockchain is the only option. Important to mention is that neither the literature nor the experts claim that a public blockchain is suitable only when trust is low, meaning that nothing stands in the way of using a public blockchain if a company has high trust.

Moreover, the literature mentions that if the relationship between the actors is more characterised by a network where the identities of the actors are known, trusted and registered (O'Leary, 2017; Oh & Shong, 2017), a consortium blockchain might be the better choice. As described in the literature and by BC1, a consortium blockchain requires trust in the majority of the nodes, indicating that the required trust is lower than with a private blockchain, where only one actor is validating the transactions (Zheng et al., 2016). It is thereby a viable option only in the cases when the trust between actors is high. Thus, when trust is non-existent or low, a public blockchain is the only option. When trust is medium, either a consortium or public blockchain can work. If trust is high, all options are possible, although it is the only case where a private blockchain can be used.

The three interviewed companies that ranked their trust as high could thereby use a private blockchain, a consortium or a public blockchain, depending on their wants and needs of other characteristics of blockchain. For the three companies that ranked their level of trust as being medium, a consortium or public blockchain could be possible. However, although the companies ranked the trust in their supply chains as medium or high, it appeared in the interviews that none of the companies has complete trust in their suppliers. Based on this, it could be argued that a consortium blockchain could be more suitable for the industry in general. Further arguments for a consortium is that many of the companies describe that they have some main suppliers where the trust is high. Thereby, their current state of relations could be considered to be similar to the one present in a consortium blockchain. Thereby, it could be argued that a consortium blockchain is compatible based on the companies' current ways of working.

Summary
Half of the companies ranked their level of trust as high, meaning that their current state of relations, based on the assumption that more trust equals more options, corresponds to all three configurations of blockchains (Alternative 1). The other half ranked their level of trust as medium, which according to the same argumentation corresponds to a consortium or public blockchain (Alternative 2). In general, the experts agree with the literature about the level of trust that corresponds to the different configurations of blockchains. Thus, no adjustment will be made based on the findings from the experts.

	Private Blockchain	Consortium Blockchain	Public Blockchain
Level of Existing Trust	High	Medium	Low
Alternative 1	FFC1, FFC3, FFC5,		
Alternative 2		FFC2, FFC4, FFC6	

Table 5.3: Compatibility of Level of Existing Trust. Compiled by authors.

5.2.1.2 Benefits of Blockchains

Protection Against Cyber Attacks

All companies discuss protection against cyber attacks as an important issue in general. It is also described as a priority held by the majority of the companies. Despite this, FFC2 ranks its will to achieve this in its supply chain as low as it does not consider itself as very threatened by it. This would indicate that a private blockchain would be sufficient. The company argues that its risk of being exposed to a cyber attack is mitigated based on the fact that it performs a lot of tasks manually. However, the company at the same time mentions that it sees a need to take the next step and to improve its IT capacity. Based on the argumentation made by FFC4 of that bigger companies are more exposed than smaller, it could be argued that a company on the path to becoming a bigger player on the market also need a stronger protection against cyber attacks.

Even though FFC2 express that they do not feel particularly threatened, all companies agree that more security is always beneficial and desirable. Thus, a company is not negatively affected by achieving a higher level of security per se. However, they would be negatively affected by a lower level of security than what is wished for. This indicates that all configurations would be suitable if the want of protection is low, but not if the companies express that they want high security. Two of the companies rank their wanting to be protected against cyber attacks as medium, and the remaining three rank their will to achieve this as high. Based on what was identified in the literature (Kshetri, 2017; Zheng et al., 2016;

Bauman et al. 2016; Priya; 2018; IBM, 2017a), this would indicate that a consortium blockchain versus a public blockchain would be suitable for these companies.

The experts agrees with the literature (Xu, 2016; Lin, et al., 2018) that when a high level of protection is needed, an increasing numbers of actors, and thereby increasing distribution of copies of the ledger, will increase the security since there are more copies that need to be hacked (A1, A2, BC1, BSC3). A1 and BC1 both mention that when a network is growing larger, it becomes increasingly expensive to break the system, which is something the literature agree upon (Berke, 2017).

Summary
One company ranked its will to achieve protection against cyber attacks as low, which would be achievable with the use of a private blockchain. However, based on the assumption that the companies would accept a higher degree of the benefits, a consortium or public would be possible as well (Alternative 1). Two companies ranked this as medium, which according to the same argumentation corresponds to a consortium or public blockchain (Alternative 2). Finally, three companies ranked it as high, corresponding to a public blockchain (Alternative 3). In regards of protection against cyber attacks, both the literature and experts agree that many nodes equal higher security. Thus, no adjustment will be made based on the findings from the experts.

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
Protection against cyber attacks	Low	Medium	High
Alternative 1	FFC2		
Alternative 2		FFC4, FFC5	
Alternative 3			FFC1, FFC3, FFC6

Table 5.4: Compatibility of Protection against cyber attacks. Compiled by authors.

Immutability

Regarding security in terms of immutability, the perceptions of the companies are more consistent. Only one company ranked their wanting of immutability as medium, while the rest rank it as high. The company that ranked immutability as medium, FFC4, explains that it is not a problem for them, but argues for the importance in a business setting in general. Based on what was found in the literature (Ross, 2017; Bauman et al. 2016; Bano et al, 2017), a public blockchain would be suitable for the majority of the fast fashion companies. According to the literature, immutability is, in similarity with protection against cyber attacks, increased the more actors that participate in the network. Thus, the higher number of actors participating in a public blockchain makes it more suitable if high immutability is wished for. This is confirmed by the majority of the experts arguing that security increases by the number of nodes (A1, A2, BC1, BSC3). Similar arguments could be made about immutability, as with protection against cyber attacks, that all companies agree that more security is always beneficial and desirable. Thus, also in immutability, a company is not considered to be negatively affected by achieving a higher level of security per se. However, they would be negatively affected by a lower level of security, meaning that a public blockchain could be considered acceptable also for FFC4.

Whilst the literature (Xu, 2016; Lin, et al., 2018) argue that security increases by the number of nodes, speaking for a public blockchain, BC2 questions the fact that it would be more secure to rely on a public network where the identity of the actors is hidden than on a permissioned, and thereby trusted, network. BSC2 also argues that the number of nodes is less important in a trusted network. Both BC2 and BCS2 argue that a consortium blockchain would be more suitable to use in a business setting. BC2 explains that 10-20 nodes should be enough to ensure high security in form of immutability since companies only need to be sure that half of the trusted network behaves in good faith to be ensured of immutability. Since BSC3 mentions that ill-behaved actors can get kicked out in consortium blockchain this speaks for an increased likelihood that the actor will behave and thereby be trusted not to tamper with the data. The fact that A1 describes an upper limit of the number of nodes giving increasing value in terms of security, something that cannot be found in the literature, is further strengthening the reasoning. This argument thereby indicates that even though the majority of the companies have a wish for high immutability, the consortium might still be able to be compatible.

Summary
One company ranked its will to achieve immutability as medium, corresponding to a consortium or a public blockchain (Alternative 1). The remaining five companies ranked it as high, corresponding to a public blockchain according to the literature and most of the experts (Alternative 2). However, some of the experts also point out that a public blockchain might not be suitable in a business setting and that not as many actors might be needed to achieve a high level of immutability in a trusted environment. This could indicate that a consortium could be a suitable choice also for companies striving for high immutability when there is trust, which cannot be identified in the literature. Thereby, the consortium has been adjusted and marked yellow when the wish of immutability is high (Alternative 2).

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
Immutability	Low	Medium	High
Alternative 1		FFC4	
Alternative 2			FFC1, FFC2, FFC3, FFC5, FFC6

Table 5.5: Compatibility of Immutability. Compiled by Authors.

Transparency

The companies mention transparency as something that is increasingly desirable. Some have visibility further up in the supply chain but most companies do not have visibility beyond tier one or two, which is similar to what Deloitte (2017) described in the automotive industry. The companies point out that even though they only express a certain need for transparency, they, for example FFC1 and FFC3, would always welcome more information. However, some companies (FFC1, FFC2, FFC6) also state that you should be careful not to get overloaded with information and that it is important to get the right type of information. This can be connected to the statements made by BC1 and BC3 about the fact that a public blockchain should not be overused, as it is both slow and expensive. To conclude, a blockchain providing the minimum transparency required by a company could be compatible as long as it only provides the necessary information. In this case, one half of the companies rank transparency as high, and the other half rank it as medium, which according to the literature would be achievable by the use of a public versus a consortium blockchain.

The experts (A1, BC3, BSC2, BSC3) agree with the literature (Abeyratne & Monfared, 2016; Apte & Petrovsky, 2016; Loop, 2017) regarding that blockchain could increase transparency in supply chains. In addition, the literature (Abeyratne & Monfared, 2016; Apte & Petrovsky 2016) and experts agree that a public blockchain gives the highest transparency. Loop (2017) and A1 mentions that this is due to the distributed copies of information and immutable characteristics of a public blockchain in comparison to information being stored in a centralised storage. Thus, the coherency between the literature and the experts, in combination with that the companies have the desire of achieving medium to high transparency, speak for that consortium or public would be most suitable for the companies overall.

Summary
Two of the companies rank their will to achieve transparency as medium, which corresponds to a consortium or public blockchain (Alternative 1). The remaining four companies ranked it as high, corresponding solely to a public blockchain as both the literature and experts agree upon that the fully public gives the highest transparency (Alternative 2). However, it is crucial that only relevant information is shared. Since the experts and the literature are in agreement, no adjustment has been made.

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
Transparency	Low	Medium	High
Alternative 1		FFC1, FFC2	
Alternative 2			FFC3, FFC4, FFC5, FFC6

Table 5.6: Compatibility of Transparency. Compiled by authors.

Traceability

In similarity with transparency, the companies describe traceability as becoming increasingly important. Almost all companies rank traceability as either high or medium, which according to the literature would be achievable by the use of a public versus consortium blockchain. FFC2 stand out from the rest of the companies by ranking traceability as low, speaking for a private blockchain. Like transparency, the experts are in agreement with the literature (Apte & Petrovsky, 2016) that traceability is highest in a public blockchain and lowest in a private blockchain since the data is more secure.

The literature mentions that the traceability enabled by blockchains can increase the information flow, which will bridge the gap between the firm and its customers. This will enable consumers to exclude companies that do not follow the norms and values of the society (Loop, 2017; Abeyratne & Monfared, 2016). The experts (A1, BSC2, BSC3) agree that the traceability enables companies to market themselves as ethical and sustainable with the immutable record as proof. This is of importance for the companies since the majority of the interviewed companies experience an increased pressure from consumers to share information about the origin of products due to sustainability issues. Most companies believe that this will come to increase even more in the future, which would mean that the importance of having traceability and transparency in the supply chain might come to increase as well. This indicates that even though a blockchain would not be fully compatible in all other aspects today, the pressure might force companies to adopt the technology regardless. This is also strengthened by the fact that the majority of the companies say that you can never get too much information. The argumentation made for why companies would welcome more transparency, but not accept less, is assumed to also be valid for traceability.

Summary
One company ranked its will to achieve traceability as low, which would be achieved by a private blockchain (Alternative 1). This company could also go with a consortium blockchain or public blockchain, assuming that it would accept more. Two companies rank it as medium, corresponding to a consortium or public blockchain (Alternative 2). The remaining three rank it as high, which can only be fulfilled with a public blockchain (Alternative 3). The majority of the fast fashion companies agree that the pressure from consumers to share information about a garment's origin, material and working conditions is something that will continue to increase. This would indicate that a technology such as blockchains could become increasingly important. Since there are no discrepancies between the experts and the literature in this regard, the compatibility of traceability stays the same and no adjustment in the table needs to be made.

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
Traceability	Low	Medium	High
Alternative 1	FFC2		
Alternative 2		FFC1, FFC6	
Alternative 3			FFC3, FFC4, FFC5

Table 5.7: Compatibility of Traceability. Compiled by Authors.

5.2.1.3 Operations Needs

Scalability

All fast fashion companies agree that the need of scalability, in terms of transactions, generally is low in the fashion industry, even though FFC3 ranked its individual need as medium. This is also confirmed by A1. The literature describes scalability as being highly limited in a public blockchain (Lemieux, 2016; Buterin, 2016: Brennan & Lunn, 2016), which is confirmed by many of the experts (A1, A2, BC1, BC2, BSC3). Based on the literature and the experts, it is apparent that there is a trade-off between security and scalability since the low scalability is a mechanism that rather ensures the high security in line with what Berke (2017), Lipton (2018) and Oh and Shong (2017) describes. This indicates that a company that wants high security must deal with low scalability. However, since the companies do not see a great need of scalability, there would be no obstacle, in terms of the trade-off, for these companies to achieve high security. Consequently, for all the companies that ranked scalability as low, all configurations could be argued to be possible options according to both literature and experts. This because, despite the fact that the companies state that the industry is slow-moving, they would likely not be negatively affected by having higher scalability per se. The majority of the companies describe that even though they do not need a high scalability due to the slow-moving business, they would like to get information as soon as possible. Furthermore, as stated by BSC3, a public blockchain might be too slow to truly support the needs of a global supply chain. For FFC3, that ranked its need of scalability as medium, only the permissioned blockchains, the consortium and private, would be possible options since the scalability that is needed could not be achieved by a public blockchain.

Summary
One company ranks it need of scalability as medium, which is supported by the use of a consortium or private blockchain according to the literature and experts (Alternative 1). The remaining companies rank it as low, which is supported by all three configurations of blockchains (Alternative 2). The companies and experts agree that the need of scalability is low in the fashion industry, which overall speaks for that the trade-off would not affect the configurations suitability much. Since there are no discrepancies between the experts and the literature in this regard, the compatibility of scalability stays the same and no adjustment in the table needs to be made.

	Private Blockchain	Consortium Blockchain	Public Blockchain
Need of Scalability	High	Medium	Low
Alternative 1		FFC3	
Alternative 2			FFC1, FFC2, FFC4, FFC5, FFC6

Table 5.8: Compatibility of Need of Scalability. Compiled by authors.

Flexibility

All companies except FFC2 state that they need a high level of flexibility. Several companies describe that the industry in general lacks flexibility and that they would like to see this being improved. Although one company rank its need of flexibility as low, all companies describe flexibility as something that is important to have. Hence, it could be argued that the companies would accept more flexibility than the degree they rank that they need. When discussing the importance of flexibility, the companies in particular discussed the ability to change rules and settings in both systems and processes. FFC5 and FFC6 mentioned that it should be easy to include and exclude actors, and FFC4 said that changing the terms and settings should be possible to perform easily.

According to the literature (Oh & Shong, 2017), a great need for flexibility would be most suitably fulfilled by a private blockchain and the least by a public blockchain. In fact, the lack of flexibility, explained by BSC3, that is caused by the fact that a public blockchain does not allow any actors to be excluded or any documents to be removed, can cause problems in a business setting. If actors engage in unethical activities or store illegal documents onto the blockchain that is used in a business setting, this might cause problems for the companies. The possibilities to exclude misbehaving actors in a public blockchain are, both by the literature and experts explained, as non-existent. In a consortium, the actors can instead collaboratively decide who can participate or not which BSC3 argues for would fit better in a global supply chain in a business setting. The literature (Zheng et al., 2016) and the experts (A2, BSC3) agree that since a private blockchain is only governed by one single actor, that actor can decide everything, which makes the flexibility very high.

Even though almost all actors ranked their need of flexibility as high, it is evident from the interviews that the current need of flexibility in the fashion industry is low (FFC1, FFC3).

Hence, a public or consortium blockchain would not necessarily worsen the current state, but could even be an improvement, depending on the situation. Moreover, BSC3 explains that a consortium blockchain may be suitable in a business environment since the actors are known and trusted. In similar with immutability, BC2's arguments about the closed and trusted network with setup rules, it can be argued that the consortium might be able to achieve similar flexibility as a private blockchain. Based on the experts' opinions of blockchains in a business setting explained above, it could thereby be argued that a consortium would be compatible with the operations need of flexibility.

Summary
All but one company rank their need of flexibility as high, which only corresponds to a private blockchain according to the literature (Alternative 1). The other company ranked its need of flexibility as low, which would be supported in all three configurations, assuming that the company would accept the possibility of more flexibility (Alternative 2). Due to the pressure to follow the regulation present in a business setting, it can be crucial to have the ability to exclude actors that do not follow the laws, rules or routines, speaking against the use of a public blockchain in a business setting. The companies state that the current level of flexibility is low, i.e. not corresponding to the high degree of flexibility that the majority of the companies prefer. This could indicate that a consortium blockchain would not necessarily be worse than the current state. If programmed with specific rules between the actors, as is a possibility mentioned by the experts, it gives flexibility closer to a private blockchain, indicating an increased compatibility. Thereby, the consortium blockchain has been adjusted marked yellow when the need of flexibility is needed to be high (Alternative 1).

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
Need of Flexibility	High	Medium	Low
Alternative 1	FFC1, FFC3, FFC4, FFC5, FFC6		
Alternative 2			FFC2

Table 5.9: Compatibility of Need of Flexibility. Compiled by authors.

Privacy

Regarding privacy, the majority of the companies rank their need of privacy as high, and the remaining companies as medium, which based on the literature would indicate that a permissioned, such as a private versus a consortium blockchain, would be compatible. Several companies bring up names of suppliers, purchase prices, order quantities and designs as sensitive information. As FFC2 and FFC6 argue that the purchase prices are similar in the industry, the importance of concealing this information could be argued to be somewhat reduced. However, even though some of the companies ranked privacy as medium, no company sees that it could be negatively affected by achieving more privacy. One particularly important aspect for many of the companies is to be able to conceal private information about their customers, which FFC3 and FFC5 explicitly say increases the pressure of privacy. As BSC3 mentions the importance of the new data protection legislation GDPR as an example of sensitive data that would be difficult to assure to be protected in a public blockchain, the suitability could be further questioned in line with the literature.

However, it is pointed out by several experts that there is often a way of concealing sensitive information by encrypting it and the use of private and public keys. Although the literature also mentions this solution, the main concern is that the encrypted information is still broadcasted amongst the whole network (Oh & Shong, 2017; Ross, 2017; Xu, 2016). This is something the literature (Maxwell & Salmon, 2017) mentions could bring problems in terms of actors getting singled out in a public blockchain. It could thereby be questioned if information such as price and quantity might be able to be pointed out as well. In supply chain networks, it could thereby be argued that confidential information regarding for example from what suppliers the company buys from could be in danger of being figured out on a more public blockchain. In regard to this, BC2 and BSC3 also mention that companies in the industry probably would feel safer to only share data, even if encrypted, to actors that need it. This is also in line with Casey and Wong's (2017) argument that companies seeking to protect market share and profit probably would like to share information, even encrypted, solely with collaborating parties involved. This implies that even though both the literature (Oh & Shong, 2017; Ross, 2017) and the experts (A1, A2, BC1), mention that when the data has the possibility to be hidden and encrypted, the companies might still not dare to spread confidential or sensitive information on a broad network, speaking for that a private or consortium blockchain is most compatible if companies do not wish to reveal this kind of information.

BC2 mentions ways, due to the adaptability, in a consortium blockchain that he calls channels where confidential information between different actors in the supply chain can be hidden. This indicates that it would be as confidential as in a private blockchain. As this is one of the main information concerns that the companies bring up, a consortium blockchain could be argued to be able to be acceptable even for the companies that have ranked privacy as high, which according to the literature otherwise would indicate that a private blockchain as compatible. Thus, even though companies might want their confidential data secure, which BC1 explains needs to be broadcasted in order to be validated, the fact that BC1 also mentions the alternative to use a form of digital fingerprint (hash) to conceal the data also indicates that other blockchains than a private blockchain might be possible when the need of privacy is high.

Summary
Four companies rank their need of privacy as high, corresponding to a private blockchain (Alternative 1). Two companies instead rank it as medium, corresponding to a consortium or a private blockchain if assuming that they would accept more privacy (Alternative 2). Experts in supply chains further mention that the companies probably would only dare to share data, even encrypted, in a closed network, which is close to how a consortium blockchain works. With this in mind and the discussion made by the experts that the consortium, due to its adaptability, it could be argued to be suitable when if the need of privacy is high, which is not mentioned in the literature. Thereby, the consortium has been adjusted and marked yellow when the need of privacy is high (Alternative 1).

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
Need of Privacy	High	Medium	Low
Alternative 1	FFC3, FFC4, FFC5, FFC6		
Alternative 2		FFC1, FFC2	

Table 5.10: Compatibility of Need of Privacy. Compiled by authors.

5.2.1.4 Blockchain Design Decisions

Cost

In general, companies do not have any specific view on what level of cost that they would accept if implementing blockchain. They state that it depends on what level benefit that it would provide. According to A1, BC1 and BSC3, a public blockchain is more expensive to run since it requires more computing power and often a monetary reward for the validators. This is confirmed by the literature (Brennan and Lunn, 2016; Bauman et al., 2017; IBM, 2017b). As mentioned by A1, blockchains are the only technology that has increased the transaction costs. Due to that the companies do not have a clear view or specific opinion of how they would react to cost, it indicates that it would not affect compatibility.

Consensus Power

When it comes to the consensus process, it is evident from the interviews that the companies do not know what they would prefer. The experts are in accordance with the literature regarding that for a private blockchain, the central authority decides on its own. They also agree that for a consortium blockchain, there is a consensus among the majority of trusted and identified actors. They also agree that a public blockchain there is a need to be consensus between more than 50% of the network with unlimited actors. (Zheng et al., 2016, O'Leary, 2017; Oh & Shong, 2017;) Important to note, however, is that all participants do not need to be nodes in accordance with the experts.

Incentives

In general, the companies do not have a preference of what incentive that would be used in a potential implementation if blockchain. The literature (Brennan & Lunn, 2016) and experts (A2, BC2) describe that in private and consortium blockchain, the incentive to be a part of the network, the so-called stake, is that the actors have to run the blockchain. It is described in the literature that a monetary reward is used in public blockchains to create an incentive for trustless actors to use their computing power to participate in the blockchain (Brennan & Lunn, 2016; Walport, 2016). This goes in line with the fact that A2 describes that a monetary reward usually is used as a way to incentivise in cases where trust is low.

5.2.2 The Coherency of the Fast Fashion Companies' Perception of the Characteristics

This part of the analysis will add to the assessment of compatibility by examining and discussing the coherency of the characteristics of the blockchain configurations. The results of how each fast fashion company perceives the characteristics are presented in Appendix E, together with an illustration of the compatibility based on the literature and the additional adjustments made by the experts as described. As none of the companies expressed any specific views of the blockchain implementation design characteristics, these are excluded from the discussion of coherency.

When looking at FFC1 (see Appendix E), it is shown that a public blockchain is coherent with the company's current state of relations, wants of benefits and need of scalability. However, its need of privacy and flexibility is ranked as medium and high, which hinder the compatibility of the public blockchain. Based on the adjustments made by the experts, a consortium blockchain could be compatible for FFC1 with the exception of protection against cyber attacks while a private does not achieve the benefits that FFC1 wants. In comparison, a consortium blockchain would be compatible for FFC2 (see Appendix E) when taking the adjustment based on the experts' views into account, due to the coherency of matched characteristics. A public blockchain could have been considered to be compatible if the company would have expressed its need of privacy as being low since it was matched with all other characteristics. Thus, the trade-off does not seem to be very significant for FFC2. The trade-off is more distinct at FFC3 (see Appendix E), which has ranked all benefits as high and its needs as either low or medium. In terms of the company's level of trust, all configurations of blockchains would be possible options. From the perspective of achieving the benefits of blockchains, a public would be the most suitable choice but does not achieve the operation needs. From the perspective of operation needs however, a private or a consortium would fit the needs, but does not achieve the degree of wanted benefits. Thereby, by looking at the coherency for FFC3, none of the configurations seems to be a full match.

FFC4 (see Appendix E) wants a medium degree of the benefits in security and a high degree of transparency and traceability, which speak for a public blockchain. Also, since trust is ranked as medium, a private blockchain is not an option. However, two of the operation needs are also ranked as high, making the trade-off evident. A consortium would be compatible if transparency and traceability would have been ranked as medium or lower. Thus, none of the configurations is fully compatible. Similar results can be found for FFC5 and FFC6 (see Appendix E), with the exception of that FFC5 ranks trust and immutability as high instead of medium and that FFC6 ranks security as high, and traceability as medium. Despite these differences, the trade-off is still evident, which indicates that none of the configurations is fully compatible.

Based on above, it is evident that it is generally difficult to identify one configuration that is fully matched with the company's current state of relations, wanted benefits and operation needs. This confirms that the identified trade-off has significance, not just in theory, but for the companies as well. FFC2 is the only company that is fully matched with a configuration, a consortium blockchain. This company is also the one differing the most from the other companies in terms of how it perceives the characteristics. If assuming that the interviewed fast fashion companies would give an indication about the fast fashion industry in general, it shows that the results differ somewhat between companies. However, although the companies have differing views, some patterns seem to be present. In broad strokes, the fast fashion companies have high trust within their supply chains, although no company describes the trust to be complete. The companies generally want to achieve a medium to high degree of the benefits that blockchain can provide. Moreover, the need of scalability is low, but the need of flexibility and privacy is generally medium to high. Finally, no company is sure what they would prefer when it comes to the blockchain implementation design.

5.3 Determining the Compatibility

The following section aims to determine the compatibility of the different configurations of blockchains in the SCM in the fast fashion industry. In order to do this, the characteristics distinguishing the configurations of blockchains have to be consistent with how the companies in the fast fashion industry perceive these characteristics. In addition, due to the trade-offs evident between the clusters of characteristics, there has to be a coherency between the companies' perception of their current state, wanted benefits and operation needs.

The compatibility of the three configurations of blockchains identified in the literature will be discussed separately below. It is identified that the experts agree with the literature about the division of blockchain technology into permissionless blockchains, which are described as blockchains where actors cannot be excluded, and permissioned blockchains, which are restricted in terms of the actors that can participate. The permissionless consists of the configuration called public blockchain and the permissioned consists of the configurations private blockchain and consortium blockchain.

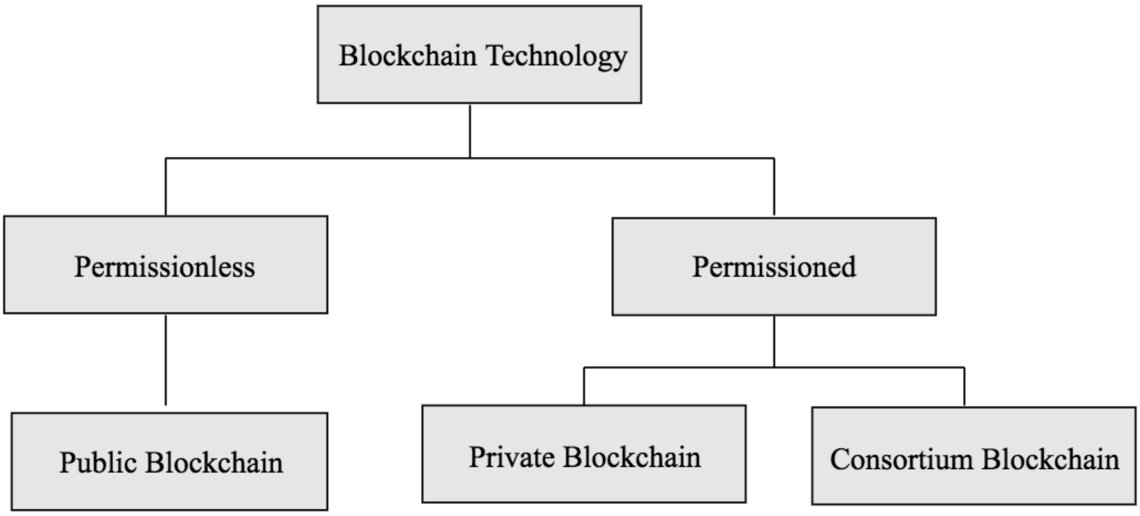

Figure 5.3: Division of Blockchain Technology. Compiled by authors based on literature review.

5.3.1 Public Blockchain

Experts are in agreement with the literature regarding the characteristics defining a public blockchain. No adjustment has therefore been made based on the findings from the experts. There are, however, differences between the interviewed experts. Some say that a public blockchain is not suitable to use in a business setting due to its lack of flexibility and the anonymity of the actors, while others say that the public is superior compared to the other configurations since it is the most secure one. It is argued by BC1 that a public blockchain can be used for storing only certain type of data as a way to keep specific data secure but not use it in the day to day operations.

Regarding the fast fashion companies and their business, the public blockchain is furthest away from how they work today, which might affect the compatibility. For example, several of the companies are currently not very integrated with their suppliers, which indicates that their existing work style is quite different from, as BSC2 and A1 describe, the integrated distributed way of data sharing and storage that a public blockchain entails. Thereby, moving from a not integrated to fully integrated system would likely be a big adjustment for several of the companies.

Regardless, a public blockchain is compatible with the majority of the companies' wanted benefits, existing level of trust and scalability. The fact that the companies express a need for high benefits but low scalability indicates that the trade-off is not evident in this case. The blockchain implementation design does not affect the compatibility for a public blockchain either since the companies are not against or opposed the implementing design associated with a fully public blockchain. However, when it comes to the other characteristics of operation needs, e.g. flexibility and privacy, the public blockchain does not fulfil the existing needs in the companies, making the trade-off evident in this regard. Thereby, since all companies' need of privacy and all but one's need of flexibility are not achieved, it could be indicated that these needs in the industry reduce the compatibility of the public blockchain. With this in mind, and that multiple experts mention that a public blockchain is not easily governed, it is indicated that the fully public might not be fully compatible in the fast fashion companies' SCM today.

5.3.2 Private Blockchain

Experts are generally in agreement with the literature about the characteristics defining a private blockchain. Thus, no adjustments have been made based on the empirical findings from the experts. Several experts brought up that a private blockchain might not be beneficial to use as it provides little benefits, but has many drawbacks. According to the literature (Christidis & Devetsikiotis, 2016) and the experts, the private blockchain might be more compatible in some specific environments, such as when the environment is very controlled, for internal pilots for learning about the technology or for reputational purposes. The experts describe that the reason for this is that it is perceived as being less risky. Having all control over the system as in a private blockchain could be argued to be closer to the existing ways that the companies' current IT-system work today. This would indicate that the companies might feel more comfortable, at least in the beginning, to start with this configuration of blockchain as a pilot. However, when it comes to more large-scale implementations, it can according to the experts be more beneficial to use other alternatives.

The fast fashion companies express that they generally have a high need of flexibility and privacy, which is achievable by the use of a private blockchain. As the companies perceived the operation need of scalability as low, the private is still, with the assumption that a higher scalability would be acceptable, compatible in this regard. Thereby, it can be concluded that all operation needs fit with the private blockchain. As several of the companies describe their current level of trust to be high also speaks for a private blockchain. However, half of the companies describe their trust as medium, which indicates that it cannot for certain be said that a private blockchain is compatible. Also, the trade-off is evident since the companies at the same time perceive the importance of the benefits as high, which is not achievable in the private. The blockchain implementation design does not affect the compatibility since the companies are not against or opposed to the implementing design associated with a fully private blockchain. In terms of coherency, none of the interviewed companies is fully matched with a private blockchain, which indicates that it cannot be concluded that this configuration is fully compatible with the industry's SCM.

5.3.3 Consortium Blockchain

The experts agree with the literature about the characteristics. However, when analysing the results, several things were identified that are not evident in the literature. Firstly, regarding immutability, the experts argue that when having a network of trusted actors, a consortium blockchain could be suitable even if the wish of immutability is high. This is strengthened by the fact that a consortium blockchain provides the possibility to exclude misbehaving actors, which may incentivise the participating actors to behave. Secondly, regarding flexibility, it is in similarity with immutability argued that with a trusted network, a consortium blockchain is not limited to achieving medium flexibility. Lastly, regarding privacy, some experts argue that due to the adaptability of the consortium blockchain, it could be used even if the need of privacy is high.

Although the literature generally describes the consortium blockchain as achieving a degree of the characteristics in the middle of a private and a public (Oh and Shong, 2017), the fact that experts describe the consortium as adaptable means that the consortium blockchain does not necessary have to lie in the exact middle of the two extremes. Thereby, based on the fact that a consortium blockchain is more adaptable, and is able to be designed in accordance to what is wished for, it can be argued to solve some of the trade-off issues between the benefits and needs. Further, as the current states of the companies can generally be described as networks with trust between known actors, the use of a consortium blockchain could be argued to be quite close to their existing work practices. Thus, implementing a consortium blockchain may not be such a large leap from their current state as implementing a fully public blockchain may be.

When considering the coherency between the fast fashion companies' perception of the characteristics, it is identifiable that a consortium match all characteristics for one of the companies. For the remaining companies, the characteristics of a consortium blockchain were matched with all operation needs and the existing level of trust, but not of all benefits. Although it is argued by experts that the consortium could be compatible when it comes to immutability, many companies expressed that they still want a high degree of protection against cyber attack, transparency and traceability. The blockchain implementation design does not affect the compatibility for a consortium since the companies are not against or opposed to the implementing design associated with a consortium blockchain. The fact that most companies were positive towards collaboration amongst trusted partners could indicate that a consortium of trusted authorities might be acceptable. This is speaking for a consortium blockchain, but as the companies are not really sure and want to know more specifically before deciding, it cannot be said with certainty.

Moreover, one suggestion brought up BC1 that could possibly increase some of the benefits, if not reached, was that a company could use a consortium blockchain for the daily operations to achieve the operation needs and regularly timestamp the ledger on a public blockchain. This suggestion could be argued to improve compatibility by getting some degree of the benefits achievable by a public, but at the same time having increased flexibility and privacy achievable in a consortium, and thereby bypassing some of the trade-offs.

5.3.4 Identified Factors Affecting the Compatibility

As mentioned by Rogers (1983), a technology needs to be perceived to be consistent with what the values, needs and past experiences of potential adopters. Thus, the following section will discuss some identified challenges of using blockchains in supply chains and the interviewed companies' view on innovation. The section will end with a future outlook on the different configurations of blockchains in SCM in the fast fashion industry.

5.3.4.1 Challenges of Blockchains in Supply Chains

When discussing the use of blockchain in the SCM in the fashion industry, the companies and the experts discuss some challenges that could indicate that blockchains are not perceived to be completely consistent. The main challenges that the experts and companies perceive are the difficulty of data input and human error, the transferring of physical assets into digital records and finally, the varying IT capacity among suppliers. They will be discussed separately below.

Regarding data input and human error, the majority of the companies discuss the fact that although blockchain technology would provide an increased security and information flow, the data might be incorrect from the beginning. Several companies argue that this is caused by the fact that a lot of data is manually entered. Although Abeyratne and Monfared (2016) mention that blockchain can help reduce the human error, the experts confirm that the effect of the increased immutability is reduced if the data is wrong to begin with. As mentioned by BSC1 and BSC3, this can be difficult to change unless all activities become automated, e.g. by use of IoT in order to exclude the human error totally. But many experts (BC1, BC2, BSC2, BSC3) mention that IoT in combination with blockchain technology would improve the performance. Similarly, FFC5 says that the problem could be avoided by transferred electronically. Since immutability is considered as highly important for the companies, this can be considered as an important factor for the compatibility.

When discussing the potential use of blockchains, the companies also expressed concern regarding the need of transferring physical assets into a digital record. FFC3 argues that physical objects need to be able to be traced and controlled in the supply chain. Several of the companies mention the sample process as being in particular need of identifying the physical object and that this is an area in great need of innovation. Many companies describe this as important for the information flow and FFC3 describes that they work a lot with physical samples that are manually handled and difficult to put into the IT system in their design process. The experts agree that a difficulty of using blockchain in supply chains is the ability to transfer physical data into a digital record. BC3 explains that it requires a digital ID, which BC3 explains is difficult to find if the physical good does not have something unique. Apparel and samples that are quite generic could thereby be argued to be difficult to find a proper digital ID, which could be argued to affect the compatibility since this way of registering the physical asset to a digital record is far from the company's existing work style. However, as BC2 and BSC3 suggest, there are technologies being developed in order to solve this problem that could argue for an increased compatibility. This is also in line with that BC1, BC2, BSC2, BSC3 describe that IoT would increase the performance of blockchains in supply chains.

Thirdly, the companies argued that an obstacle for implementing blockchains in their supply chains could be the varying IT capacity among suppliers. FFC1 even express that it can be difficult to make the suppliers upload simple data electronically. The companies agree that the level of IT capacity varies depending on supplier and the country where the supplier operates. When discussing this issue with the experts, BC3 and BSC2 agree that not all suppliers will have the adequate IT capacity to be nodes in a potential blockchain. However, BC2 does not see this as an obstacle since the IT required to upload data is not that expensive and that all participants do not need to be nodes. FFC1 mentions that it could be necessary to only collaborate with suppliers from more developed countries if it would come to implement blockchain. Several experts mention ways of bypassing the lacking IT capacity by letting external organisations assist suppliers with low IT capacity to upload data.

5.3.4.2 The Fast Fashion Companies' View of Innovation

In addition to this, it is evident from the interviews that almost none of the companies has any experience of blockchain technology, although some of them have a somewhat positive idea of what it could contribute to their supply chain. Several of the companies, however, state that they need further insight into the benefits it can provide in their SCM in order to consider an implementation. Moreover, the majority of the companies have positive experiences of innovation but has a lack of experience regarding innovation in upstream activities. FFC2 and FFC6 say that it will not be likely that they will invest in their upstream activities, while FFC1 and FFC3 would prefer to see innovations in their upstream activities.

5.3.4.3 Future Outlook

Important to note is that the interviewed companies only constitutes a sample, and might not be representative for the whole fast fashion industry. However, the findings imply that the current state, wants and operation needs, with the exception of FFC2, are somewhat similar between the companies. Hence, it can give an indication of what is important in the SCM in the fast fashion industry in terms of the different configurations of blockchains.

As the literature describes, there is a tendency for standards to become established (Schilling, 2013). A1, however, does not think that there will be a standard of blockchain technology due to the fact that the suitability of the configurations depends so much on what a company needs, which is also mentioned by Laurence (2017). This is further strengthened by the trade-off evident between the benefits and operation needs. Based on this reasoning, there will not become a standard as there will not be one single blockchain fulfilling all the wants and needs of the companies but rather that many different blockchains are likely to be developed based on companies' specific wants and needs. As already stated, a consortium blockchain can, due to its adaptability, reduce the effect of the trade-off. However, the adaptability also means that it is likely that many different types emerge also within the configuration of consortium blockchain. This strengthens the reasoning that it likely will not be a standard of one big blockchain, as with the Internet, but rather multiple versions.

6. Conclusions

This chapter will present the conclusions of the study. It will first go through the background before going over to answering the research question. The answer to the research question is illustrated in a figure and is then described in more detail for each of the configurations separately. In the end of the chapter, some recommendations and suggestions for future research will be presented.

6.1 Background to Answering the Research Question

In the process of answering the research question, it was identified that there are a lot of discrepancies, within the literature, among the blockchain experts and between the literature and the blockchain experts. The different views are mostly concerning what to call the different configurations, what counts as a blockchain, and what configuration that is the most suitable in what context. However, the three main configurations identified in the literature review were determined as relevant to keep examine in the process of answering the research question.

It was further identified, with help from the literature and the empirical findings from experts, that there are different clusters and trade-offs that play a role when determining the compatibility of the different configurations. It has been discovered that in order to assess what configuration of blockchain that would be compatible, it is important to take the companies' current level of trust, wanted benefits and operation needs into consideration. Based on this, an analysis model was built in order to answer the research question of the study. In order for a configuration to be compatible, it is argued that its characteristics have to be a fully matched with the company's perception of all clusters of characteristics identified.

6.2 Answering the Research Question

The aim of this study is to investigate what configuration of blockchain that is compatible with supply chain management by applying it to fast fashion industry. Based on this, the following research question was formulated:

How compatible are the different configurations of blockchains with supply chain management in the fast fashion industry?

Overall, it seems that, when assessing the compatibility of different configurations of blockchains in SCM in the fast fashion industry, based on the analysis model built in this study, no configuration is fully compatible. However, the study indicates that each configuration is compatible to a certain extent and in different settings. It is also identified that a consortium blockchain is found to be the most compatible out of the three main configurations. The compatibility of each of the configurations has been illustrated in Figure 6.1. This is then described in more detail in the succeeding sections.

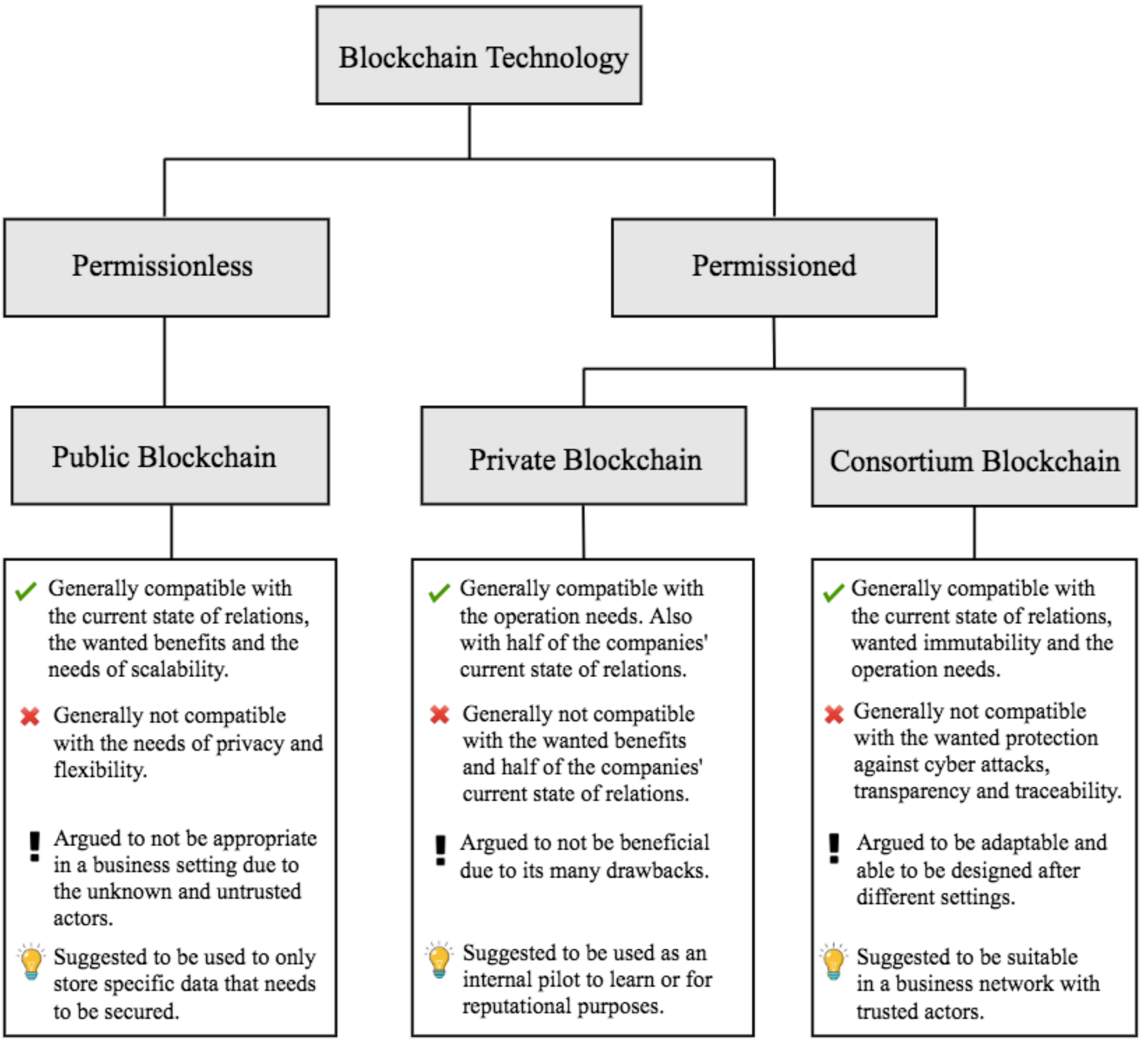

Figure 6.1: Illustration of the Answer to the Research Question. Compiled by authors.

6.2.1 Public Blockchain

Based on the literature, the empirical findings and the analysis model, it has been discussed and concluded that there is an indication that a public blockchain is not fully compatible with the SCM in the fast fashion industry today. Generally, there seems to be a tendency that a public blockchain is consistent with fast fashion companies' current state of relations, the wanted benefits and the need of scalability. However, the characteristics reducing the compatibility are the fast fashion companies' perceived need of high flexibility and privacy. Thereby, there is an indication that the trade-off between benefits and operation needs (flexibility and privacy) is evident in the industry and that there is not a fully match of coherency. Thereby, it is indicated that the public blockchain is not fully compatible. In addition to this, it is mentioned by the experts that a public blockchain may not be appropriate in a business setting, and thereby in SCM, further reducing the compatibility of the public blockchain in SCM in fast fashion industry. Nonetheless, it could be argued as good when wanting to keep specific data secure, but not as a part of the day-to-day operations.

6.2.2 Private Blockchain

Similar to a public blockchain, the result of the study indicates that a private blockchain is not fully compatible with the SCM in the fast fashion industry today. It does, however, show the opposite relationship. Generally, a private blockchain seems to be to be consistent with the fast fashion companies' operation needs of scalability, flexibility and privacy. The characteristics reducing the compatibility are the tendency of fast fashion companies' wanting a high degree of the benefits. Also, only half of the companies have a high level of trust in their supply chains, indicating that the current state of relations reduces the compatibility of a private blockchain. There is thereby no full match found between any of the companies' current state of relations, wanted benefits and operation needs. It is further mentioned by the experts that a private blockchain may bring more disadvantages than advantages, indicating that it might not be fully compatible in the SCM of the fast fashion industry. It might rather be suitable to use a private blockchain for an internal pilot in order to learn about blockchain technology, as it is perceived as less risky, or for reputational purposes as argued by the experts.

6.2.3 Consortium Blockchain

Discrepancies between the empirical findings and the literature indicate that the compatibility of three characteristics (immutability, flexibility and privacy) is higher, not necessary in the middle of private and public, than what were identified in the literature. In general, a consortium blockchain is consistent with the fast fashion companies' current state of relations, perceived want of immutability and operation needs. For the majority of the companies, it was generally the perception of wanting a high degree of protection of cyber attacks, transparency and traceability that reduced the compatibility of the consortium blockchain. Thereby, also for the consortium blockchain, there is not a full match between the majority of the companies' existing level of trust, wanted benefits and operation needs, which indicate that consortium blockchain is not fully compatible with the industry. However, one of the companies constitutes an exception where the consortium, based on the analysis model, can be considered compatible.

When discussing the compatibility of a consortium blockchain, the experts emphasise its adaptability, meaning that the degree of the characteristics does not necessarily have to lay in the exact middle of a private and a public blockchain. Thus, the compatibility of a consortium blockchain might thereby be considered more compatible since it can be more adaptable to a company's practices and argued to solve some of the trade-off issues between the benefits and needs. Further, the experts argue that a consortium is beneficial in a business setting where there is trust in the network. Thus, since the companies generally describe that they have a somewhat trusted network, the consortium could be argued to not be a large leap from their current state. Based on this, the general compatibility of the consortium blockchain in the SCM in fast fashion industry could be increased.

6.3 Recommendations

After conducting the study and answering the research question, there are four recommendations that the authors would like to propose. The first one is a recommendation for assessing what configuration of blockchain that is compatible in a company, and the remaining three are concerned with increasing the overall compatibility in regards to the challenges of blockchains in supply chain identified in the study.

The first recommendation is that when a company wants to assess what configuration of blockchains that is compatible with its SCM, it could potentially identify and, into more detail, assess the current state of relations, wanted benefits, operation needs and blockchain implementing design choice, based on the analysis model (Figure 5.4). This can give a company a general mapping of which blockchain that might be suitable for its business. The second recommendation is to look into the possibilities of automation and use of IoT in order to reduce the human error and that falsely data is put onto the potential blockchain. Thereby avoiding the risk that the benefit of immutability is being decreased due to these potential errors.

The third recommendation is to determine if there is a possibility to assess and create a digital ID for the goods in the industry. This will help in regards to the challenges of putting physical asset onto a digital record. It could also be done by investigating new technologies discussed in the study that in the future might enable the participant to scan the material in order to verify with the digital record. The fourth and last recommendation is to assess the IT capacity of the suppliers, also further down in the supply chain. This in order to map the possible suppliers that could take part in the blockchain. That not all participants need to be nodes and help run the system reduces the need for large IT capacity at all suppliers.

6.4 Future Research

Blockchain technology is still a very new and unexplored subject in the literature and from a business perspective. The authors have by this study attempted to generate a compilation and an analysis model for different configurations compatibility in order to assess the compatibility. However, more and deeper research about the technology is needed. After conducting the study, the authors have some suggestions for future research that will be described below.

Firstly, the identified lack of coherency between academics and practitioners concerning what to call the different configurations and what counts as a blockchain indicates a need for future research and a more fully comprehensive compilation is needed. The authors thereby suggest further investigation regarding this in a more deep and extensive manner than what was performed in this study. This will further help investigate the extensiveness of the compilation presented in this study and thereby strengthen the literature regarding different configurations. As the technology is new and changes in a fast pace, more updated versions will probably be needed in the future.

Secondly, as blockchain technology is still in an early stage of adoption, it would be interesting with further research of the compatibility of different configuration by using the analysis model in other industries and with companies that have reached further in the decision of implementing blockchain. It would be of interest to study the compatibility with more extensive answers regarding the blockchain implementation design cluster. In addition, further research regarding whether the trade-offs identified are evident in other industries could be valuable to gain knowledge for future adoption of the technology. By testing the analysis model it will further build on the existing literature.

Thirdly, during the research, the authors found out that the companies had little knowledge of blockchain technology and had some difficulties to identify and understand the benefits of blockchain to the extent where they felt that an implementation would be necessary. Thereby, to increase the adoption rate of the technology, the authors suggest more research regarding the benefits that blockchain can specifically provide in SCM in fast fashion industries, building upon the existing literature about the benefits that can be achieved within SCM.

7. References

Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology 5*(09), 1-10.

Agarwal, R., & Karahanna, E. (1998). On the multi-dimensional nature of compatibility beliefs in technology acceptance. In *Proceedings of the 19th annual international conference on information systems* (pp. 13-16).

Andrews, M. (1995). Against Good Advice: Reflections on Conducting Research in a Country Where You Don't Speak the Language. *The Oral History Review, 22*(2), 75-86.

Apte, S. & Petrovsky, N. (2016) Will blockchain technology revolutionize excipient supply chain management?. *Journal of Excipients and Food Chemicals 7*(3), pp. 76–78.

Arsov, A. (2017). *Periodic Table of Cryptocurrencies: Blockchain Categorization.* [online] Retrieved 2018-01-30 from: https://ssrn.com/abstract=3095169

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the Age of Blockchains. *arXiv preprint arXiv:1711.03936*.

Bauman, D., Lindblom, P., & Olsson, C. (2016). *Blockchain: Decentralized trust*. Näringspolitiskt forum rapport #15. Entreprenörskapsforum. Örebro Universitet.

Berke. A. (2017). How Safe Are Blockchains? It Depends. *Harvard Business Review.* Retrieved 2018-02-16 from: https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

Brennan, C., & Lunn, W. (2016). *Blockchain Connection series - The Trust Disrupter.* Credit Suisse. Retrieved 2018-02-04 from: https://plus.credit-suisse.com/rpc4/ravDocView?docid=NQDC92AF-WErFXS

Bruce, M., and L. Daly. 2011. Adding Value: Challenges for UK Apparel Supply Chain Management– A Review. *Production Planning & Control* 22 (3): 210–220.

Bruce, M., Daly, L., & Towers, N. (2004). Lean or agile: A solution for supply chain management in the textiles and clothing industry? *International Journal of Operations & Production Management, 24*(2), 151-170.

Bryman, A. & Bell, E. (2011) Business Research Methods. 3rd edition. Oxford University Press: New York

Buchanan, D. (2017). *The Zara workers' protest shows why fast fashion should worry all of us.* The Guardian. Retrieved 2018-04-28 from: https://www.theguardian.com/commentisfree/2017/nov/08/zara-workers-protest-fast-fashion-worry-all-of-us

Burbidge, R. (2017). The blockchain is in fashion. *The Trademark Reporter* 107(6), 1262-1268.

Buterin, V. (2015, August 7). *On public and private blockchain. [Blog Post]* Retrieved 2018-02-20 from: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Buterin, V. (2016, January 15). *Privacy on a Blockchain. [Blog Post]* Retrieved 2018-02-22 from: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

Casey, M., & Wong, P. (2017, March). Global supply chains are about to get better, thanks to blockchain. *Harvard Business Review*. Retreived 2018-03-05 from: https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain

Chan, Ngai, & Moon. (2017). The effects of strategic and manufacturing flexibilities and supply chain agility on firm performance in the fashion industry. *European Journal of Operational Research, 259*(2), 486-499.

Chan, F., & Qi, H. (2003). An innovative performance measurement method for supply chain management. *Supply Chain Management: An International Journal, 8*(3), 209-223.

Chang, C., Chiang, D., & Pai, F. (2012). Cooperative strategy in supply chain networks. *Industrial Marketing Management, 41*(7), 1114-1124.

Chou, D., Tan, & Yen. (2004). Web technology and supply chain management. *Information Management & Computer Security, 12*(4), 338-349.

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

Christopher, M., Lowson, R., & Peck, H. (2004). Creating agile supply chains in the fashion industry. *International Journal of Retail & Distribution Management, 32*(8), 367-376.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of* (pp. 1-6). IEEE.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Wattenhofer, R. (2016, February). On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security* (pp. 106-125). Springer, Berlin, Heidelberg.

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017, May). Blockbench: A framework for analyzing private blockchains. In *Proceedings of the 2017 ACM International Conference on Management of Data* (pp. 1085-1100). ACM.

Eriksson, P. and Kovalainen, A. (2008). *Qualitative Methods for Business Research*. London: Sage

Etwaru, R. [TEDx Talks] (2017, January 29). *Blockchain: Massively Simplified* [Video File]. Retrieved from: https://www.youtube.com/watch?v=k53LUZxUF50

Fanning, K. & Centers, D. P. (2016). Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance, 27*(5), 53-57.

Foerstl, K., Schleper, M.C., & Henke, M. (2017). Purchasing and supply management: From efficiency to effectiveness in an integrated supply chain. *Journal of Purchasing and Supply Management. 23*(4). p 223-228

Galbraith, J. and Kazanjian, R. (1986). Strategy Implementation: Structure, Systems, and Process. St Paul: West Publishing

Deloitte. (2017). *When two chains combine - Supply chain meets blockchain.* Retrieved 2018-03-03 from:
https://www2.deloitte.com/ch/en/pages/technology/articles/supply-chain-meets-blockchain.html

Hendriksz, V. (2017). *UK fashion brands still lacking transparency in their supply chains.* Fashion United. Retrieved 2018-03-30 from: https://fashionunited.uk/news/business/uk-fashion-brands-still-lacking-transparency-in-their-supply-chains/2017042724321

IBM. (2017a) *Blockchain security: What keeps your transaction data safe?* Retrieved 2018-02-10 from: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

IBM. (2017b). *The similarities of public and private blockchain.* Retrieved: 2018-02-10 from: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Kaur, H. (2016). *Low wages, unsafe conditions and harassment: fashion must do more to protect female workers.* The Guardian. Retrieved 2018-04-28 from: https://www.theguardian.com/sustainable-business/2016/mar/08/fashion-industry-protect-women-unsafe-low-wages-harassment

Khurana, K., & Ricchetti, M. (2016). Two decades of sustainable supply chain management in the fashion business, an appraisal. *Journal of Fashion Marketing and Management, 20*(1), 89-104.

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *In Security and Privacy (SP), 2016 IEEE Symposium on (pp. 839-858). IEEE.*

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027-1038.

Laurence, T. (2017). *Debunking Blockchain Myths (And How They Will Impact The Future Of Business.* Forbes. Retrieved 2018-02-09 from: https://www.forbes.com/sites/yec/2017/05/04/debunking-blockchain-myths-and-how-they-will-impact-the-future-of-business/#21e89e725609

Lefroy, W. (2017). *Blockchain: Changing Interaction in the F&A Supply Chain from Paddock to Plate.* Retreived 2018-04-24 from: https://research.rabobank.com/far/en/sectors/farm-inputs/Blockchain_changing-interaction-in-the-FandA-supply-chain-from-paddock-to-plate.html

Lemieux, V. L. (2016). Trusting records: is Blockchain technology the answer?. *Records Management Journal*, *26*(2), 110-139.

Levy, M. and Weitz, B.A. (2008), Retailing Management, 7th ed., McGraw-Hill Irwin, Boston, MA.

Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, *19*(5), 653-659.

Lin, J., Shen, Z., Miao, C., & Liu, S. (2017). Using blockchain to build trusted LoRaWAN sharing server. *International Journal of Crowd Science*, *1*(3), 270-280.

Lipton, A. (2018). Blockchains and distributed ledgers in retrospective and perspective. *The Journal of Risk Finance, 19*(1), 4-25

Loop, P. (2017). *Blockchain: The Next Evolution of Supply Chains.* Industry Week. Retrieved 2018-01-21 from: http://m.industryweek.com/supply-chain/blockchain-next-evolution-supply-chains

Lopes de Sousa Jabbour, A., Gomes Alves Filho, A., Backx Noronha Viana, A., & José Chiappetta Jabbour, C. (2011). Measuring supply chain management practices. *Measuring Business Excellence, 15*(2), 18-31.

Lu, Q., & Xu, X. (2017). Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. *IEEE Software*, *34*(6), 21-27.

Masteika, & Čepinskis. (2015). Dynamic Capabilities in Supply Chain Management. *Procedia - Social and Behavioral Sciences, 213*, 830-835.

Mattila, J. (2016). *The Blockchain Phenomenon–The Disruptive Potential of Distributed Consensus Architectures* (No. 38). The Research Institute of the Finnish Economy.

Maxwell, W., & Salmon, J. (2017). *A guide to blockchain and data collection.* Hogan Lovells. Retrieved 2018-02-20 from: https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192-222.

Mouritsen, J., Skjøtt-Larsen, T., & Kotzab, H. (2003) Exploring the contours of supply chain management. *Integrated Manufacturing Systems*. 14(8), 686-695

Moyano, J. P., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, *59*(6), 411-423.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. [White Paper] Retrieved 2018-02-02 from: https://bitcoin.org/bitcoin.pdf

Nicovich, S.G. and Dibrell, C.C. (2007). Integration of value chain and Porter's (1980) competitive strategies into market orientation conversation: an examination upstream and downstream activities. *Journal of Business and Economic Studies, 113*(2), 91-106.

Nowiński, W. & Kozma, M. (2017) How Can Blockchain Technology Disrupt the Existing Business Models? *Entrepreneurial Business and Economics Review : EBER, 5*(3), 173-188.

Oh, J., & Shong, I. (2017). A case study on business model innovations using Blockchain: focusing on financial institutions. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 335-344.

O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. *Intelligent Systems in Accounting, Finance and Management*, *24*(4), 138-147.

Perry, P. (2018). *Water pollution, toxic chemical use and textile waste: fast fashion comes at a huge cost to the environment.* Independent. Retrieved 2018-04-28 from: https://www.independent.co.uk/life-style/fashion/environment-costs-fast-fashion-pollution-waste-sustainability-a8139386.html

Porter, M. (1985). Competitive advantage: Creating and sustaining superior performance. New York: Free Press.

Power, D. (2005) Supply chain management integration and implementation: a literature review. *Supply Chain Management: An International Journal*. 10(4), 252-263.

Priya, M. (2018). A prospective study on the emerging Blockchain with IoT. *International Conference on Advances in computer Science and Technology (IC-ACT'18) - 2018* Retreived 2018-03-03 from: http://www.ijetjournal.org/Special-Issues/ICACT18/ICACT18101.pdf

Provenance. (2016). *From shore to plate: Tracking tuna on the blockchain.* Retrieved 2018-02-10 from: https://www.provenance.org/tracking-tuna-on-the-blockchain

Provenance. 2018. *Increasing transparency in fashion with blockchain.* Retrieved 2018-04-29 from: https://www.provenance.org/case-studies/martine-jarlgaard

PWC. (2016a). *A primer on blockchain (infographic).* Retrieved 2018-04-19 from: http://usblogs.pwc.com/emerging-technology/a-primer-on-blockchain-infographic/

PWC. (2016b). *The evolution of bitcoin' public blockchain will usher in resilient, ubiquitous online marketplaces that won't need intermediaries at all.* Retrieved 2018-02-07 from: http://usblogs.pwc.com/emerging-technology/private-blockchains-public-or-both/

ResearchBriefs (2018) *Banking Is Only The Beginning: 36 Big Industries Blockchain Could Transform*. Retrieved 2018-02-18 from: https://www.cbinsights.com/research/industries-disrupted-blockchain/

Rogers, E. (1962). *Diffusion of innovations.* New York: Free Press of Glencoe.

Rogers, E. (1983). *Diffusion of innovations* (3rd ed). New York: Free Press.

Rogers, E. (2003). *Diffusion of innovations* (5th ed). New York: Free Press.

Ross, E. S. (2017). Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues. *Catholic University Journal of Law and Technology*, *25*(2), 7.

Schilling, M. (2013). *Strategic Management of Technological Innovation*. 4th ed., New York: McGraw-Hill.

Sherif, K., Zmud, R., & Browne, G. (2006). Managing Peer-to-Peer Conflicts in Disruptive Information Technology Innovations: The Case of Software Reuse. *MIS Quarterly,30*(2), 339-356.

Siegle, L. (2013, October 6) *How ethical are high-street clothes?* The Guardian. Retrieved 2018-03-28 from: https://www.theguardian.com/environment/2013/oct/06/ethical-high-street-clothes-supply-chain-bangladesh

Suárez, F., & Utterback, J. (1995). Dominant designs and the survival of firms. *Strategic Management Journal, 16*(6), 415-430.

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (First ed.). Sebastopol: O'Reilly Media.

Swan, M. (2017). Anticipating the Economic Benefits of Blockchain. *Technology Innovation Management Review 7*(10), 6-13.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Penguin Random House

Tsang, E. (1998). Inside Story: Mind Your Identity When Conducting Cross National Research. *Organization Studies, 19*(3), 511-515.

Utterback, J. & Abernathy, W. (1975) A Dynamic Model of Process and Product Innovation. *Omega* 3(6), 639-656

Walport, M., (2016). *Distributed Ledger Technology - Beyond Block Chain*. London: UK Government of Science.

Warburg, B. [TED] (2016, January 29). *How blockchain will radically transform the economy* [Video File]. Retrieved from: https://www.youtube.com/watch?v=RplnSVTzvnU

Xu, J. J. (2016). Are blockchains immune to all malicious attacks?. *Financial Innovation*, *2*(1), 2:25.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?-A Systematic Review. *PLoS ONE, 11*(10), E0163477.

Zalan. (2018). Born Global on blockchain. *Review of International Business and Strategy*, 28(1), 19-34.

Zarley Watson, M., & Yan, R. N. (2013). An exploratory study of the decision processes of fast versus slow fashion consumers. *Journal of Fashion Marketing and Management: An International Journal*, *17*(2), 141-159.

Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). *Blockchain challenges and opportunities: A survey. Work Pap.–2016.* Retrieved 2018-02-02 from: https://www.researchgate.net/profile/Hong-Ning_Dai/publication/319058582_Blockchain_Challenges_and_Opportunities_A_Survey/links/59d86d50a6fdcc2aad0a2f2a/Blockchain-Challenges-and-Opportunities-A-Survey.pdf

8. Appendix

Appendix A: Keywords for Literature Review

New Technology Adoption

Keywords Phase 1	Keywords Phase 2	
Diffusion of innovation		
Diffusion of new technology		
New technology adoption		
Innovation adoption		
Compatibility	+	Innovation
		New technology
		Blockchain technology

Blockchain Technology

Keywords Phase 1	Keywords Phase 2	
Blockchains	+	Configuration
Block-chain		Types
Blockchain technology		Public
		Private
		Consortium
		Permissionless
		Permissioned
		Difference between
		Uncertainties
		Challanges
		Supply chain
		Supply chain management
		Fast fashion industry

Appendix B: E-mail

Dear,

We are two students from the School of Business, Economic, and Law at the University of Gothenburg, Sweden, studying the MSc. in Innovation and Industrial. We are currently writing our master thesis about Blockchain technology in the fashion industry, focusing on the supply chain management.

Supply chains are said to experience radical improvements by blockchain technology. However, there is a gap in how it will be used in a practical sense. As the fashion industry is highly reliant upon an efficient supply chain, we seek to investigate what blockchains would need to look like in order to be applied in your industry. Our aim is to map the fast fashion industry in order to assess what kind of blockchain that would be suitable in the supply chain management.

Thereby, we would like to get in touch with persons with knowledge and strategic insight in the needs, challenges and objectives in your supply chain. To be clear, we are not looking for any knowledge about blockchains, but rather to get insight into the supply chain process. We would be very grateful to get in contact with a person who has the time to contribute with an interview (preferably in March). You can, of course, choose to be anonymous in the report.

Please get back to us with a time and date if you find this interesting, or if know someone else that might be valuable for us to talk with. Do not hesitate to ask if you want to know more about the study.

Thank you in advance!

Appendix C: Interview Guides

Interview Guide for Experts

The interviews were performed by initially asking general questions about blockchain technology and the different configurations. If all characteristics distinguishing the configurations were not brought up in the general part, specific questions about them were asked.

General information of blockchains	
• Could you give a short presentation about yourself and what kind of experience/knowledge you have of blockchains? • Could you describe the different types of blockchains? Differences between them? • What is the difference between a private and a public? • What is the difference between a public and consortium? • What is the difference between a private and consortium? • What is the difference between a private and a traditional database? • What problems or limitations are there with the different types? • What are your thoughts about blockchains in supply chains? • Which type do you think will be the most used one in the future?	
Characteristics of the Different Configurations of Blockchains	
Consensus Power	• How does the power/control structure look like in the different types?
Immutability	• How do the different types differ in terms of immutability?
Protection against cyber attacks	• How do the different types differ in terms of cyber security
Scalability	• How do the different types handle transactions? In terms of how fast a transaction can be registered/performed and how many transactions that can be made in the blockchain?
Cost	• What kind of costs is associated with the different kinds of blockchain? At implementing? At maintenance?
Existing Trust	• How important is the relationship with those who have access to the blockchain?
Flexibility	• What opportunities do the different types provide in terms of flexibility?
Privacy	• What type of information is possible to conceal in the different types?
Incentives	• How does the incentives look like in the different types?
Transparency	• What information can be shared in the different types?
Traceability	• How much information can be traced in the different types?

Interview Guide for Fast Fashion Companies

The first part of the interview consisted of a general part, aiming to map the companies' supply chains. During the second part, each of the characteristics distinguishing the configurations of blockchain was discussed if they had not been brought up in the first part. In addition to discussing each characteristic in general, the companies were asked how they perceive the characteristics asked about their perception of each characteristic based on the way it is distinguished in the different configurations of blockchains. For example, after discussing consensus power, the respondents were asked what they would prefer out of the alternatives "single authority", "consortium of authority" and "fully distributed authority" in their supply chain. Similarly, after discussing immutability, the respondents were asked whether they perceive the importance of immutability in their supply chain as "low". "medium" or "high".

General information about supply chain

- Can you briefly describe your supply chain? By supply chain we mean all the activities taking place from the start of the chain until the products arrive to you, thereby not including distribution to customer.
- What do you need in order for the supply chain to work well?
- What challenges do you see in your supply chain?
- What are your view on innovation in your supply chain?
    - Do you have any prior experiences of implementing a shared system in your supply chain?
    - Prior experiences of blockchains?
- How far back in your supply chain do you get information?

Characteristics	**Questions**	**Private**	**Consortium**	**Public**
Consensus Power *The distribution of consensus power.*	If you would implement blockchain, who in the supply chain would you like to have the power to validate transactions?	*Single Authority*	*Consortium of Authority*	*Fully Distributed Authority*
Immutability *Being sure that information has not been tampered with.*	When you receive information in your supply chain, what are your thoughts about if this information could have been tampered with?	*Low*	*Medium*	*High*
Protection against cyber attacks *Being protected against external cyber attacks and hacking.*	What are your thoughts about cyber attacks in your supply chain?	*Low*	*Medium*	*High*
Scalability *The ability to perform a high amount of transactions. **	How fast do you get information about things that have occurred in your supply chain?	*High*	*Medium*	*Low*
Cost *The level of transaction cost.*	What are your thoughts about cost if you were to implement blockchain in your supply chain?	*Low*	*Medium*	*High*

Existing Trust *The existing level of trust between actors.*	What are your thoughts about trust in your supply chain?	*High*	*Medium*	*Low*
Flexibility *Being able to change rules and settings about the sharing of information and transactions.*	What are your thoughts about flexibility in your supply chain?	*High*	*Medium*	*Low*
Privacy *Being sure that confidential information is concealed.*	What are your thoughts about privacy in your supply chain?	*High*	*Medium*	*Low*
Incentives *The incentives for actors to run the network.*	Do you think that the incentives for people in your supply chain to add information onto the blockchain would be based on monetary rewards or that all work for a common goal?	*Stake*	*Stake*	*Monetary Reward*
Transparency *Having access to information that is shared between the actors in the supply chain.*	What are your perspective on transparency in your supply chain?	*Low*	*Medium*	*High*
Traceability *Being able to trace products back in the supply chain.*	What are your perspective on traceability in your supply chain?	*Low*	*Medium*	*High*
Finally, do you have something you would like to add?				

** Explanation: Low = 7 transactions per second or less, High = 2 000 transactions per second or more.*

Appendix D: Perception of Each Characteristics Inserted in the Analysis Model

Below is the compilation of the empirical findings of the companies' perception of each characteristic.

	Private Blockchain	Consortium Blockchain	Public Blockchain
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*	FC1, FC3, FC5	FC2, FC4, FC6	
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*	FC2	FC4, FC5	FC1, FC3, FC6
Immutability *The degree of wanting to be sure that information has not been tampered with.*		FC4	FC1, FC2, FC3, FC5, FC6
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*		FC1, FC2	FC3, FC4, FC5, FC6
Traceability *The degree of wanting to be able to trace products back in the supply chain.*	FC2	FC1, FC6	FC3, FC4, FC5
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*		FC3	FC1, FC2, FC4, FC5, FC6
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	FC1, FC3, FC4, FC5, FC6		FC2
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*	FC3, FC4, FC5, FC6	FC1, FC2	

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$ $ Medium	$ $ $ High
	n/a	n/a	n/a
Consensus power *The distribution of consensus power connected to each configuration of blockchain.*	• Single Authority	Consortium of Authority	∞ Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward

Appendix E: Coherency of Characteristics for each Fast Fashion Company

From the discussion about the current state of relations, it can be read that the more trust there is between the actors, the more configurations are suitable, while less trust means that less configurations are possible. Moreover, based on what the companies discussed in the interviews, it was evident that even though some companies ranked the benefits of blockchains as medium or low, it was repeatedly mentioned that this was only a minimum requirement, and that they would the always like more of it. Similarly with the operation needs, the companies described that their ranking was in fact what they need, but that they would not be negatively affected by achieving more of it. If assuming that this reasoning is valid for all companies, more configurations than the one corresponding with what a company ranked can be compatible. Moreover, a number of experts point out some issues related to the characteristics that indicate that more alternatives can be compatible than what initially could be read from the literature.

Thus, the square corresponding to what the company ranked will be marked with dark green, indicating that this is degree of a characteristic is compatible with what the company has, wants or needs. However, in the analysis, it was identified that the characteristics have different relationships to compatibility. Based on this, the lighter green will be used to mark the squares that also depict compatibility assuming that: (1) The company's current state of relations, its level of trust, is seen as a minimum level when it comes to the suitability of the configurations, meaning that a blockchain that requires the same, or a lower, level of trust that the company has is consistent. (2) The company is not opposed to achieving a higher level of the benefits of blockchains that the stated degree of importance, such as protection against cyber attacks, immutability, transparency and traceability. (3) The company is not opposed to getting more of the operation needs than the stated degree of importance, such as scalability, flexibility or privacy.

When the experts have expressed views that differ from the literature, adjustments will be made in the table showing the result by marking the additional compatible alternative will yellow. The squares with the degree of characteristics that is not compatible with what the companies ranked will instead be marked with red. Thus, this will include the trust levels that are higher than the company has, that the degrees of benefits that are less than the company wants and the degrees of the operations needs that are less than the company needs.

Explanation of Colours and Symbols	
	Compatible, based on the alternative chosen by the fast fashion company.
	Compatible, based on the discussion from the fast fashion companies.
	Compatible, based on the findings from the blockchain experts.
	Not compatible.

Fast Fashion Company 1

	Private Blockchain	Consortium Blockchain	Public Blockchain
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*	FFC1		
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*			FFC1
Immutability *The degree of wanting to be sure that information has not been tampered with.*			FFC1
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*		FFC1	
Traceability *The degree of wanting to be able to trace products back in the supply chain.*		FFC1	
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*			FFC1
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	FFC1		
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*		FFC1	

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$$ Medium	$$$ High
	n/a	n/a	n/a
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	∞ Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward
	n/a	n/a	n/a

Fast Fashion Company 2

	Private Blockchain	Consortium Blockchain	Public Blockchain
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*		FFC2	
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*	FFC2		
Immutability *The degree of wanting to be sure that information has not been tampered with.*			FFC2
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*		FFC2	
Traceability *The degree of wanting to be able to trace products back in the supply chain.*	FFC2		
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*			FFC2
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*			FFC2
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*		FFC2	

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$$ Medium	$$$ High
	n/a	n/a	n/a
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward
	n/a	n/a	n/a

Fast Fashion Company 3

	Private Blockchain	Consortium Blockchain	Public Blockchain
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*	FFC3		
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*			FFC3
Immutability *The degree of wanting to be sure that information has not been tampered with.*			FFC3
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*			FFC3
Traceability *The degree of wanting to be able to trace products back in the supply chain.*			FFC3
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*		FFC3	
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	FFC3		
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*	FFC3		

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$$ Medium	$$$ High
	n/a	n/a	n/a
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward
	n/a	n/a	n/a

Fast Fashion Company 4

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*		FFC4	
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*		FFC4	
Immutability *The degree of wanting to be sure that information has not been tampered with.*		FFC4	
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*			FFC4
Traceability *The degree of wanting to be able to trace products back in the supply chain.*			FFC4
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*			FFC4
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	FFC4		
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*	FFC4		

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$$ Medium	$$$ High
	n/a	n/a	n/a
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward
	n/a	n/a	n/a

Fast Fashion Company 5

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*	FFC5		
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*		FFC5	
Immutability *The degree of wanting to be sure that information has not been tampered with.*			FFC5
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*			FFC5
Traceability *The degree of wanting to be able to trace products back in the supply chain.*			FFC5
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*			FFC5
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	FFC5		
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*	FFC5		

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$$ Medium	$$$ High
	n/a	n/a	n/a
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	∞ Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward
	n/a	n/a	n/a

Fast Fashion Company 6

	Private Blockchain	**Consortium Blockchain**	**Public Blockchain**
CURRENT STATE OF RELATIONS	High	Medium	Low
Existing Trust *The current level of trust between the actors.*		FFC6	
BENEFITS OF BLOCKCHAINS	Low	Medium	High
Protection against cyber attacks *The degree of wanting to be protected against external cyber attacks and hacking.*			FFC6
Immutability *The degree of wanting to be sure that information has not been tampered with.*			FFC6
Transparency *The degree of wanting access to information that is shared between the actors in the supply chain.*			FFC6
Traceability *The degree of wanting to be able to trace products back in the supply chain.*		FFC6	
OPERATION NEEDS	High	Medium	Low
Need of Scalability *The degree of needing to perform a high amount of transactions*			FFC6
Need of Flexibility *The degree of needing to change rules and settings about the sharing of information and transactions.*	FFC6		
Need of Privacy *The degree of needing to be sure that confidential information is concealed.*	FFC6		

BLOCKCHAIN IMPLEMENTATION DESIGN			
Cost *The level of transaction cost connected to each configuration of blockchain.*	$ Low	$ $ Medium	$ $ $ High
	n/a	n/a	n/a
Consensus Power *The distribution of consensus power connected to each configuration of blockchain.*	Single Authority	Consortium of Authority	∞ Fully Distributed Authority
	n/a	n/a	n/a
Incentives *The incentives for actors to run the network in each configuration of blockchain.*	Stake	Stake	Monetary Reward
	n/a	n/a	n/a