CHALMERS
UNIVERSITY OF TECHNOLOGY

Counter the Counterfeiters

Examining Blockchain's Suitability in Industrial Supply Chains

Master's Thesis in the Master's Programme
Management and Economics of Innovation

MARTIN BJÖNTEGAARD
LOVISA HOLMGREN

Department of Technology Management and Economics
Division of Entrepreneurship and Strategy
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2019
Report No. E 2019:083

Master's thesis E2019:083

Counter the Counterfeiters

Examining Blockchain's Suitability in Industrial Supply Chains

Martin Björntegaard
Lovisa Holmgren

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Technology Management and Economics
Division of Entrepreneurship and Strategy
Chalmers University of Technology
Gothenburg, Sweden 2019

Counter the Counterfeiters
Examining Blockchain's Suitability in Industrial Supply Chains
Martin Björntegaard, Lovisa Holmgren

Supervisor: Charlotta Kronblad, Division of Entrepreneurship and Strategy
Examiner: Joakim Björkdahl, Department of Technology Management and Economics

Master's Thesis E2019:083
Department of Technology Management and Economics
Division of Entrepreneurship and Strategy
Chalmers University of Technology
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Abstract

The problem with counterfeiting of physical products is increasing worldwide and affects global manufacturing companies' supply chains to a large extent. Blockchain is a relatively new technology that is involved in many supply chains projects today and could potentially help to mitigate this problem.

The purpose of this thesis is to examine the applicability of blockchain technology in industrial supply chains to assess its suitability to prevent counterfeiting of physical products. The authors will also provide SKF with further implications and recommendations based on the suitability.

The study was performed through the use of a qualitative approach, with an abductive process that allowed the authors to iterate between theory and social observations. First, a theoretical framework was created to enable a good understanding of the blockchain technology and global supply chains in general. Second, interviews, a case study of SKF's extensive supply chain together with secondary data constituted the data collection to enable the authors to answer the underlying research questions. Finally, the collected data was compared with the theoretical framework and formed a basis for the analysis and final conclusion to answer the general research question.

The research reveals that there exist no universal definition of blockchain but the benefits of using the technology in a supply chain could be many. Transparency, decentralized power, immutability and security just to mention a few. However, there are also several challenges connected with this that needs to be taken into account. A large amount of actors are hard to coordinate, high variation of digitalization between the actors and the difficulties to tag the unique product could be seen as the main challenges.

At first, blockchain seems suitable to implement in a supply chain due to its many benefits, but soon the challenges outweigh these benefits leading to the conclusion that it is not suitable for the intended purpose.

Acknowledgements

First of all, we would like to thank our supervisor at Chalmers, Charlotta Kronblad, for helping us along the way with constructive feedback and recommendations when needed. A sincere thank you is also addressed to SKF and especially the Group Brand Protection Unit for making this thesis possible and giving us the opportunity to work alongside them every day. This includes thanking our supervisor at SKF, Petter Rönnborg, and the unit's director, Johan Bravert.

Furthermore, we are very grateful for the opportunity to interview all the blockchain experts, SKF employees and industry experts and receiving their valuable knowledge, which contributed a great deal to the result of this study. We also thank everyone who helped us with this thesis in general through feedback and insights.

Finally, a generous thank you to Chalmers and our fellow students for helping us through these five years, it has been marvelous.

Lovisa Holmgren & Martin Björntegaard

Gothenburg, May 2019

Contents

List of Figures

Terminology

Bitcoin - A digital cryptocurrency that was launched in 2009 and that is based on blockchain technology.

CPU - Central Processing Unit. Electronic circuit in a computer that carries out the instructions of a computer program.

Double-spending - When a digital currency is spent twice.

EDI - Electronic Data Interchange. EDI means that there is an integration between business systems of the seller and buyer, where orders can be automatically generated without any human intervention.

GBP - Group Brand Protection. The unit responsible for SKF's trademarks, and that fights counterfeiting of SKF bearings.

ICT- Information and Communications Technology.

OEM - Original Equipment Manufacturer. For example a car manufacturing company.

SKU - Stock Keeping Unit. A unique code that is given to every individual product item that a manufacturer produce, in order to be able to identify that specific product.

1

Introduction

This chapter gives an introduction to this thesis and the problems it aims to tackle. The problem of counterfeiting is presented from a holistic perspective and then some existing ways to work against it are briefly discussed. The potential for blockchain technology to make it harder for counterfeiters is then broadly introduced. Thereafter, the background to the thesis is presented, before defining the purpose and research questions along with delimitations of the study.

1.1 What Is Counterfeiting?

Counterfeiting is one of the problems connected to global trade and globalization, and the World Trade Organization (WTO) define it as *"unauthorized representation of a registered trademark carried on goods identical or similar to goods for which the trademark is registered, with a view to deceiving the purchaser into believing that he/she is buying the original goods"* (WTO, 2019). According to the Organization for Economic Co-Operation and Development (OECD) (2007), counterfeiting is growing in scope, scale and threat. This since fake products are being produced and consumed in virtually all economies, with Asia emerging as the single largest producing region. The types of products being counterfeit has, during the recent years, expanded from luxury items to products that have an impact on personal health and safety. OECD (2007) further argue that counterfeit products are of concern to governments, businesses and consumers. To governments they are of concern because of the negative impact they might have on innovation, the threat they pose to the welfare of consumers and the substantial resources that they channel to criminal networks, organized crime and other groups that disrupt and corrupt society. To businesses, counterfeit products are of concern because of the impact they might have on sales and licensing, brand value and firm reputation as well as the ability of firms to benefit from the breakthroughs they make in developing new products. Since substandard counterfeit and pirated products could pose vital safety and health risks, they are of concern to those who consume them as well.

Berman (2008) classifies counterfeit products into four different types: (1) knockoffs

- a duplicate of the original that bear a different name and customers are aware that they are purchasing an inexpensive copy; (2) true counterfeit products - products that are very similar to the original and use the same brand name; (3) products manufactured by an outsourced supplier by using a "third shift" that the original manufacturer is unaware of and (4) products manufactured by an outsourced supplier that do not meet the required standard but are not properly labeled as defect or destroyed. Thus, there are two different types of counterfeiters; the ones who sell the product for a similar price as for the original product and the one who sell the product for a significant lower price. That leads to two different types of consumers of counterfeit products; the ones who think they are buying the original product and the ones that know they are buying a counterfeit.

According to a study conducted by OECD in collaboration with the European Union Intellectual Property Office (EUIPO) (2016), the international trade of counterfeit products in 2013 corresponded to 2,5% of world trade, which is equivalent to USD 461 billion. In the European Union, these products amounted up to 5,1% of imports the same year, comparable to USD 116 billion. A previous study made by the same organizations in 2008 estimates that the market for these products was 1,9% of world imports, implying that the threat of counterfeiting has increased during the past ten years. These numbers also imply that the impact of counterfeit products is twice as high for countries within the EU than it is for the world as a whole. The increasing use of e-commerce provides the counterfeiters with a platform to cost efficiently capture a large number of potential customers (OECD/EUIPO, 2016). E-commerce enables counterfeiters to get access to areas that were previously beyond their scope. Counterfeiters are also able to avoid being caught by functioning across multiple jurisdictions as well as closing down and setting up websites overnight without decreasing their customer base. Counterfeiting is therefore a profitable market since by imitating a product there are no costs associated with research and development, advertising, quality control standards or regulated labor (Harvey, 1987). Hence, counterfeiters have none of the traditional costs related to introducing or selling a specific product which enables them to sell the product at a lower price while still generating profit. Thereof, it is important for companies producing the original product to fight counterfeiting and piracy to both maintain and regain sales but also to protect their brand.

1.2 Counter the Counterfeiters

Since a company's brand is one of the most valuable intangible assets they posses and brand success raise counterfeiters, it is crucial to protect it as much as possible (Green and Smith, 2002). WTO developed the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) as an effort to control counterfeiting. TRIPS is an international legal agreement, that all the member nations of WTO has to be a part of, that sets minimum standards of regulations by national governments regarding multiple forms of intellectual property. This means that individual gov-

ernments can put pressure on countries that lacks laws and rules about intellectual property, and try to influence their activities.

Other courses of action to address counterfeiting are to educate stakeholders at the source by convincing governments that intellectual property protection is in their best long-term interest, and use advertising to inform customers about counterfeiting to eliminate the market for such products (Shultz and Saporito, 1996). Companies exposed to counterfeiting can also use different techniques to tag their products in way that is difficult to duplicate, which is further described in section *3.3 Techniques to Create Unique Identities*. They can also create coalitions with other industry members to battle the counterfeiting together. Further, examples of raids of manufacturers that sell and produce counterfeit products have shown to be an effective way to reduce counterfeiting and regain sales (Green and Smith, 2002).

1.3 Blockchain and Counterfeiting

In later years, blockchain technology, further referred to as simply blockchain, have rapidly gained a strong interest in society. During the end of 2017, a large surge was created around the technology and businesses in several industries tried to jump on the bandwagon and drive business with what they claimed to be blockchain-backed products and services. Web searches on the term "Blockchain" exploded and reached its peak a few days before Christmas that year (Google, 2019). The sudden increase in interest largely affected the world's biggest cryptocurrency Bitcoin (which is based on blockchain), that reached its all-time high closing price of $19 345 on the 16th of December 2017 (Yahoo, 2019). The price then plummeted almost as fast as it had reached its peak during the beginning of 2018, before stabilizing a little bit and continue in a modest decrease. Today, May 17th 2019, the value for one Bitcoin is approximately $7 200. Bitcoin's price development seem to closely correlate with the hype around blockchain, and web searches for "Blockchain" today is around 28% of the amount they were at the height of the peak (Google, 2019).

Before, during and after the blockchain and Bitcoin hype, there have been many examples of projects that try to use blockchain for other applications than for a cryptocurrency. Examples include IBM and Maersk's joint venture TradeLens from 2018, a shipping digitization project to improve visibility and decrease costs, and the company Everledger's Ecosystems of trust, a transparent platform in the diamond industry to increase trust in the value chain. According to Chang, Iakovou, and Shi (2019), the application of blockchain in supply chain related projects are expected to have a compounded annual growth rate of 87% from 2018 to 2023. Blockchain will there provide better traceability, automate processes and secure chain-of-custody, among other things. Given these and other blockchain capabilities, hope exists that blockchain can be an efficient tool in the fight against counterfeiters. Several question marks does however still exist. Is it possible to implement a blockchain solution in the network of actors that constitutes a supply chain? What potential

benefits exists and do they outweigh the costs of the implementation itself? What challenges exists when trying to implement blockchain in such a network? This study therefore intended to explore the area of blockchain application in supply chain, to better understand its suitability.

1.4 Background

The initiative to this master thesis was taken by SKF AB, from here on only SKF. Today, SKF is a global company that manufactures bearings to be used in all different kinds of machines that covers most industries in the world, where mechanical tools and machines are required for operating (SKF, 2019). Currently, the company is present in approximately 130 countries and have about 45 000 employees worldwide. They have production factories in 24 countries around the world, and have around 400 000 active SKUs in their assortment. SKF's bearings are renown for their superior quality, which is why their customers trust them to be the supplier of bearings to machines which operate in the most exposed and extreme conditions. It also enables SKF to charge a premium price for their products as compared to their competitors.

In many parts of the world, SKF have a problem with counterfeiting as other manufacturers produce bearings and then brand them as genuine SKF products. These counterfeits do not have the same quality as the SKF products, but can for an untrained eye look very similar. This leads to that some customers purchase fake products which can potentially lead to severe consequences. To counter the counterfeiters, SKF have a department called Group Brand Protection (GBP) that solely work with activities to counteract fraudulent bearings and the people creating and selling them. They are responsible for managing and protecting SKF's trademarks. The group's objective is to ensure that SKF's customers receive genuine products and are not cheated by counterfeiters, something that could lead to severe implications. They mainly want to achieve that by increasing awareness in the market, but also by making it more costly to produce and sell fake products, thus minimizing the amount of fake products being sold. Today, some of the progress is measured in estimations of sales recovery, i.e. increase in sales due to brand protection activities, which is a clear indicator for the effect of their work. The unit consists of 13 people worldwide, of which most are based in Gothenburg. Compared to other similar companies, this is a relatively large department to tackle issues of counterfeiting and trademark infringements. They also have a different approach than many, where they try to win back business rather the punish the counterfeiters.

When GBP started their operations in 2009, it was easier to verify that a product was fake based on a few parameters. In later years, counterfeiters have however become better at copying the genuine products, making it harder for the group to determine if they are fake or not. Given this development, GBP are constantly trying to find new ways to make verification easier and more secure, and to make copying

harder. They have heard about blockchain projects from contacts in the market, and therefore wanted to investigate the possibility to use blockchain for product authentication and secure traceability in their supply chain. If this thesis would present potential to use blockchain in the authentication of products in supply chain networks, SKF might pursuit investing in the technology in order to establish a more reliable distribution and recover sales that were previously held by counterfeiters. A full description of SKF's supply chain together with a deeper description of the counterfeiting problem and GBP's operations is found in section *4.3 SKF - A Case Study.*

1.5 Purpose

The purpose of this study is to examine the applicability of blockchain technology in industrial supply chains to assess its suitability to prevent counterfeiting of physical products.

1.6 Research Questions

To serve the purpose of the study, the following general research question and corresponding sub-questions have been formulated:

Is blockchain technology suitable to use in an extensive industrial supply chain in order to prevent counterfeiting of physical products?

(a) What is blockchain technology and what are the applications used today?

(b) Can a physical product and the digital blockchain be irrevocably linked together?

(c) What can be the main benefits of applying blockchain technology in a supply chain?

(d) What can be the main challenges of applying blockchain technology in a supply chain?

(e) What processes in a supply chain are suitable for blockchain application?

(f) How could the adoption of blockchain technology develop in the future?

1.7 Delimitations

The study will exclusively research blockchain's possible applicability for tracing physical products, hence intangible services will not be examined further. Regarding the different classifications of counterfeit products, the study will solely focus on *true counterfeit products*, i.e. products that are very similar to the original and use the same brand name. Furthermore, no alternative methods other than the use of blockchain to avoid counterfeiting will be investigated during the study, however some will be presented to describe the current situation. The costs associated with further investigations and implementation of blockchain will not be examined in detail. In the case study on SKF, only the downstream supply chain from SKF to end customers will be considered.

2

Method

This chapter aims to thoroughly describe the method used to conduct this study to give the reader a deep understanding of how the authors proceeded to find answers to the existing research questions previously presented.

2.1 Research Strategy and Design

Bryman and Bell (2015) distinguish between two different research strategies that a study can employ. These are quantitative and qualitative research, and differs in the way they aspire to conduct research. While the first distinction on these two is made on the collection and analysis of data, where the quantitative approach emphasize quantification and the qualitative emphasize words, there is more separating the approaches. On a general level, qualitative research is often associated with the development of new theories, rather than testing existing theories which is more associated with the quantitative approach. For the purpose of this study, extensive theory does not exist on blockchain application in supply chains to prevent counterfeiting, making a quantitative study hard to conduct. To address this problem, the study took an exploratory stance, making the qualitative strategy with interviews and descriptive data most suitable.

There are three main perspectives of looking at the role of theory in research (Bryman and Bell, 2015). These different views are deductive, inductive and abductive, and they lead to different processes of working in a research project. In the deductive approach, the researcher starts with theory and the knowledge of a specific domain, to form a hypothesis that puts the theory to the test and is either confirmed or rejected. However, in the inductive approach, the result of the research is theory. Based on observations and findings, inductive research often aim to draw general conclusions that builds new theory. Deduction is often associated with quantitative research, whereas induction is associated with qualitative research. A more pragmatic view is the abductive approach, which can be seen as a combination of the previous ones. Abduction begins with a puzzling phenomenon that cannot be fully explained by existing theory. Through back-and-forth iteration between the

social observations and literature, abductive reasoning seeks to find the conditions for which the phenomenon can be explained. This approach was applied in the study, as the capability of blockchain application to prevent counterfeiting could be seen as a puzzling phenomenon. It was necessary to iterate between literature and collection and analysis of data (Figure 2.1), as neither could help to explain the research questions solely.

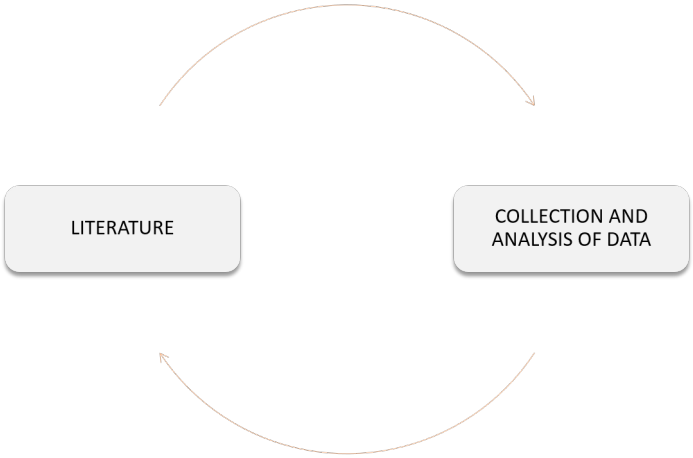

Figure 2.1: *Abductive research with iteration between literature and data*

When conducting a research study, it is important to decide how to collect and analyze data. According to Bryman and Bell (2015), this procedure is called research design and there exists five different types: experimental, cross-sectional, longitudinal, case study and comparative. Case study was deemed most appropriate since it entails the detailed and intensive analysis of a single case. Comparisons with other blockchain projects were also made to get a better understanding of the blockchain technology and its application areas. A further motivation for using a case study is explained below.

2.1.1 Case Study

It is important for empirical research to have a strong foundation in related literature, in order to identify a gap in the existing literature that the study intends to fill (Eisenhardt and Graebner, 2007). However, if the proposed research strategy is to use cases to build theory that could help to answer the existing research questions, such an approach must be well motivated. For the purpose of this study, it was important to get a good understanding of a global supply chain to evaluate what processes are ready for blockchain implementation along with difficulties in doing so. Given that SKF has such an extensive supply chain, and that their products are being counterfeit, they seemed suitable for a case study.

Building theory from case studies is an approach that means to use one or several

cases describing a certain phenomenon in order to create theoretical constructs or propositions based on empirical evidence (Eisenhardt and Graebner, 2007). A case study was deemed appropriate as a part of the study to use as a comparison with other cases and theory in order to draw conclusions about blockchain's suitability in supply chains. To be able to build new theory about the phenomenon, the sampling of studies should not be random like many may argue (Eisenhardt and Graebner, 2007). Instead, SKF was chosen specifically because it present a case that offer insight to the studied context.

The data from case studies can be rich in variety, ranging from interviews and observations to archival and survey data (Eisenhardt and Graebner, 2007). Interviews are especially good to gather rich data, but at the same time present a risk of bias among the respondents (Eisenhardt and Graebner, 2007). Aside from interviews with employees, work on the project was mainly conducted on SKF premises. This allowed the authors to observe how GBP conducted the daily work and better understand the context of counterfeiting in the SKF supply chain, as well as an understanding of the supply chain itself. Observational notes were here made if relevant to the case, to be used as data in the study. The case is presented in full under *4.3 SKF - A Case Study*.

2.2 Data Collection

The data collection was constituted by two different methods, namely conducting interviews and by the search and compilation of secondary data. The data was gathered as a basis for analysis that intended to bring clarity to the purpose of the study.

2.2.1 Interviews

The interviews held during the course of the study were conducted in a semi-structured way, as this format was deemed most suitable to collect rich, qualitative data. A semi-structured interview is a flexible process where researchers start with a quite specific set of areas to be covered but allow for wide variations in the respondent's answers (Bryman and Bell, 2015). Questions are prepared beforehand but might not be asked in the predetermined order, and deviations due to follow-up questions are allowed. Some main things that are important to consider when preparing a semi-structured interview guide are to create a certain level of order on the question topics, formulate questions so that they help to answer the research question(s) of the study and to not ask leading questions. This is the structure that was followed during the interviews. Before interviews, interview guides were prepared, containing questions that were developed based on the impression of what the person could give insight to and contribute with. Since it was not always possi-

ble to determine this beforehand, the interviews had to be semi-structured to allow for collecting deviating answers that were richer than anticipated, or gave insights in different areas than expected.

When sampling informants, there are many different methods to employ. In qualitative research, snowball sampling is the most used method and occurs when the informants provide the researchers with contact information to other informants (Noy, 2008). The process is as follows: the informant refers to other informants, who are then contacted by the researchers and then in turn refer to additional informants et cetera. For this study, a few persons with great knowledge about blockchain was contacted who then further referred to other people with knowledge about the technology within their networks. According to Noy (2008), this is an effective tool to gather information and knowledge about areas where the experts are hard to distinguish from an outside perspective. If the contacted persons had possibility to participate with their knowledge, an interview was scheduled.

During the study, several interviews were held and the participants were separated into three different categories and are presented in Table 2.1 below. These categories consist of (1) blockchain technology experts, that gave insight to the technology's capabilities and limitations, (2) SKF employees, that helped to build an understanding of the case of SKF's supply chain and (3) employees at other companies trying out blockchain in their supply chain. Six blockchain experts were interviewed and some questions about blockchain were only asked to them in the beginning of the study, to give the authors a clarifying understanding of the technology due to its complex nature. A total of five interviews were held to study the case of SKF and build an understanding of their supply chain and anti-counterfeit operations. Mainly, employees were interviewed based on their role in the company. To mitigate the risk of bias, however, some questions were asked to several respondents to present different perspectives. An interview was also carried out with an industry expert to gain knowledge about a specific blockchain project. Overall, interviews were conducted until the data started to converge into similar types of answer, and additional interviews did not add much extra value. The data was later codified and is presented under *4.1 Expert Interview Data*.

Name	Company	Position	Date
Blockchain Experts:			
Oliver Oram	Chainvine	CEO	2019-02-25
Ludvig Öberg	Genesis Block Consultancy	Founder	2019-02-26
Frida Höjvall	RISE	Project Leader	2019-02-27
Peter Altmann	RISE	PhD. Senior Researcher	2019-03-11
Mats Snäll	Lantmäteriet	Chief Innovation Officer	2019-03-14
Sukesh Kumar Tedla	Swedish Blockchain Association	Chairman	2019-03-26
SKF Employees:			
Johan Bravert Petter Rönnborg	SKF	Director GBP & Brand Protection Manager	2019-02-07
Ulf J Andersson	SKF	L&DC Planning Sales & Operations	2019-03-14
Hans Sjöström	SKF	P&ICR Automotive & Aerospace & Global	2019-03-25
Ulrica Nilsson	SKF	Brand Protection Manager	2019-04-15
Ketil Eliassen	SKF	Brand Protection Manager	2019-04-16
Industry Experts:			
Hans Svensson	Stena Steel	Vice CEO & Market Director	2019-04-10

Table 2.1: *Interview objects*

2.2.2 Secondary Data

The need for secondary data from other blockchain project was motivated by the fact that blockchain is a relatively new field of technology where there is a lack of theory on its application in supply chains. Since there are many examples of companies using blockchain in some sort of supply chain, the projects presented in *4.2 Examples of Blockchain Projects* were specifically chosen because they presented a different set of application areas for blockchain. To find these projects, the authors used several databases, such as Google, Google Scholar and Chalmers' library's digital platform, together with asking blockchain experts for examples during the interviews.

2.3 Data Analysis

The data gathered consisted as previously mentioned of expert interviews on the topic of blockchain, secondary data on other use cases for blockchain application and case study interviews with SKF representatives. The thorough analysis of this data together with theory was then the foundation for answering the study's research questions.

The first step of the data analysis was thus to collect the data. Even if collecting data per se is not analysis, it gradually builds up an understanding of the studied subject. Second, to get a better overview of what the interviews had covered up to that point, the data from the expert interviews was mapped against the research questions. This activity was done together by the authors in an unstructured way, meaning that both read through each interview and mapped data under the research question it was most relevant to answer against. The activity was valuable to make sure that both authors got a deep understanding of the existing data, but also enabled an understanding of how well the accumulated data answered the research questions and what gaps still existed. The third step of analysis was to codify data in a more detailed manner. Domains were identified under each research question and then built out with data and examples of expert quotes, to show similarities and differences between the answers of the experts. Fourth, the data from interviews with SKF employees were used to map up the existing SKF supply chain and how GBP conduct their work. The blockchain projects were used to compare similarities with the supply chain at SKF as well as identify general challenges with blockchain implementation. By connecting the codified data with the understanding of SKF's supply chain, examples of other blockchain projects and theory, insights were either gained and discussed under *5 Analysis and Discussion*, or gaps were identified. If gaps could not be filled by generating new constructs from the existing data, new interviews were needed that addressed the identified the gaps. The data from the second round of interviews was then directly codified into the already developed constructs since there was no need to map it against a specific research question. This iterative analysis processes is presented in Figure 2.2 below.

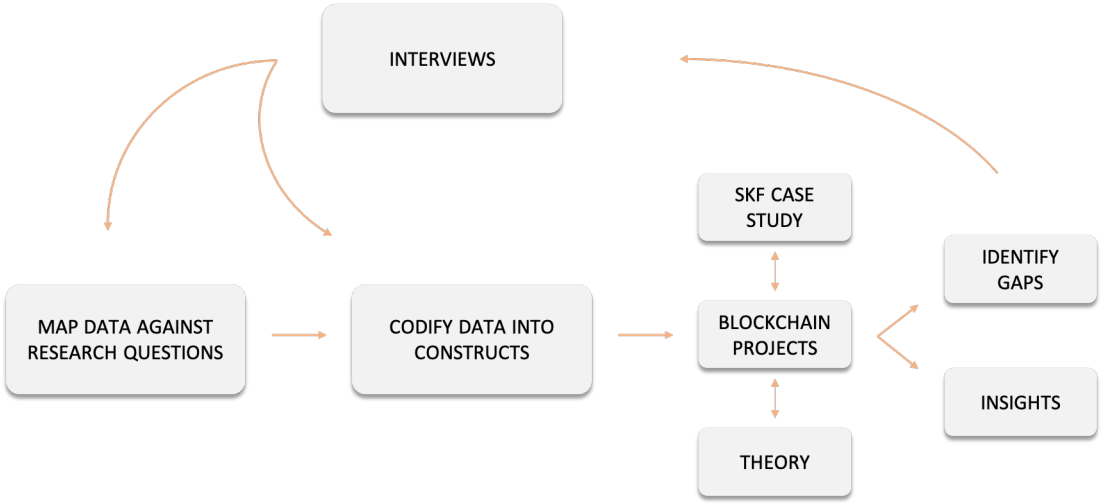

Figure 2.2: *The analytical framework*

2.4 Research Quality

This section presents how the authors ensured a good thesis quality as well as some ethical considerations that were taken into account.

2.4.1 Reliability and Validity

There are three main criteria for assessing the quality of a research; reliability, replication and validity (Bryman and Bell, 2015). Reliability is concerned with the quality of measures, if knowledge is gathered in a consistent and trustworthy way. This is important to enable the result of a research to be repeated but with other objects. The research must also be capable of replication to determine the reliability of a measure. Bryman and Bell (2015) divide reliability into internal and external reliability. The former entails whether or not the researchers agree about what they are observing, while the latter is the degree to which the research can be replicated. For qualitative research, external reliability is difficult to meet since a social setting is easily changed, making it hard to replicate the initial research. This study has tried to maintain reliability and trustworthiness by being transparent about the different interview objects, how they were contacted and what questions were asked during these meetings. The authors have also described in detail how the study was conducted to enable replication and reliability.

Validity is seen as the most essential criterion of research and can in general be defined as the relevance of the collected data, i. e. if the researchers are observing or measuring what they are supposed to (Bryman and Bell, 2015). A valid measure needs to be reliable and measure what it is intended to measure. Similar to reliability,

validity is also divided into internal and external validity. Here, internal validity entails how well the observations match the theoretical ideas, while external validity involves the findings ability to be generalized. To obtain high validity throughout the study, the authors have used triangulation, which according to Bryman and Bell (2015) involves using more than one method to collect data on the same topic. As mentioned above, the data concerning blockchain technology was collected through interviews, a case study and secondary data. Regarding high quality of theory, the literature mostly consists of academic research papers and books, but also extend to announcements made by legit actors in the blockchain community and educationally written articles from online forums. The latter sources were only used on a few occasions, and were then critically evaluated before used as they are not to the same extent reviewed before published. This was done by confirming the information with other, more formal sources, but the sources were still kept as they provided a simpler way of explaining the theory in those cases.

2.4.2 Ethics

Bryman and Bell (2015) present ethical considerations that needs to be taken into account when conducting a research: data management, copyright, reciprocity and trust along with affiliation and conflicts of interest. During this study, these consideration have been managed by informing interviewees about the purpose of the study and how the information given by them would be used. The authors have also asked for the interviewees permission to use that information in this report. Furthermore, contracts with SKF was signed to clarify conditions about sensitive information. A final version of this report was presented to SKF before publishing to ensure their consent.

3

Theoretical framework

An important part when exploring a new topic is to create a theoretical framework of literature in relevant domains. The first purpose of this activity was to bring an understanding of the individual building blocks of theory that were relevant to comprehend the setting of the study. Another purpose was to iterate between collected data and theory, to see if what was observed and analyzed could find support in existing theory. A third purpose was to use theory to find or develop frameworks that helped to better analyze collected data.

3.1 Introduction to the Theoretical Framework

In order to give an answer to the general research question, i.e. if blockchain is suitable to use in a supply chain to prevent counterfeiting of physical products, several theoretical areas need to be addressed. These areas are: blockchain technology, tags that can create unique identities, global supply chains, digitalization of supply chains and chain of custody. A section explaining the blockchain technology, and its different components, is needed to give the reader a brief understanding of what blockchain actually is. This is then followed by a section presenting a few different techniques to uniquely tag a product, to show which methods are used today. To further investigate whether blockchain is suitable to use in a supply chain of physical products, global supply chains are addressed to demonstrate how the different actors in a supply chain are connected to each other, as well as problems and risks associated with them. This is then naturally followed by a section explaining how digitalization has changed supply chains along with demands, benefits and risks of digital supply chains, to give the reader an understanding of what blockchains role can be in a supply chain. Finally, four chain of custody models describing how the ownership of a product changes within a supply chain are presented to show how traceability is done today. How these theoretical areas relate to each other is visualized in Figure 3.1 below.

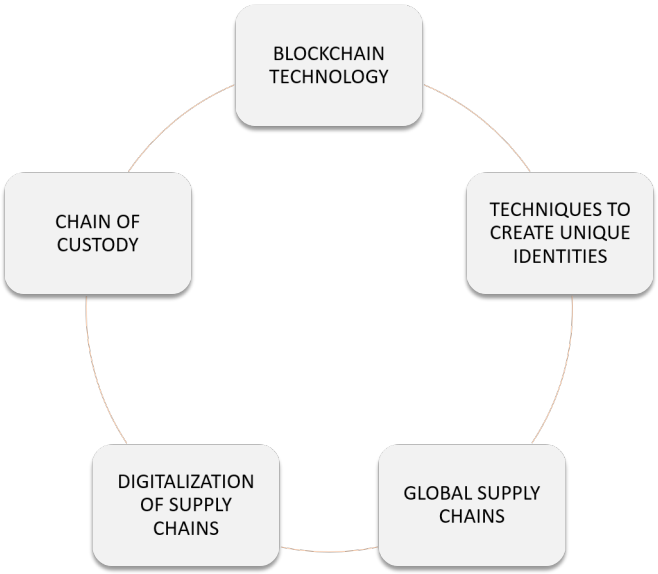

Figure 3.1: *A conceptual model of the theoretical framework*

3.2 Blockchain Technology

Blockchain can briefly be described as a decentralized and distributed database system for transactions of different types of assets, including currency, material and immaterial property (Swan, 2015; Appelbaum and Smith, 2018). Swan (2015) describes blockchain as a big spreadsheet containing all assets in a global network that can be seen by all participants in the network. Originally, blockchain was created to enable safe transactions between two parties without the need for a third party or the element of trust, as it enables transactions directly between two parties and is visible to and verified by the whole network (Nakamoto, 2008). This lead to the creation of the cryptocurrency Bitcoin, which is the first application of blockchain. In Bitcoin, the blockchain is the public record of all Bitcoin transactions that have ever occurred and the technology builds up a safe payment system (Swan, 2015).

Given that the intention of this section is to provide the reader with an overview of blockchain that enables an understanding of the thesis, blockchain is not presented in full depth. Therefore, the authors do not claim that this is a complete description of what blockchain is, but sufficient enough for the purpose of reading this thesis.

3.2.1 Describing Blockchain as Applied in Bitcoin

Explaining blockchain in a straight line from start to finish is not simple. There are several different parts that together constitutes blockchain and are circularly dependent on each other. To understand blockchain is a matter of understanding

the individual parts and then connecting them together. Therefore, it could be suitable to explain these parts individually at first, to establish the domain in which blockchain exists. The parts considered here are the network of nodes, transactions and how they are conducted, blocks of transactions and how they are linked together in a chain, the consensus algorithm and the incentives that exist in a decentralized system like Bitcoin.

Since Bitcoin is the first application of blockchain, and currency is an intuitive way to understand transactions, explaining blockchain through its application in Bitcoin seems suitable. The cryptocurrency Bitcoin was created by the person or the group of persons called Satoshi Nakamoto and was released on the 9th of January 2009 (Nakamoto, 2009). Before Bitcoin was released, Nakamoto wrote a paper called *"Bitcoin: A Peer-to-Peer Electronic Cash System"* which explained the problems with existing electronic payment systems and proposed a solution that removed the need for a trusted third party and solved the problem of double-spending (Nakamoto, 2008). Nakamoto further argues that in most transactions over the Internet, financial institutions such as banks are needed as a third party to process electronic payments and make these payments trusted by consumers and make the system work. As electronic payments are not visible and tangible, banks are needed to legitimate transactions. At the same time, they incur transaction costs and make transactions less efficient and flexible. By creating a technology that uses computers in a network to keep track of a timestamp server that is distributed peer-to-peer and requires proof to be computed, Nakamoto built an electronic payment system that removed the third party and still kept the transactions safe and currency impossible to double-spend.

3.2.1.1 Network

The world of Bitcoin is built up by a network of nodes, where the nodes constitute every computer that is connected to the Bitcoin network (D'Aliessi, 2016). These nodes are interconnected to each other (Nakamoto, 2008). The interconnection between nodes and how a transaction is spread in the network is illustrated in Figure 3.2. Every node in the network has a copy of the public record, a so called ledger, of every transaction of Bitcoin that has ever been recorded (D'Aliessi, 2016). Thus, the system is distributed, meaning that the ledger is not stored in a central location, but separately within each node, so that no one has full authority. How to make sure that all nodes share the same ledger, and thus transactions history, is described in the following sections.

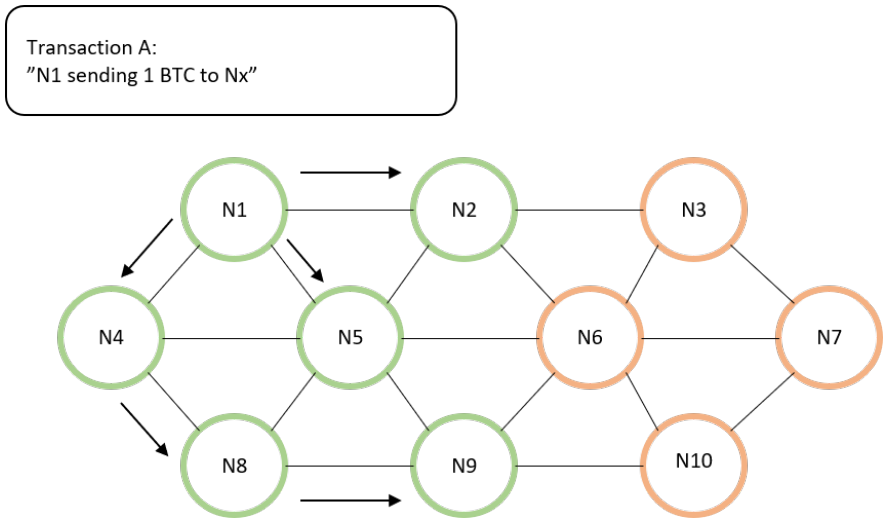

Figure 3.2: *The Bitcoin network and the transmission of a transaction*

3.2.1.2 Transactions

With digital currencies, how can it be made sure that each unit of that currency is only spent once by the owner that holds it? Since a digital currency is not a material product that can be at only one location at any given time, this can be more difficult than it seems. As described above, this problem has often been solved by having a third party, like a bank, verifying transactions by checking them for double-spending (Nakamoto, 2008). In such a system, privacy could be kept in between the sender, recipient and the third party, and these would be the only ones to know about the transaction. In Bitcoin however, to avoid the problem of double-spending everyone needs to know about the full transaction history to know that money being sent has not been spent before. Therefore, all transactions must be announced to the whole system and nodes in the system must agree on a single history of transactions. Otherwise, an owner would be able to digitally verify the same unit of currency multiple times and send it to several different recipients. If everyone knows about the transactions that has happened in the system, such double transactions will not be accepted. A node can therefore only create outgoing transactions by referring to previously incoming transactions to its address, which implies that the network is self-referring (Bitcoin.org, 2019).

But why would anyone accept that their monetary transactions are publicly known in a global network? The solution to that problem in blockchain is that every node in the network has an address, to which transactions are directed (Nakamoto, 2008). The identity of the owner of the address is not stored anywhere, and is therefore anonymous. The network can thus see that transactions are directed to a certain address, but do not know who the person receiving the money is.

So when transactions are anonymous, how can one be sure that the money sent in a transaction are coming from the address it says it is coming from? To solve this

problem, Bitcoin use public-private key cryptography which means that every node has a pair of a private key and a public key (Massessi, 2018). The private key is a string of random data and the public key is then generated from that private key (Bitcoin.org, 2019). The public key is then cryptographically hashed, which means that it is shortened and altered so that it cannot be re-engineered back to the original public and private key. A hash function is a function that converts data of any size into data of fixed size and is cryptographically secure (Konstantopoulos, 2017). This makes manual transactions easier and provides security against unexpected problems. The hashed public key could then be seen as a Bitcoin address to where transactions are to be sent (Bitcoin.org, 2019).

Briefly explained, the private key is used to sign transactions and broadcast messages, while the public key is then used by others to verify that the message or transaction was sent from that specific private key (Massessi, 2018). For example, as shown in Figure 3.3 below, actor A uses its private key to digitally sign and encrypt a transaction message for 5 Bitcoins (BTC) to actor B, and then broadcasts it to the network. Nodes receiving the transaction message then use the public key of actor A to verify that it was indeed actor A that broadcasted the transaction in the network, thus verifying that it is legit. This is possible because the digital signature generated when encrypting a transaction with the private key is a string of text depending on the transaction request together with the private key (D'Aliessi, 2016). Hence, if the transaction request is changed, the digital signature will change, making it difficult for someone else to alter it. Thus, the public key is the only thing that can decrypt an encrypted message from the corresponding private key and vice versa (Massessi, 2018).

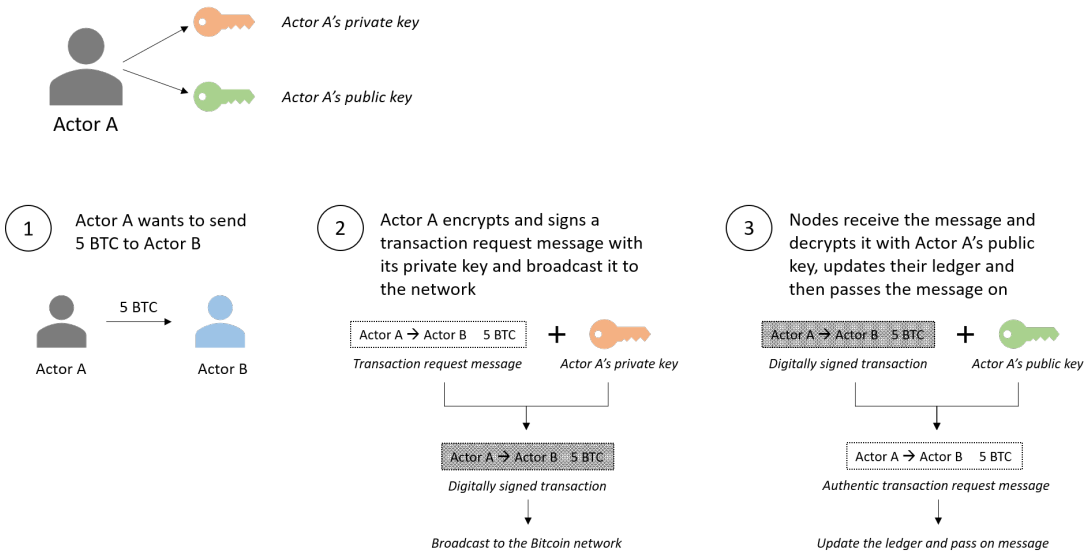

Figure 3.3: *The functionality of private and public key cryptography*

The private key is kept secret to prevent others from using it but the hashed public key can be distributed to the network without any problems since it merely is a Bitcoin address as well as a verifying tool (Massessi, 2018). The keys are simply used to sign and verify all transactions made in the blockchain network. Since the public key is anonymous, a new key pair could be used for every new transaction to prevent them from being linked to a common owner (Nakamoto, 2008).

3.2.1.3 Blocks

In order to verify that transactions are valid and not previously spent, they must be placed in a chronological order after each other (Nakamoto, 2008). Therefore, transactions must be collected in blocks where the hash of a block must be timestamped and transmitted widely in the network. Since each timestamp includes a link to the timestamp of the previous block, the blocks get ordered after each other in a chain of blocks: a blockchain. This is visualized in Figure 3.4 below. As transactions within the same block are considered to have occurred at the same time, it is possible to say what transactions occurred first as new blocks are added to the chain and therefore make sure that Bitcoins are not being double-spent. From the moment a new block is created and accepted, nodes collect all new transactions that reach them into a new, private block of transactions (Nakamoto, 2008). While doing so, they work on solving a mathematical problem called proof-of-work, which is explained below.

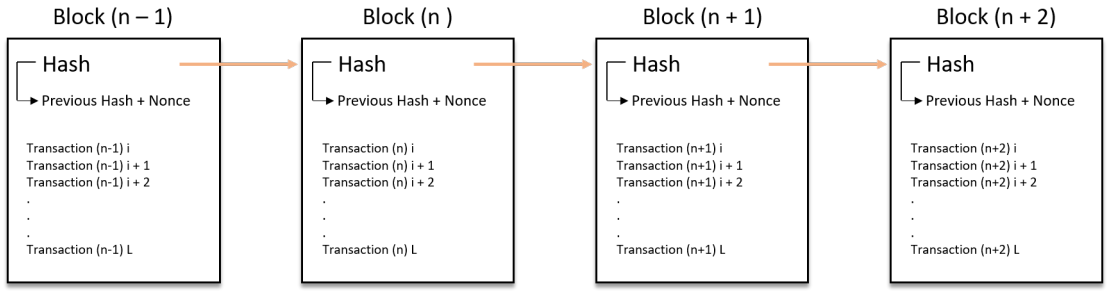

Figure 3.4: *An illustration of a blockchain and how blocks are linked together*

3.2.1.4 Proof-of-Work

Consensus about which block is added next in the blockchain is needed to agree on the single, valid transaction history in the blockchain. The algorithm used to do so is a mathematical problem or puzzle, that needs to be solved before a new block can be added to the chain, called proof-of-work (Crosby, Pattanayak, Verma, and Kalyanaraman, 2016). The name refers to that the node creating the new block needs to prove that it has used enough CPU power to solve the mathematical problem for that specific block. Solving the mathematical problem involves adding a random number, called a nonce, to a given data so that the hash outcome is less than a predefined number (Martinez, 2018). Reversing the hash function is

impossible, which means that trying all different combinations is the sole way to solve the problem (Konstantopoulos, 2017). The more computing power that a node put in to solve the problem, the faster it will solve it.

Once a node finds the proof-of-work, i.e. discover the correct nonce, it earns the right to broadcast the block it has been working on, its private block, to the whole network (Nakamoto, 2008). Other nodes then verifies the validity of that specific block by controlling that the hash outcome is less than the predefined number (Konstantopoulos, 2017). Certain nodes, so called full-nodes, also verify that the transactions in the block are valid and that those Bitcoins have not been spent in earlier transactions (Nakamoto, 2008). If two nodes solve the proof-of-work at the same time and broadcast their private block to the network, both blocks could be accepted and connected to the blockchain and create a so called fork (Bitcoin.org, 2019). Some nodes receive one of the blocks and some nodes receive the other. To show that they have accepted the new block, nodes start to work on adding the next block after the one just created. The consensus model in Bitcoin implies that the longest chain of blocks is the single valid history of transactions, because most work has gone into that chain (Nakamoto, 2008). So the first side of the fork that adds an additional block will be considered the correct one. Thus, the network has agreed on a single, valid history of transactions.

Due to the large amount of work to be done before proposing a new block, there is little risk of a block containing fraudulent transactions since this block will be rejected by the other nodes and thus become very costly for the node proposing the block (Singhal, Dhameja, and Sekhar Panda, 2018). For an average computer, solving the proof-of-work could take approximately one year (D'Aliessi, 2016). Given the large number of computers (or nodes) in the network, the average time to add a new block to the blockchain is ten minutes. Since changing a transaction in a previous block requires the need to redo all proof-of-work for all subsequent blocks, each additional block reinforces the ones that came before it (Bitcoin.org, 2019).

3.2.1.5 Incentives in a Decentralized System

The risk for fraudulent transactions and adding blocks containing them, logically decreases with the proof-of-work algorithm. But why would any node want to try to solve the mathematical problem if it costs a lot of electricity and CPU power? There are two main monetary reasons for that in the Bitcoin network. The first reason is that whoever solves the problem and gets to add the new block to the blockchain also gets to create a special transaction in the block that sends Bitcoin to their own address (Nakamoto, 2008). This will however not continue forever; the number of coins are predetermined and eventually all Bitcoins will be distributed in the network. The second reason is that transaction fees can be added to transactions broadcasted to the network, and these will belong to the creator of the new block. Once all Bitcoins have been distributed, the incentives could potentially transition to only be constituted by the fees added to transactions (Nakamoto, 2008).

There is another major reason to play by the rules in the Bitcoin network. If an attacker would try to cheat the system and double-spend coins or try to overtake the system, the outcome would simply be that the system was undermined and not trusted. This leads to that the wealth of the attacker would lose its validity and value (Nakamoto, 2008).

With this said, not all nodes see the need to try to solve the proof-of-work and add new blocks to the blockchain. Some just participate in the network to send and receive Bitcoins, using it as a payment system that is safe, trusted and flexible without having a central third party. The activity of running a software to try to solve the mathematical problem is called mining (D'Aliessi, 2016). Like gold miners invest their resources to mine gold, Bitcoin miners invest CPU power and electricity (Nakamoto, 2008). Since there are so many nodes in the network, and each individual node would take a long time to find the correct solution to the proof-of-work, nodes that conduct mining often arrange themselves in groups and split up the task between each other to speed up the process (D'Aliessi, 2016). When they find the solution, they split the rewards between themselves.

3.2.2 Private and Public Blockchains

Since this field of study is relatively new, several definitions of blockchain exist and the community has not yet reached consensus on a definition of the technology. Potentially, one could make a distinction between two types of blockchains; permissionless and permissioned (Bussmann, 2017). For example Peck (2017) argues that a permissionless, also known as public, blockchain is open for anyone to enter and anyone who does is anonymous. Bitcoin is an example of a public blockchain were anyone could join and there is no central actor that is in charge of the network. Peck (2017) further argues that a permissioned blockchain instead contains actors with known identities, and only selected actors can view the data on the blockchain. In a permissioned blockchain, an actor needs to be approved by the authority or authorities owning it (Peck, 2017). Cachin and Vukoli (2017) have a similar definition, but add that a permissioned blockchain is operated by a group of entities that create a blockchain for a certain context. Cachin and Vukoli (2017) further argue for a third type of blockchain called private, which is a special permissioned blockchain that is operated by one single entity.

A permissioned blockchain is suitable when all actors in the network already have a small degree of trust among them and would like to replace the services of a neutral third party (Peck, 2017). The consensus problem regarding what block is added to the chain is, as previously mentioned, often solved by proof-of-work in a public blockchain, but in a permissioned one it is a bit different. Since the right to add new blocks is assigned by the owner of the private blockchain, there is no need for proof-of-work. Instead, there are several other ways to reach consensus. One common approach is that the nodes within the network vote for which block should

be added with their digital signature, and the block is then added to the chain when the majority of the nodes have approved it (Cachin and Vukoli, 2017).

3.2.3 Smart Contracts

In order to extend blockchains beyond monetary transactions, the ability to add conditions to a transaction is needed. For this purpose, something called a smart contract is used. These contracts allow for the possibility to exchange anything of value, not just money, without the need for a third party (Blockgeeks, 2018). The concept of smart contracts was introduced in 1994 by Nick Szabo who defines them as "a computerized transaction protocol that executes the terms of a contract" (Christidis and Devetsikiotis, 2016). Smart contracts are automated self-executing contracts that contains specific instructions which gets executed when certain conditions are met (Blockgeeks, 2018). The term self-executing refers to that when one set of instructions are done, the next set of instructions are executed and so on until the end of the contract. Sillaber and Waltl (2017) argue that smart contracts consists of three components: the contractual arrangements between the parties, governance and preconditions along with execution of the contract. The first component means that the involved parties agree on certain conditions which then are transcribed into executable program code that is stored in the blockchain. Each party is identified through their blockchain address. The second component means that all nodes evaluate whether the preconditions defined in the contract is met or not. The last component is the actual execution of the contract. If the preconditions have been met, the contract is executed and the transactions between the involved parties are performed.

All transactions made through the smart contract is recorded and updated by the network, which makes each involved party accountable for their actions. Smart contracts are scripts stored on a blockchain that has a unique address and are triggered when a transaction is sent to that address (Christidis and Devetsikiotis, 2016). A smart contract needs to be deterministic, hence the same input must always produce the same output. Otherwise, when it is executed on every node, it might return different random results which would lead to difficulties in reaching consensus throughout the network. All interactions with a contract occur through signed messages that uses the same private and public key cryptography as explained above (Szabo, 1997).

3.3 Techniques to Create Unique Identities

As counterfeiters become better at making copies of genuine products, it becomes harder for the manufacturers of the original goods to verify whether a product is genuine or not. Therefore, manufacturers try to find new ways of tagging or

labeling their products that are difficult and expensive to copy, but easy to verify and preferably as cheap as possible. Below, a few of the methods existing today are presented.

A very common way to identify different products is to stamp a barcode on the product or its packaging. A barcode is simply a visual representation of data describing the product and can be read by a machine. A QR-code could be said to be a type of barcode. Barcodes are an easy way to identify a product, but can however easily be copied and printed onto fake products. Therefore, it barely offers any protection against counterfeiters.

One method to identify a living organism is by its DNA. Jeffreys, Wilson, and Thein (1985) early showed that it was possible to create "fingerprints" from DNA that was completely specific to a person, or an identical twin, from as little as one drop of blood. It was later shown that this method was suitable to use as a forensic approach to identify suspects (Gill, Jeffreys, and Werrett, 1985). Given these characteristics of DNA-tests, they can be made to identify for example chickens, to ensure that they come from the farm they are claimed to be from. However, most physical products do not have a DNA.

Another way to create a unique identity for an item is by DNA marking it (Selectamark Security Systems, 2019). The marking liquid, or spray, contains a unique DNA combination that is applied to the object and can be registered in a database. Removing the mark is hard, and even if it could be removed, it cannot be reattached to another item (Jung, Hayward, Liang, and Berrada, 2016). According to Jung, Hayward, Liang, and Berrada (2016), DNA marking also have physical properties that cannot be replicated, creating a sufficient level of unique identification to enable authentication and provide a track and trace system for marked items. DNA marking does however not apply to a large amount of identical physical products since it would require a new spray for each item.

Quantum dots are semiconductors in the size of nanoparticles (Murphy, 2002). Excitation of quantum dots create an emission wavelength spectra when hit by a light source, and given their unique optical properties this makes them suitable for applications like anti-fake labeling and security identification (Bai, Du, Zeng, and Yu, 2008). Chen, Lai, Marchewka, Berry, and Tam (2016) present a low-cost method for producing nano-thin films of quantum dots and cellulose nano-crystals that can be used for anti-counterfeiting purposes. Many different colors can be emissioned by adjusting the concentrations of the two building blocks of the film.

Radio Frequency Identification (RFID) is a device with an antenna connected to a microchip that provide identification of different products or goods (Tuyls and Batina, 2006). The information can be accessed through a reader and used for authentication and tracing, possibly for anti-counterfeiting purposes. If the necessary information is there, the product is declared to be genuine. However, the information on the chip can be captured and copied onto a new chip, making it possible to

clone it.

3.4 Global Supply Chains

In the manufacturing sector, the supply chain can be viewed as a network of actors that are interdependent of each other and together physically transform materials, components and substances into finished products (Klötzer and Pflaum, 2017). These actors are together responsible for managing and improving the flow of material from suppliers to the end users. In the global economy, companies operating internationally will have to manage a global supply chain. Due to many different factors, such as different currencies, tariffs and taxation differences, an international supply chain becomes more difficult to manage than those contained within one single country (Vidal and Goetschalckx, 1997). In order to understand the complexities in the supply chain of a global company it is important to first build an understanding of the complexities within a single market. Mattsson (2003) has a markets-as-networks view, describing markets as *"networks of multidimensional, dynamic exchange relationships between economic actors who control resources and carry out activities"*. Markets can be viewed in terms of connectivity, which describes the amount of direct and indirect connections between actors on the market. Here, Mattsson (2003) makes the distinction between positive and negative connections. A positive connection is based on cooperation between e.g. a supplier and a buyer, while a negative connection is based on competition for relationships third parties. To a large extent, processes in the market is endogenously created through the activities of the present actors. At the same time exogenous forces exists on a market to affect its structure and rules to play by, stemming from actors that are not seen as part of the market, such as governments.

Since any firm's supply chain can be seen as embedded in the markets-as-networks view, it is dependent on all the actions made by actors within the network (Mattsson, 2003). In the network view of markets, each actor can be seen to have one position in the market, which is built up by the connections they have in the market and the internal resources they control. But, as relationships between actors constantly changes, interconnection with other markets become less or more prominent. Since actors enter and exit the market, the market is highly dynamic.

There are several problems associated with the global supply chain of a firm. (Mattsson, 2003). Internally the firm must organize to coordinate activities across nations and externally the firm is connected to other actors on the market in cooperative and competitive relationships. Thus, the firm is not only affected by the actions they do themselves, but also by those of other actors in the market network such as competitors etc.

The risks associated with a global supply chain increases since it often have been extended, is more complex and harder to evaluate in terms of impact of potential

disruptions (Manners-Bell, 2014). With extended supply chains, problems like e.g. more hand-offs to other parties, quality control challenges and corruption further down the chain can appear.

3.5 Digitalization of Supply Chains

Under this section, the concept of digitalization is presented, and it is elaborated on how digitalization has changed the operations and management of supply chains in later years. The new set of demands on the Digital Supply Chain is also explained, along with the benefits and risk. Finally, a brief understanding of how blockchain could be applied in this environment is presented.

3.5.1 What Is Digitalization?

The term digitalization is often thought of as the process of making data and processes digital. This is only partly true, which is why it is necessary to define some terms before continuing.

Digitization is the process of converting analog data to digital data, which means to transform it into digital bits (Tilson, Lyytinen, and Sörensen, 2010; Gobble, 2018. This definition is confirmed by Gartner (2019), that describe digitization as "taking an analog process and change it to a digital form without any different-in-kind changes to the process itself".

Digitalization, on the the other hand, is something different. Tilson et al. (2010) describe it as applying digitization in a wider social and institutional context, where the digital technologies become infrastructural. Further, digitalization could be referred to as using digitization and the digital technology to create new ways to generate value. To make a distinction between the two, digitization does not change the underlying business model, while digitalization in the end does (Tilson et al., 2010; Gobble, 2018). A visualization of these two concepts can be viewed in Figure 3.5 below.

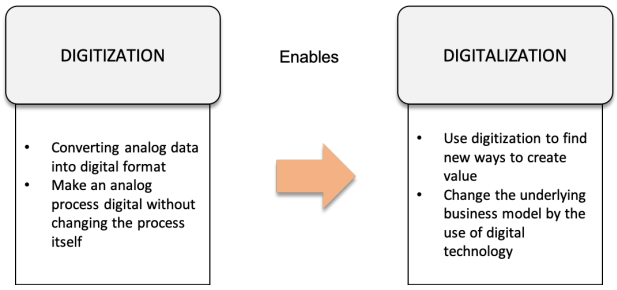

Figure 3.5: *Digitization and Digitalization*

3.5.2 How Digitalization Has Changed Supply Chains

The relatively recent development of digitalization of the economy has affected, and is continuously expected to affect, the development and management of global supply chains (Klötzer and Pflaum, 2017). In this era where companies become more digital, data and information is of critical importance. Gunasekaran and Ngai (2007) define a digital enterprise as *"characterized by the application of Information and Communications Technology (ICTs) [...] for the integration of activities in different functional areas as well as the so-called extended enterprises or partnering firms in the supply chain"*. Given the definition of supply chains, it follows that integration between actors in them require integration of processes and information (Korpela, Hallikas, and Dahlberg, 2017). Digital technology, e.g. Electronic Data Interchange (EDI), has enabled this integration between supply chain partners, to base actions on the same data (Christopher, 2016). This has in later years changed business models in the supply chain to be based on real data instead of forecasts. Christopher (2016) argues that this type of collaboration is becoming more common and is also needed as companies tend to focus more on their core competencies and outsource remaining activities. The term Extended Enterprise can be used to describe these collaborative relationships where buyers and sellers share a vision to create larger end-user value to beat competing supply chains (Spekman and Davis, 2016). In the Extended Enterprise environment, where big companies becomes hubs in their network, collaboration for integration is needed throughout the whole supply chain and not just between two actors (Korpela et al., 2017). While there are several methods to integrate information directly between actors in the supply chain, companies still use third parties like banks for transactions between each other.

The last years' digital development in supply chains have led to the term Supply Chain 4.0, which Alicke, Rachor, and Seyfert (2016) define in the following way:

> Supply Chain 4.0 - the application of the Internet of Things, the use of advanced robotics, and the application of advanced analytics of big data in supply chain management: place sensors in everything, create networks everywhere, automate anything, and analyze everything to significantly improve performance and customer satisfaction.

Customer expectations are growing in the Supply Chain 4.0. The competition between supply chains is driven by transparency and the access to a wide range of product and channel options enabled by online functionality (Alicke et al., 2016). Overall, the Supply Chain 4.0 will thus include features like complete transparency of data, knowing location and conditions of individual shipments, automated feedback on operations from machines, shared capacities in logistics between supply chain partners and flexibility to re-route shipments last minute.

3.5.3 Demands, Benefits and Risks of Digital Supply Chains

The digitalization means that a new set of demands are placed on the supply chain. Gunasekaran and Ngai's (2007) digital enterprises will create a network of both internal and external partners. To succeed in such an environment, a common vision, alignment of goals and trust will be the foundation. Participants must feel confident that the technology system is secured and that privacy is protected. When talking about the Extended Enterprise, things like sharing of risks, rewards, information and technology is essential to succeed with collaboration and joint strategies (Spekman and Davis, 2016). Klötzer and Pflaum (2017) also add to the Extended Enterprise concept that the data and information itself is of critical importance. In this new paradigm of shared information, trust and commitment, joint determination towards strategies and transparency of information is needed in order to succeed (Christopher, 2016). Spekman and Davis (2016) also agree that since open communication and the use of technology to transfer information is critical for collaboration success, trust is essential.

Looking more upon the technical demands on digital supply chains, the new trends and demands in the economy will force them to improve in several ways in order to stay competitive. The Supply Chain 4.0 needs to be *faster*, which requires advanced forecasting approaches based on e.g. internal demand data (Alicke et al., 2016). It needs to be more *flexible* by being dynamic to changes in demand through using real-time planning to a further extent. It also needs to be more *granular* when product customization will continue to become more present, and microsegmentation of customers is needed to achieve this. Further, Supply Chain 4.0 will have to be more *accurate* as its performance management systems will have real-time transparency throughout the supply chain. To achieve this, a huge amount of information from all levels and integrated between actors will provide a shared information base upon which different stakeholders make their decisions on. Finally, Supply Chain 4.0 needs to be more *efficient*. This will be achieved through an increased intensity of automation, both in planning and in operations. Robots will handle material flows by themselves in the warehouse processes, through activities such as receiving and unloading as well as picking, packing and sending goods.

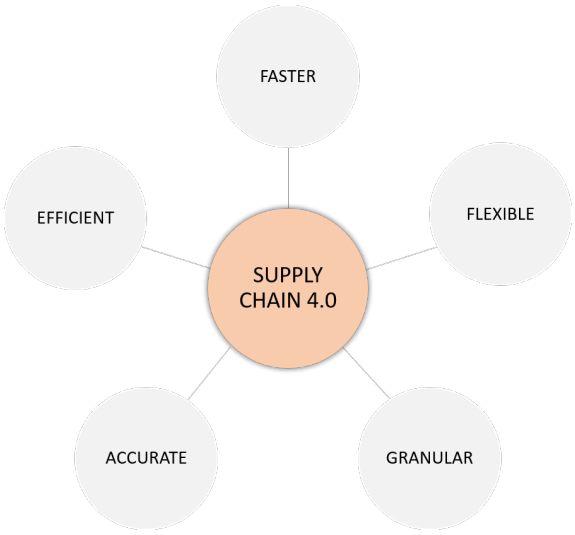

Figure 3.6: *Demands on Supply Chain 4.0*

A few benefits of a digital supply chain are increased efficiency and minimized cost for governing relationships to other actors (Korpela et al., 2017). The digital supply chain also makes information entries more frequent and accurate when it is properly used, minimizing the need for manual entry of data and in extension the amount of errors. Other benefits include reduced lead times and increased flexibility in the supply chain, delivering better value to customers through better services, more accurate prediction of demand and visibility.

Regarding risks, Spekman and Davis (2016) mention six risk areas for the Extended Enterprise, from which a few can be associated with the changes inherent from digitalization. In the Extended Enterprise, there is a security risk regarding a company's internal information systems, both formal IT systems but also informal channels of communication. The risk is not the information itself, but who has access to it. Another risk is related to interdependence with other actors in the supply chain and the relationships built therein. With many relationships and shared information, there is a risk for opportunistic behavior from dishonest partners to for example steal information and act in their best self-interest. Risks need to be managed carefully, because in the end a higher degree of risk will result in lower supply chain performance.

3.5.4 Possible Role for Blockchain in Digital Supply Chains

When using third parties for transactions between actors in a digital supply chain, there are some drawbacks from a collaboration perspective (Korpela et al., 2017). First, full automation of data transfer is only possible for payments, and to a smaller extent also invoices. Second, involving more parties for exchange of documents in the supply chain leads to transaction costs and reduced speed. Third, there is a

risk regarding cybersecurity, that criminals will hack into the system, e.g. a bank's system, to steal sensitive information.

To conduct transactions and exchange documents in a digital supply chain, parties must beforehand agree on how this is to be done (Korpela et al., 2017). A blockchain feature that can achieve this, not only for monetary transactions, is smart contracts described above. With smart contracts, digital supply chain transactions can be automated at a very granular level without the need for a third party. Due to blockchain's capabilities, the technology seems suitable to provide similar services as the integration processes existing, but in a more flexible way with lower transaction costs. Blockchain does not however meet the need for standardization of electronic documents in the supply chain. To ensure full automation in documentation transfer, international standards would have to be relied on, and those would have to be further developed to be compatible for blockchain implementation.

Even though current intermediates, such as EDI, have been practiced in supply chains for over 20 years, they lack functionalities that digital supply chains require for integration (Korpela et al., 2017). The authors mention lack of standardization, timestamping of transactions, overviewing and tracking flows of information as well as secure delivery of information. Blockchain technology have the potential to fill some of these gaps, which is needed to build a digital supply chain that is flexible and cost-effective. This would accelerate the integration between companies in a digital supply chain more than other systems could. However, integration requires standards for interoperability between systems, and that is something that blockchain in itself does not offer more than any other solution does.

3.6 Chain of Custody

Chain of custody refers to the chronological sequence that occurs when ownership or control of an asset is transferred from one actor to another in the supply chain (ISEAL Alliance, 2016). ISEAL Alliance (2016) define four commonly used chain of custody models that describe the systems used to trace the assets in a supply chain: (1) identity preservation, (2) segregation, (3) mass balance and (4) certificate trading. Identity preservation enables certified products, i.e. products that meet a certain standard, to be traced back to the point of origin. Since each batch of certified physical products is treated separately, this model ensures that both the products and corresponding documentation are separated from other sources, making the traceability possible. The second model, segregation, separates certified products from non-certified products, but it is not possible to identify the exact point of origin since certified products from different sources are mixed. Mass balance is slightly different from the two models just described, since it involves balancing volumes in the supply chain. Here, certified and non-certified products can be mixed, but the volume of certified products that enters the operation is equivalent to the volume of products leaving the operation that can be sold as certified. For

example, if 10 kg of certified products enter an operation, only 10 kg of the products leaving the operation can be sold as certified. The volumes regarded in this model can be balanced at batch, site or group level. The final model, certificate trading, is similar to mass balance and used when certified and non-certified products are mixed freely within the supply chain. Certificates are issued in the beginning of the supply chain and can then be bought by actors on the market through a certificate or credit trading platform. This model intends to reward the producers of a product when it is difficult to trace the physical product back to the point of origin in the supply chain. However, there is no guarantee in any of these models that the physical end product is certified just because it has a supplied certificate since the product and the certificate is often sold separately.

4

Empirical Data and Findings

This chapter presents the empirical data that was gathered for this study. The data consists of three different parts, as mentioned in the method chapter. These parts are expert interview data, primary and secondary data from other blockchain application projects and the case study of SKF. First, the expert interview data is divided based on the different research questions and presented individually. Second, the blockchain projects are presented in a descriptive manner, based on data gathered through official sources and interviews. Third and final, the SKF case study is presented, also that in a descriptive manner but here the data was also gathered through on-site observations.

4.1 Expert Interview Data

The expert interview data is presented under six different subsections, where each of the six sections correlates to the underlying research questions, one at a time. Per research question, the data is mapped against the different domains that were found and results for these domains are presented in tables, with exemplifying quotes if possible.

4.1.1 What Is Blockchain and What Are the Applications Used Today?

In Table 4.1.1 below, data that answers against this research question is compiled. A broad description of blockchain is already presented in the theory chapter, so this expert data is presented merely to complement that description and to summarize the main attributes and capabilities. A summary of blockchain *attributes* is that it as a technology is not yet defined. However, most agree that it is a distributed and decentralized technology that is transparent to all actors in the network. The governance in a blockchain network, and the incentives to govern it, exist on the data structure and the protocol itself. Blockchain has the *capability* to automate processes

such as transactions, and reduce the trust needed in a network. Today, it is mainly applied in cryptocurrencies like Bitcoin. Given that blockchain is not defined, the experts acknowledge that the discussion around different types of blockchains exist, even though some are of the opinion that only public blockchains are blockchains at all. In the interviews, three types have been discussed. The are public, public and permissioned and private blockchains, and differ on the level of transparency and authorization that different actors in and around the network have.

4.1.1 What Is Blockchain and What Are the Applications Used Today?

Domain	***Result***	***Exemplifying quotes***
Attributes	• No universal definition of blockchain • Distributed • Decentralized • Immutable without network noticing • Transparent • Secure • Self-referring • Public/private-key cryptography • Governance and incentives are a part of the structure and the protocol of the blockchain • Consensus algorithm to coordinate around (mathematical problem, Proof-of-work) • Data structure is a linked list of blocks, where blocks are a collection of transactions	*"First, the immutability of it. Inability to change data put on the blockchain."* *"Another way is to talk more holistically about it, and this is my opinion, that what is new with blockchains is that the administrative, governance and incentive layers are a part of the protocol. It hasn't been that way before, then you have had an administrator that you have to ask for permission. And then the logic is outside the blockchain"* *"The transparency, auditability and security. All three key parts that makes BC so special."* *"[...] what is the very idea of blockchain solutions that they are distributed, information distributed and preferably on different parties."* *"It is a bit fuzzy about what is a blockchain and what isn't, but some kind of distributed network, a database that manages transactions of some kind, not just financial but it can be data."*
Capabilities	• Automate activities and processes • Reduce the amount of trust needed in a network • Make transactions secure • Enable smart contract implementation • Enable user anonymity • Counteract double spending • Enable traceability • Log information about transactions • Enable auditability	*"The blockchain tries to address the trust, not completely but to a certain level."* *"[...] blockchain won't replace the trust, but reduce the cost of trust and thereby the cost of doing business [...] "*
Applications today	• Cryptocurrencies, mainly Bitcoin and Ethereum • Certificate trading on diamonds, Everledger • As an overlaying layer to a database	*"Blockchain in its true form is completely open, and purists only recognize Bitcoin and Ethereum public."*
Public vs Private	• **Public:** Permissionless blockchains that anyone can join and then view, add and receive transactions. Consensus is reached through e.g. PoW. • **Public and permissioned**: Anyone can see the information, but only certain actors can add information to the blockchain. Identity rules and security can be defined in a more custom way. • **Private:** Some roles from a public blockchain are restricted in a private blockchain. Only authorized parties validate information, and only certain actors can access personal information. Often nodes vote to validate transactions as consensus algorithm, which limits security when actors can collude. Some say that these are not blockchains, but distributed ledgers or databases.	*"People call them private BCs but in my opinion they are just distributed ledgers or Distributed Database. They don't go with the ideology of BCs like transparency or decentralization. They just call it private BC because it's fancy and it makes money."* *"A private blockchain is a nonsense term since the administrative logic ends up outside the chain so what is the point?"* *"Yes but you can [call it a private blockchain]. [...] The main content and capability for this technology is that you can't manipulate the information without it being noticed, without affecting the others. That is the core to me. Then you can have different models. Then I know that there are those who thinks that then it's not a blockchain. It's like a religion, there are different views."* *"I usually say that there are several roles in the network; those that send transactions, those that receive [them], those that can see what happens in the network, those who create blocks and verify these transactions. In Bitcoin, all of these are open. [...] A public blockchain. Private is when you limit some of these [roles], usually it's that you limit who can verify transactions and sometimes also who can send and see transactions. That you limit to a predefined group."*

4.1.2 Can a Physical Product and the Digital Blockchain Be Irrevocably Linked Together?

Regarding this research question, there are two distinct opinions whether or not this is possible to do. Some of the interviewed experts claim that to link the product and the blockchain together, an IoT device, forensic approaches, a QR-code/Barcode or some sort of tag could be used. However, other experts argue that these techniques does not ensure that the physical product matches the digital blockchain since for example QR-codes can be copied onto fake products and tags can be removed. With current technologies, the product requires a unique DNA for it to be impossible to copy. Thus, today the links are often between the digital representation and some sort of abstraction instead of between the product itself and the blockchain. Demands on the link is that it needs to be impossible to copy, durable and have the possibility to create a 1-1 link between the product and the blockchain. It must also be cheap to ensure that the benefit of having the link exceeds the cost of producing it. The data gathered to answer this research question is summarized in Table 4.1.2 below.

4.1.2 Can a Physical Product and the Digital Blockchain Be Irrevocably Linked Together?

Domain	***Result***	***Exemplifying quotes***
Examples on how to tag the physical product to create a unique identity	• IoT device attached to the product with a unique identity on the blockchain • Forensic approach: using DNA or other unique attributes that are impossible to copy, e.g. a diamond cut, to create a unique identity on the blockchain • QR/Bar-code with a digital twin on the blockchain • RFID-tag/Quantum dot with a digital twin on the blockchain	*"Got an IoT device, gave the device a unique identity through blockchain, and the bottle of wine as well. Married the two. [...] What they wanted to do was to demonstrate that the marriage between IoT and physical works. [...] Blockchain backed technology creates a digital identity for the bottle to make sure it was not copied, since the digital identity cannot be duplicated."* *"Look at Everledger [...] securing diamonds. Unique with diamonds is that you can translate a physical diamond to a digital representation. You have certain physical attributes like size, color, transparency, the cut and similar. Through this, a digital certificate is created from the mine, where you as owner of the certificate can prove that you have a diamond that looks like this"*
Difficulties with creating a link between a tag/physical product and a digital blockchain	• If the physical product lack a unique DNA, it can be copied or manipulated in some way • Today it is difficult to create a 1-1 link instead of a 1-abstraction link • QR codes can be copied onto fake products • Tags can be removed or destroyed • A digital representation of a physical product could potentially be used in several transactions	*"The problem is that serial numbers can be copied. So you don't know if the good you get actually match the digital certificate."* *"We don't know how to connect the physical to the digital, it's a major problem"* *"What I mean is that the links we create today is not really between the physical flow and the digital representation, but between some digital representation and some abstraction instead. For example, if it regards ore, we tag the amount of kilos and not the ore itself."* *"Let's say I only need to buy one correct bearing from SKF, then I buy 10 counterfeited bearings from some other firm. Then I give the fake bearings exactly the same QR code as the one I got from the only genuine bearing I bought. So all buyers will see that the bearing has gone the whole way [through the digital flow], but they are not aware of each other."*

4.1.2 Continued: Can a Physical Product and the Digital Blockchain Be Irrevocably Linked Together?

Domain	***Result***	***Exemplifying quotes***
Demands on a tag/link between a physical product and a digital blockchain	• Durable • Cheap • Possibility to create a 1-1 link • Impossible to duplicate/copy • The benefit of having the link and being able to verify the product must be greater than the cost of producing it • The cyber-physical link must (probably) be verified in the end of the supply chain	*"There are techniques that varies from simple tags to very advanced tags. [...] These tags depend on the cost, how durable they are and if they can create that 1-1 relation. No one knows how to do these tags today."* *"If [SKF] cannot tag their products there is nothing they can do."* *"Then you have to sit with an analytical tool in the end to verify, but maybe you do. That you can do with spot-checks, but if you have the possibility to verify that it is exactly the same metal that was put in the bearing in the beginning at the end, then you can work in that way that you have spot-checks or randomly selected."*

4.1.3 What Can Be the Main Benefits of Applying Blockchain in a Supply Chain?

As seen in Table 4.1.3, there are many benefits of using blockchain in a supply chain. A summary of these benefits is that blockchain enhance transparency of all transactions made within the supply chain, which enables traceability and strengthens the trust in the network. Due to the transparency, the information in the blockchain cannot be manipulated without it being seen by the whole network, double-spending is not possible and it makes the system secure. With a blockchain, it also becomes more difficult for counterfeiters to sell fake products.

4.1.3 What Can Be the Main Benefits of Applying Blockchain in a Supply Chain?

Domain	***Result***	***Exemplifying quotes***
Benefits of blockchains in supply chains	• Enhance transparency • Offer secure transactions • Counteract double spending • Enable traceability • Strengthen the trust in the network • Remove the need for a central party • Offer possibility to store unique identities • Make it difficult for counterfeiters • Unable information to be manipulated without network noticing • Serve as evidence of earlier transactions in a dispute • Enable auditability	*"You can't stop people from trying to cheat the system, but you can make it economically unviable to try"* *"The major thing that the blockchain bring is that you can have an overview of each step [in the supply chain] and counteract double spending."* *"What makes the blockchain unique and the capability they have been looking for, there the digital flow is impossible to change without it being visible. Therefore, one can digitize the parts that contain physical elements that can be manipulated and made wrong, and automate to a large extent also and still have confidence that it is correctly done. That is the strength, that you can digitize without risking manipulation and impact."* *"What you used the blockchain for was to save the steps and the signatures [in the workflow], in case someone would break the agreement later. At this time, this person undertook to pay but hasn't done it. You could have that as evidence. You know then that the certification cannot be manipulated, because the blockchain technology prevents it."* *"Even if you cannot tell if the physical product is authentic, you can tell if the digital certificate is. So that means that you can only counterfeit as many products as there are digital certificates, which limits the possibility to sell counterfeits and makes it more expensive for the cheaters."*

4.1.4 What Can Be the Main Challenges of Applying Blockchain in a Supply Chain?

The challenges connected to using blockchain in a supply chain is presented in two domains: in general for all blockchains and in private blockchains. The data gathered is compiled in Table 4.1.4.

One major challenge that applies to all blockchains is the point of entry for the information. Since the blockchain itself cannot communicate if the information in it is correct or not, there is no efficient way to say if the information is authentic or not. Therefore, a good expression is *"garbage in, garbage out"*. Here, it means that the information entering the blockchain will stay there regardless if it is false or not. In summary, other challenges that apply to all blockchains are long transaction times, coordination difficulties with many actors along with difficulties connected to the implementation part such as the cost, legal issues and the user experience. Further, it is a challenge to create incentives for people to participate and validate public blockchains for applied blockchains.

Regarding private blockchains, all the above mentioned challenges exist together with a few others. In a private blockchain there can be difficulties managing governance since the whole point of a blockchain is to remove the central controlling actor. Furthermore, deciding on a consensus algorithm or what actors in the supply chain that should be nodes in the blockchain network, constitutes a challenge if not all actors can be trusted. Another major challenge for the private blockchains is that there can exist several different blockchains within the same industry and no company want to join someone else's.

4.1.4 What Can Be the Main Challenges of Applying Blockchain in a Supply Chain?

Domain	***Result***	***Exemplifying quotes***
In general	• Point of entry for information • Long transaction times (if you want real-time information) • Legal issues, that makes it hard to implement • Lack of knowledge about how to regulate decentralized systems • Costly to implement • Hard to coordinate with many actors • Lack of knowledge about the technology • Lack of trust for the digital system and the technology • Difficult to use due to bad user experience • Teach people the concept of private and public keys • Hard to create incentives to motivate people to participate and verify blockchain application projects • The technology itself is young and immature, which makes it harder to understand what applications are possible	*"At some point, there is always a person involved in the process, so sometimes the human element will be there. And we have a saying called garbage in, garbage out. Therefore it will always be a trust risk, although it becomes smaller with blockchain."* *"The pure blockchain view [...] where all actors can unite without someone in control will take time. It is difficult to get actors to agree."* *"The processing times of different transactions, the technology is evolving rapidly each and every day. We see in the latest blockchains, the blockchain 3.0, it is a couple of thousand transactions per second, but that is the peak amount of transactions you can share. If you want to build an application like VISA/Mastercard network, where you have millions of transactions per second, that is impossible today."* *"The other challenge is public and private keys. People doesn't understand that, they are used to username and passwords."* *"The hard part will be to get all companies to follow routines. People can still cheat, so you have to create routines that catch cheaters and can be proven with the blockchain. You have to assure that the data that enters the blockchain is correct, otherwise it will be wrong anyway."*

4.1.4 Continued: What Can Be the Main Challenges of Applying Blockchain in a Supply Chain?

Domain	***Result***	***Exemplifying quotes***
In private blockchains	• Hard to manage governance • Difficult business model • Hard to implement a common blockchain for all companies in an industry • Difficult to decide what actors can be nodes • Establishing a consensus algorithm that keeps the network safe • Mistrust if certain actors have more power in the blockchain	*"The thing that constitutes an obstacle is that we don't have any functioning way to manage governance. Specially in constellations when you mix both private and public actors."* *"There are a lot of private blockchains within the same industry where everyone wants to create their own but no one want to join someone else's."* *"The most important is that no central actor can decide over the network. Because if there is an actor that can mess it up on their own, then you haven't got what you wanted from the network and lose the point of blockchains"* *"A blockchain is needed first when there isn't any actor that everyone can trust. Because otherwise that central actor could hold the information. If the need is to be able to determine whether it is a SKF product or not, SKF can have the information that strengthens it. So then it is just about marking and the ability to find the digital twin in the cloud where all information is."* *"Another security concern is also if 2/3rds is based on the consensus they use, and the majority of the parties try to collude or change something, there is no point. It's easier to rewrite the information in the blockchain as well, basically re-mine the blocks. And you don't need super good infrastructure for that. So right now you see the private blockchain it is like no real companies are using it. They just build for their own customized purpose. But that's not really blockchain."*

4.1.5 What Processes in a Supply Chain Are Suitable for Blockchain Application?

In table 4.1.5 below, the data gathered associated with this research question is assembled. As shown, there are three outlined domains where blockchains are used today: financial services, physical products and supply chains along with other use cases. Blockchain emerged in the financial service sector and are mainly a auditing tool for the banking industry and is used for monetary transactions. Today, blockchain is used in several processes in supply chains, such as documentation and certificate trading to mention a few. Another applicable process is for example when the content of an item is the important part, and not the item itself. A contract is a good example of this where the information within the contract is more important than the paper itself.

4.1.5 What Processes in a Supply Chain Are Suitable for Blockchain Application?

Domain	***Result***	***Exemplifying quotes***
Financial services	• Auditing tool for the banking industry • Monetary transactions	*"Business margins are so tight in the banking industry. There is nothing super cool about blockchain for them more than it is a smart auditing tool."*
Physical products and supply chains	• In certificate trading processes, where the blockchain can be used to represent certificates to be traded down the supply chain • In physical activities/processes that have been automated • To automate documentation activities • Logbooks, ledgers and clearing functionalities	*"So far it is logbooks, ledgers, documents that you sign and stamp and similar clearing function, that is what has built trust for the supply chain so far. But it is inefficient, it takes time and all things that takes time becomes transaction costs and does that you also get increasing costs along the way. It also does that every step can be manipulated."* *"Maersk is a company that has profiled themselves where they have done a lot of this [digitized different processes]. Their logistics flows on the sea, with containers and everything."*
Other use cases	• In processes where the content of an item and not the item itself is important • Contracts	*"The advantage with contracts is that the content is the important part, not the paper itself. It is the agreement between two or more parties that is important, not that you have signed with your signature on the paper"*

4.1.6 How Could the Adoption of Blockchain Develop in the Future?

The data that answers against this research question is assembled in Table 4.1.6. Primarily, it is worth mentioning that the blockchain technology is still relatively new and that it is hard to outline any specific future application areas. Some experts see great potential in the near future, while others are more skeptical about how far the development of the technology has reached today and see the big breakthrough first in a few decades. It will most likely not change the world on its own but together with other technologies such as IoT and AI, it will probably have an important role in the future. Some future application areas that the interviewees believe in are documentation verification, the mobility sector, in different supply chains and identity verification both in the IoT society but also in governmental systems for civilians.

4.1.6 How Could the Adoption of Blockchain Develop in the Future?

Domain	***Result***	***Exemplifying quotes***
Potential future blockchain application areas	• Hard to say since the technology is relatively new • Most likely it will be used together with other technologies • As secured documentation verification • In the mobility sector • In supply chains • To verify identities in the IoT society • Identity verification in governmental systems, e.g. instead of the current Mobile Bank ID	*"[Blockchain] is not going to change the world tomorrow, but will be a part of the change together with IoT and AI"* *"As everything becomes more digital and IoT will have a big part in society, blockchains role will be to verify all the information and the identities in the system."* *"It's like asking someone in the 1960's, who has been involved in the development of the absolute first thoughts of the internet, what will the internet look like in 2019? There is not a chance that they will be able to describe that. They wouldn't even be able to tell what the internet would look like 15 years later. It's impossible, and it's the exact same thing with blockchains today."* *"I think you will have to think that it is not before in 30 years that we will see maturity, solutions that are ready for a larger distribution. I don't think we will see them sooner than in 30 years. I think it is so long until we see them that I will probably retire before the first real solutions can be distributed."* *"Generally, when you need to share info, when people do not trust each other, where there are different incentives and roles."*

4.2 Examples of Blockchain Projects

Given the capabilities of blockchain to provide traceability, digitalization of processes, make processes more secure and the supply chain more transparent, there are many examples of how a blockchain could potentially be used beyond Bitcoin. This section presents a fraction of the many cases were solutions that claim to be based on blockchain are used.

4.2.1 Blockchain in Digitization Projects

In January of 2018, IBM announced that they together with Maersk were working on establishing a new platform to reduce barriers in global trade and increase security and efficiency in supply chains (White, 2018). The platform would be based on blockchain technology. The two main capabilities of the platform at its launch were to provide visibility throughout the supply chain for all actors, as they in a secure way could register shipping events in real time, and digitization of the massive paperwork processes that for long have been a part of the shipping industry. In August 2018, IBM and Maersk presented the result of their collaboration: TradeLens (IBM, 2018). In TradeLens, more than 100 organizations participate, including operators in ports and terminals, shippers and shipping lines, customs authorities in several countries, transportation and logistics companies. These actors are all a part of the digital supply chain, and participate to create a single view of all transactions in the ecosystem, without compromising the integrity of the individual actors. In TradeLens, actors collaborate on information exchange, creating a secure and immutable record of transactions by using a permissioned blockchain. Smart contracts are used to establish cross-organizational business processes and to prevent any actor from changing the business logic (Tradelens.com, 2019). Every step of the journey is added to the blockchain, enabling a paperless, frictionless and trusted network of actors. In TradeLens, participants can subscribe to events happening within the blockchain network. Depending on what role the own organization has within the network, it can subscribe to events regarding for example a port or a whole country. Regarding a specific shipment, only the participating actors in that shipment are able to submit, alter and approve related data. If any party would want to change anything concerning the shipment, it would require approval by all affected actors. Aside from the legitimacy aspect of these capabilities, actors can also get real time information about their shipments. According to Bridget van Kralingen, senior vice president for IBM Global Industries, Solutions and Blockchain, TradeLens have huge potential, but realizing it depends on whether the global shipping industry can unite around TradeLens as a common approach (IBM, 2018). Today, only a few months after its release, over 10 million events are processed on the platform every week (Tradelens.com, 2019).

The next example does not consist of a distinct supply chain, but could be seen as a

supply chain of information with different actors. Lantmäteriet (belonging under the Ministry of Industry and responsible for the real estate division in Sweden) investigated whether blockchain could be used in the process of property transactions. The current process of buying and selling properties today is quite complicated and involves several different parties such as seller, buyer, broker, banks, the state, Lantmäteriet et cetera. One central part of the process is the creation of a purchase agreement which is currently stipulated by law to be in paper form. Therefore, all documentation is done via physical papers and takes a long time. Thus, one of the reasons Lantmäteriet started this project was to influence the legislators and show them that it is possible to make the process digital. Together with Kairos Future, Telia Sonera and ChromaWay, Lantmäteriet developed a blockchain solution that involved every step of the process from broker to Lantmäteriet where it was finally registered. All the transactions became a workflow of digital signatures and smart contracts that were stored on the blockchain to ensure nothing was altered or manipulated afterwards. This could then be used as evidence if one of the parties later broke the contract. With this solution, the lead time of the process was reduced from four months to only a couple of days (Lantmäteriet, 2016). Regarding consensus, when a transaction or update was made, all the nodes voted and validated it if they thought it was legit. Since the law still requires purchase agreements to be done in paper form, this project was never implemented in reality. Another major obstacle for this project involved not finding a suitable way of managing governance. Since purchasing agreements require personal information about the buyer and the seller, the transparency of blockchain became problematic given the information's sensitive nature.

4.2.2 Blockchain in Traceability Projects

As mentioned, blockchain can provide traceability of assets. Therefore, another application area for this technology is within the chain of custody systems previously described in section *3.6 Chain of Custody* where sustainability is the main focus, such as the food industry. For example, IBM together with Walmart successfully traced mangoes back to its point of origin within seconds by using IBM Blockchain Platform (IBM, 2017). Further, a company called Cargill managed to track turkeys back to the farm they were raised at using a blockchain-based solution (Cargill, 2017). Blockchain reinforces the chain of custody models by increasing the transparency and trust between the actors in a network. If all transactions within the network is added to the blockchain, it enables the possibility to trace a product back to the point of origin. To enable this traceability of products, the products are in need of some sort of information tag, such as a barcode, QR-code or RFID (Abeyratne and Monfared, 2016). This information tag is what gives the product its unique identity and links the physical product to its virtual identity in the blockchain network. Through the virtual identity, it is then possible to display product information such as description, location, certifications and so on.

Regarding certificate trading, blockchain can secure and strengthen the digital certificates to make sure that they are not altered or manipulated before being transferred to another actor. Provenance offers a digital platform where certifiers and licensees can meet to share verified product information stored on a blockchain (Provenance, 2019). This also enables the traceability and transparency in a supply chain.

Another example of a company using blockchain to trace products is Everledger who offers so called *ecosystems of trust* by using smart contracts, machine vision and IoT together with a blockchain platform to trace for example diamonds (Everledger, 2019). The company argues that the trust is created by the ability to transparently trace and manage assets on their way in the ecosystem through a trusted data protocol. The physical asset are here instead given a unique identity by forensic approaches rather than a tag, that later can be tracked as a digital asset stored in the blockchain network. The diamond's unique identity depends on its cut, clarity, color et cetera, which is almost impossible to copy. Before a transaction can be added to the chain, consensus across the network is needed, which counteracts fraud and error. The blockchain ledger keeps a record of high resolution photos of each diamond along with every touch point of its journey from mine to customer. It also holds certificates of authenticity as well as product details. This makes the supply chain more transparent and thus more trustworthy. Although Everledger argue that their solution is secure and impossible to manipulate after the diamond is given the unique identity, there are issues with this regarding counterfeit diamonds, according to some blockchain experts. Arguably, the identity is given to the diamond after it has been cut, resulting in the possible risk of counterfeits entering the ecosystem before the diamonds reach this state.

The final example involves Stena Steel and a company called Chainvine that offers distributed ledger technology solutions, such as blockchain. Stena Steel is, as the name reveals, a steel wholesaler and distributor that purchases big amounts of steel from different manufacturers and then sell it on to customers in smaller pieces. The desire to trace the steel is increasing due to the fact that sustainability and quality is becoming more important. Therefore, Stena Steel and Chainvine performed a pilot study where they set up a blockchain solution to trace the steel from manufacturer to end customer. Today, when the manufacturer sells the steel to Stena Steel, a certificate containing information about the steel's characteristics such as the chemical composition, weight, solidity along with the charge number is enclosed. Sometimes the steel is marked with the charge number and sometimes it is not. However, since the steel is often separated and reworked into a new shape or product by Stena Steel, it is impossible to mark all of it. With the blockchain solution, this certificate was uploaded when a manufacturer sold the steel to Stena Steel and was then verified by Stena Steel when they received the steel. This procedure was repeated when the transformed steel products were sold to customers which created a chain of secure, transparent and traceable transactions. Consensus within the network would thus mainly consist of the actors reaching an agreement between themselves. The primary reason this pilot study was never put into action was that

Stena Steel's infrastructure was not mature enough for this big change as it is today. A plan mapping what type of traceability and infrastructure Stena Steel need to have in order to manage this blockchain solution is required. Further, standards must be developed and scanning solutions must be implemented to allow for automation. Another reason involved difficulties to collaborate with all of the 5 100 actors needed to be a part of the blockchain. Stena Steel found it hard to demand that both the suppliers and the customers would need a blockchain wallet in this network in order to sell to or buy the steel from them. Today, the customer need for this blockchain solution does not exist as there is no great risk of counterfeit products in the steel industry. To implement this kind of solution in reality, it would require a large investment, both in time and money. Stena Steel's biggest challenge is how to mark the steel. The company felt that a blockchain solution would not be suitable in the near future with their way of working today.

4.3 SKF - A Case Study

As mentioned above, SKF is a reference case for this study as the firm's operations constitute a good example of an extensive industrial supply chain for physical products. Therefore, the case of SKF offers insights to the characteristics of such a supply chain, which is used as input for discussing whether blockchain is suitable for to use in that environment to prevent counterfeiting. In the presentation of the case, the supply chain and sales channels of SKF is first described. Thereafter, the operations of Group Brand Protection in their fight against counterfeiters is presented, including how they work with verification of bearings today.

4.3.1 SKF's Supply Chain and Sales Channels

The supply chain that SKF have today is to a certain extent a rest from the "Channel Concept" that the company originally introduced during the 1980s. The idea was that each factory would have a dedicated channel that they delivered to. In each channel, there would be a bottleneck operation, against which production planning was made. This heritage is not the current implementation, but the supply chain is still to a certain extent centered around sales channel thinking. On a holistic level, SKF have two different sales channels. The first one is direct sales to large customers, such as OEMs, and the other one is aftermarket sales. Sales in the second channel is often done through authorized resellers. In the case of direct sales, the relationship with the customer have often been established for a long time, and large volumes of products are bought each time. In these relationships, EDI-integration often exists between SKF and the customer, so that customers' demand is known and orders are automatically generated when customers' stocks run low.

SKF's supply chain is however not so straightforward as to just divide it into two sales channels. An overview of the supply chain is presented in Figure 4.1 below, and next described in further detail. First, bearings are produced in factories that often are highly automated and utilize robotics to a large extent and are next sent to adjacent factory warehouses. Either, products are sold directly to large OEMs from the factory warehouses, or they are sent to huge regional warehouses as a first step of the aftermarket sales channel. There are in some cases only one of these enormous warehouses per continent, and they keep basically all SKUs in stock to accommodate short lead times to customers that demand it. From regional warehouses, products mainly go to authorized resellers. The next step in the chain are local warehouses, that often can be country specific and not close to where there is any production. The local warehouses are basically sales organizations that keep stock close to the small customers in local markets. This last step in the SKF's organization is also used to keep stock for service work.

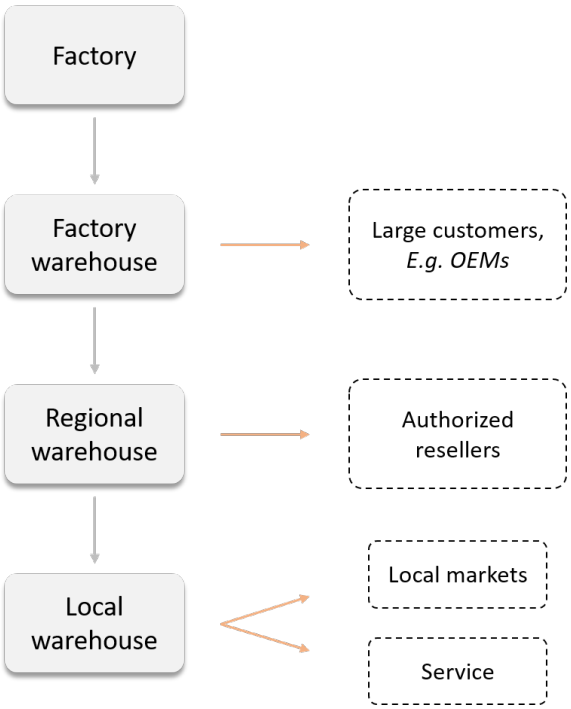

Figure 4.1: *SKF's Downstream Supply Chain*

This supply chain setup creates a replenishment system around which production is planned. This means that it is demand pull that controls production. In order to stay close to demand in their production, SKF utilize hierarchy planning. For each customer, there is a routing that specifies from which warehouse the customer should receive each item they have ordered. This is needed so that SKF plan production and allocate stock properly.

In their network, SKF have approximately 17 000 authorized resellers of their products around the world. The reasons that the company use reseller to reach end consumers are several. Historically, SKF's rapid expansion already within their first ten years of existence required the use of resellers to establish themselves on international markets, since establishing their own sales organization would be too slow and too costly. Today, knowledge of a local market is still a valid argument to use resellers, and so is lower cost and increased reach. Finally, the idea is that resellers can offer a full experience and solution, so that SKF can increase their sales more than they could on their own. Depending on country, the standard of the resellers can vary a lot. In some countries authorized resellers are well established, large firms while they in other are small companies operated by only one or a few people. Thus, their level of digitalization varies greatly. It is also worth mentioning that bearings

are sometimes sold or transferred between different resellers if one of them are low in stock. On rare occasions large customers, such as an OEM, buy more bearings than they need and then sell the residual on the market. This could then create unfair market conditions towards smaller resellers, since buyers of large volumes get a better price which they can compete with.

When transporting their products down the supply chain, SKF use most types of transportation alternatives there is. A large portion of products, especially for intercontinental transportation, is shipped by sea freight. The other main way of transporting goods is by truck, especially in certain parts of the world like North and South America. To coordinate the shipping, SKF have their own company called SKF Logistic Services that buy the service on the external market. Shipping by train is done in a limited scale, basically only when transporting goods from Europe to China. Finally, air freight is only done in emergency situations to large customers. Traceability exists in the supply chain up until the point when the products leave SKF's ownership, e.g. when they reach a reseller or OEM. Each order from a customer can be connected to a certain batch. As mentioned a lot of the network is EDI-integrated, but for smaller resellers and customers, order and freight documents together with slips are still used.

4.3.2 The Problem of Counterfeiting for SKF

There are several points of entry for counterfeit products into the distribution flow of bearings before they reach end customers. The end customers are the ones that most often contact SKF to understand whether their products are genuine or not. Local equipment dealers, that sometimes buy their bearings directly from authorized resellers, also buy goods from other actors on the aftermarket. Since the aftermarket is where most counterfeit products are traded, counterfeit bearings are sometimes purchased intentionally or accidentally by these small actors. They are then often the ones who sell them to end customers. Another point of entry that has occured in the past is when OEMs or authorized resellers buy counterfeit products from the aftermarket circulation, generally to lower prices. These actors might by the counterfeits accidentally or intentionally, to lower their costs and increase their margins. As shown by Figure 4.2, this means that the problem of counterfeiting basically exists outside SKF's supply chain.

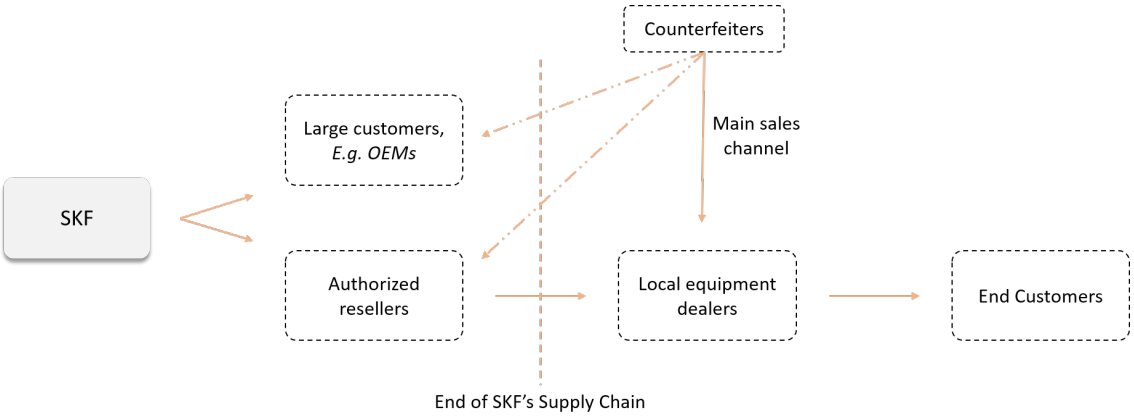

Figure 4.2: *The problem of counterfeiting exists mainly on the aftermarket*

4.3.3 SKF Brand Protection Activities

As mentioned, SKF have a Group Brand Protection (GBP) unit to counter the counterfeiters. A large portion of GBP's work is constituted by educating customers on where to find genuine SKF products by referring to authorized resellers, and to verify whether products that customers have received are genuine or not. Customers that suspect that their goods are counterfeit can send pictures of the actual bearing, and perhaps also its box, to GBP via the official mobile app SKF Authenticate. GBP receive approximately 40 requests from customers each day through this channel and aim to answer every request within 24 hours. Counterfeit products are visually very similar to genuine products and require longtime experience to be able to verify authenticity. Even with experience, determining whether a product is genuine or not can sometimes be difficult. Features both on the package as well as on the bearings are analyzed and compared with internal databases to determine whether the product is genuine or not. Other than by image requests, GBP discover fake products on the market when they are contacted by customs authorities, work proactively with them to follow suspicious players, hear from market actors about odd activities or do test purchases from resellers.

When GBP have identified that a bearing is counterfeit, the first thing they do is to notify the customer that their products are fake and advise them not to use the products. Next, they notify the local SKF sales unit in that country, which is supposed to capitalize on the business opportunity that arises from the situation. They do this by helping the customer to locate an authorized reseller and set up a business relationship with the customer. Finally, they try to require information about who the customer bought their products from, which they do not always want to reveal. After a customs seizure or if a seller of the counterfeit products is identified, GBP contact local authorities that conduct raids to seize and destroy the fake goods. It is the local authorities that carry out the raid, but GBP are present to support and identify if the products are counterfeit or not. This is also their role if the matter goes all the way to court, when the prosecutor have to convince the

judge that the goods is counterfeit. Therefore GBP only state that products are counterfeit if they feel that they can stand for it in court. Approximately, GBP assist authorities in 140 raids per year. They choose to do the raids they believe give the best return on investment and create the biggest fuzz on the market. The team do more than just conduct raids. Other activities include visiting customers, misbehaving resellers, local sales units or with embassies, police and local authorities.

5

Analysis and Discussion

The analysis is structured to in an easy way let the reader understand how it answers to the general research question: whether blockchain is suitable to use in an extensive supply chain to prevent counterfeiting of physical products, or not. This is done by first presenting the underlying problem of counterfeiting and then how blockchain could potentially help to mitigate this problem. Thereafter, it is investigated how a blockchain implemented in a supply chain would be designed, before different difficulties and challenges of using blockchain in this context are discussed.

5.1 A Summary of SKF's Counterfeiting Problem

An important part of understanding if blockchain is needed in a supply chain to prevent counterfeiting of physical products is to understand how that problem look today and in what aspects blockchain could potentially help.

As described in *4.3 SKF - A Case Study*, the problem of counterfeiting today mainly exists outside of the supply chain in which SKF operate. It does however affect the end customers of SKF's products, which is why it is important for SKF to deal with the problem. It is also a matter of regaining sales that have been lost to counterfeiters. This regardless of if the customers are satisfied with the counterfeit products or if the products risk to cause severe implications for them. The latter could mean that customers turn to SKF's competitors instead.

Today, GBP tackle counterfeiting by informing the market that the problem exists and by helping customers to verify that their products are genuine. They also conduct raids to hurt counterfeiters business, but the purpose of that activity is still to regain sales rather than to punish fraudulent actors. This is in line with what Shultz and Saporito (1996) recommend as courses of action to prevent counterfeiting. The question is whether blockchain can help to make these operations more efficient and help GBP achieve their objectives in a better way at an acceptable cost.

5.2 Potential Benefits of Blockchain and How It Could Prevent Counterfeiting

If implemented, blockchain could be beneficial by helping to drive the push towards Supply Chain 4.0. Here, complete data transparency and information on both location and condition of goods is projected to be present, together with feedback from machines and sensors to name a few examples (Alicke et al., 2016). Blockchain would definitely make data more transparent, as argued by both theory and experts. Further, as transactions on the blockchain are updated continuously as goods are moved throughout the supply chain, the transparency could give actors almost real-time information on locations of their goods, as shown in the IBM project. If machines and sensors are continued to be implemented to cater the needs of blockchain, blockchain could then provide much automation of processes that today are manual. The automation would then help to make the operations within the supply chain faster and smoother. It could also help to make the supply chain both more accurate, with automated data entries, and efficient. Overall the blockchain could help the digitalization of supply chains that in the end increase efficiency, lowers cost and can provide better products and services to its customers.

Blockchain have several other attributes and capabilities that can make it desirable in certain situations. As explained in *3.1 Blockchain Technology*, it removes the power over a network from a central party and decentralize it to its members, while still allowing the system to have safe transactions. Instead of having an administrator to govern the network that actors have to ask for permission to do certain actions, *"the administrative, governance and incentive layers are a part of the protocol"*. This means that the rules of the network are built into the source code, which all members must follow. Thus, it removes the central power from any actor, since one in order to change these rules must convince all members of the network to accept the new ones. Since collaboration within the supply chain is essential to create a larger end-user value (Christopher, 2016; Spekman and Davis, 2016), decentralization of power could be desired for enabling a better environment to achieve this.

Blockchain's distribution and transparency within the network make it possible to audit events and transactions that have occured. Therefore, if blockchain is applied to a network where it is desired to trace transactions to understand the flow of currency or products, blockchain can with these attributes offer traceability. Given that the blockchain is also immutable without the network noticing, information stored on the blockchain can serve as evidence of past transactions, as shown by for example Lantmäteriet in *4.2 Examples of Blockchain Projects*. IBM's TradeLens project also show the value of using blockchain to digitize processes that today are manual and involves a lot of paper handling, to simplify documentation and distribute data so that the information is stored in several places. Overall there are many benefits with this technology that makes it desirable in a supply chain. The question is however if these benefits could help to prevent counterfeiting of physical

products.

There are arguably two main aspects in which blockchain could be useful for this purpose; to make it harder for counterfeiters to sell their products and to help GBP to better authenticate products. The transparency of blockchain helps with the first aspect. Since it would be demanded that all actors within the supply chain participated in and conducted their transactions through the blockchain, it would be more difficult for counterfeiters to sell their products given that every transaction would be visible to everyone. Standardization and immutability means that it would be impossible to change a transaction without the whole network noticing. Thus, fraudulent transactions would be hard to carry through and even if it was possible, the evidence would still remain on the blockchain to be audited if needed. Since the transparency enables traceability of transactions in the supply chain, it could help to reinforce the chain of custody models earlier presented. If it is possible to follow all transactions of the goods throughout the chain, their provenance could more easily be tracked and different types of the same products could easier be kept separate. That could help systems that today utilise the mass balance model to move toward an identity preservation model.

The second aspect would be if blockchain helped GBP and SKF to authenticate products with more certainty and faster than they can today. If so, it would be easier to give customers advice and regain sales, and it would be easier to prove in court that products are counterfeit adjacent to conducted raids. It would also be easier to show what actors have been selling counterfeit products, exclude them from the supply chain and then remove that point of entry for these products into the market.

5.3 Blockchain Design in a Supply Chain Context

Klötzer and Pflaum (2017) view supply chains as a network of actors that are interdependent of each other and together responsible for managing and improving the flow of material from supplier to end customer. Mattsson (2003) has a markets-as-networks view and argues that every company's supply chain is a part of this view. Thus, the firm is externally connected to other actors on the market and therefore dependent on all the actions made by others in the network. This natural network, that a supply chain constitutes, is very similar to a blockchain network. In a blockchain network, all actors' actions also depends on other actions made earlier by other actors. Thus, at a first sight, blockchain might seem suitable to implement in a supply chain, especially given the potential benefits presented above. However, if blockchain is applied in a supply chain, it might have to be customized to fit into the network, and thereby potentially causing some of the original attributes to be removed. This must be carefully evaluated as it could make it hard for supply chain actors to achieve what they wanted from a blockchain in the first place.

Originally, the blockchain solution that builds up Bitcoin was invented to create a network where the need for a third party was removed, or rather replaced by the capabilities of the solution Nakamoto (2008). Nakamoto's motivation to do so was to lower transaction costs and make transactions more flexible, while still keeping a safe payment system and preventing double-spending of a digital currency. Therefore, blockchain technology seems fit to use in situations where a third party is not needed or desired. It should thus be suitable in a transaction system that exists within a network where there is no central third party that can be trusted by all actors. However, in the case of SKF and the issue of counterfeiting, this does not seem to be the case. Today, customers buy SKF bearings from different sources and if they suspect that the products are counterfeit, they contact GBP to check the authenticity. The customers have to trust the verdict that GBP gives, and there seems to be no apparent reason for them to give a false statement in such a situation. Potentially, they could claim that products are false to sell an extra round of bearings to a customer. However, given that GBP have to stand by their verdict in court and would risk to severely harm their existing business relationships, the risk of SKF doing this seems vanishingly small. This despite that verifying products' genuinity can be difficult even for SKF. One of the experts mentions that *"a blockchain is needed first when there isn't any actor that everyone can trust. Because otherwise that central actor could hold the information"*. Since SKF could act as the central party when their supply chain fights counterfeiting, a blockchain might therefore not be needed in this situation. To investigate if this is the case, an understanding of how a blockchain would be designed in such a supply chain context is first needed.

In a public blockchain, power is decentralized and members of the network together agrees on what rules to play by. The attributes of the technology are aligned with incentives to make the system safe from fraudulent behavior by its members. The data structure allows transactions to be compiled into timestamped blocks that are basically irrevocably linked to each other, and nodes throughout the network help to ensure that this is correctly done by participating in the Proof of Work consensus algorithm. Incentives exists both to make more nodes participate to establish consensus, and also deter them from doing so with a purpose to conduct fraudulent transactions. However, when talking about using blockchain in a supply chain, it seems difficult to make it a public blockchain that anyone can join.

First, with current business models of product manufacturers, it seems hard to motivate ordinary people to join their blockchain to verify transactions in the same way as for Bitcoin. What would be the reward for their help in securing a public blockchain? Incentives seems to exist mainly for the actors within the supply chain. Potentially, end customers could be interested in verifying authenticity of products they would receive in the end of the supply chain. No other reward seem to exist at the moment.

Second, the hosting organization(s) would probably not want to utilize the consensus algorithms existing in public blockchains, such as PoW, since it consumes a lot of electricity. Instead, the examples of blockchain projects and answers from experts

show that the consensus algorithm is often simplified to a vote among participants in the network or parties affected by the transaction. If this consensus algorithm is used, it could make the blockchain less secure. Theoretically it would be possible to persuade or even threaten other members outside of the blockchain to vote for a fraudulent transaction for example. Also, if only parties involved in a certain transaction need to verify it like in the case of TradeLens, then there exists a potential risk that they would collude to fraud the rest of the network. In TradeLens, involved parties can also change a previous transaction if everyone agrees. This removes one of the most central attributes in blockchain, namely the immutability of transactions. With the immutability removed, blockchain could not to the same extent be used as evidence if disputes occured.

Third, the central organization(s) around which the supply chain is structured, would probably want some authority and administrative rights over the blockchain. Since they created the blockchain for a specific purpose, they would want to determine what actors are allowed to participate in the blockchain network and what events and transactions they can add. This would leave power over the whole network with a few actors and remove the aspect of decentralization, which is fundamental to blockchain and one thing that Nakamoto (2008) aimed to achieve. For example, if a party owning the blockchain can add new members, they could potentially add themselves several times as different users. If votes are the consensus algorithm, this party could easily overtake that vote to create false transactions with their additional users. A central actor probably would not do this, since they would not want to destroy their relationships within the supply chain, but it can still be seen as a risk. With some actors having more power than others on a blockchain, other supply chain actors would likely be skeptical about joining the blockchain in the first place.

Given the discussion above, it seems likely that a blockchain designed for a supply chain would lose some of the original functionalities of blockchain and thereby make the proposed blockchain a private or permissioned one, according to both theory and experts. When this happens, it could arguably lead to unexpected implications that potentially removes the point of implementing blockchain in the first place. Some experts have a strict view about private blockchains, by saying for example that *"people call them private blockchains but in my opinion they are just distributed ledgers or distributed databases. They don't go with the ideology of blockchains like transparency or decentralization. They just call it private blockchain because it's fancy and it makes money."*. If the blockchain differs too much from the original implementation, other digital technologies such as a distributed database can potentially provide the same capabilities and benefits as a private or permissioned blockchain could.

5.4 Difficulties with Using Blockchain to Prevent Counterfeiting

To a certain extent, SKF's supply chain matches a lot of the recent changes in supply chains that are presented under section *3.5.2 How Digitalization has Changed Supply Chains*. SKF can according to Gunasekaran and Ngai (2007) be defined as a digital enterprise as they utilize ICT to integrate activities internally and externally. They also seem to value their relationships in the supply chain, and have established a collaborative approach within it in a similar way to the Extended Enterprise. It is however hard to say whether they have yet reached so far as to be up to date with Supply Chain 4.0. While their production is largely automated and robotics is used to a high extent, it is hard to understand to what degree for example sensors are implemented and if these are continuously updating information systems. Given that SKF have come relatively far in their digitalization process, they seem ready for a blockchain implementation from that perspective. However, if the goal is to use a blockchain within a supply chain to prevent counterfeiting, there exist both difficulties with implementation as well as other challenges that need to be carefully evaluated beforehand. These aspects are further elaborated below.

5.4.1 Establishing Unique Identities

The cases of IBM and Lantmäteriet provide a major insight regarding suitability for blockchain implementation. In their projects, the purpose of the blockchain is to create a supply chain of information between different actors, which does not need to involve any physical artefacts. *"The advantage with contracts is that the content is the important part, not the paper itself. It is the agreement between two or more parties that is important, not that you have signed with your signature on the paper"*, as one of the experts said. This means that it is the agreement between two parties that is essential, which is possible to upload and store on a blockchain in a secure way given its transparency and immutability. Simply put, a digital representation of a document containing certain information is easier to create than a digital representation of a physical product. When the blockchain needs to represent a physical state, such as products in a supply chain, it could be hard to know whether the information on the blockchain correctly represents the real world.

To ensure that the information on the blockchain is correct and enable authentication of a specific item, there needs to be a 1-1 link between the physical product and the digital blockchain. This requires the product to have a unique identity to distinguish it from all other copies of the same product. Today, there exist several ways to create this unique identity through e.g. tags, as can be seen under the sections *3.2 Techniques to Create Unique Identities* and *4.1.2 Can a Physical Product and the Digital Blockchain Be Irrevocably Linked Together?*. These techniques are

suitable for different purposes but some characteristics need to be present in order to counteract counterfeiting. First of all, a tag containing a unique identity must be impossible to duplicate and remove in order to generate the 1-1 link and prevent counterfeiters from using the same identity on a fake product. Second, it also needs to be durable so that it will be intact throughout the whole supply chain. Finally, the technique of creating a unique identity must be cheap enough so that the benefits of having the link between the product and the blockchain is greater than the cost of producing it. Besides products with a natural unique identity, it can be concluded from the techniques previously described that they are not sufficiently developed to fulfill all of these requirements today. As one of the blockchain experts said, *"We don't know how to connect the physical to the digital, it's a major problem"*. Today, an abstraction of a product is tagged rather than the unique physical product itself. For example, it is the amount of bearings or kilos of ore that is tagged and not the actual product itself. The creation of a tag that enables the 1-1 link between the physical and the digital is currently one of the hardest parts when trying to use blockchain in a supply chain of physical products.

However, regardless if there exist good techniques to create unique identities, linking the identity to the digital blockchain is still difficult. The link would imply that the unique identity information is stored on the blockchain's digital representation of the physical product. Thus, it must be possible to translate the unique identity into information that can be stored on the blockchain, which might not be possible for all the presented techniques. Also, a way to use the blockchain to authenticate the product like some sort of verification tool must be developed, and how this can be done is still uncertain. Now, the question arises if this information should be visible to all actors in the blockchain network or not. If the unique identity could be viewed by anyone, it could possibly be copied and put into another tag on a counterfeit product. If that possibility existed, the value of blockchain for authentication purposes would be lost. However, all actors in the supply chain would likely need to be approved by SKF to be a part of the blockchain, and thus would probably lack incentives to misuse identity information, given the risk of being excluded. Counterfeiters would presumably not be a part of the blockchain network, which would imply that neither end customers nor reseller would want to buy products from them. The blockchain must therefore be well known and SKF should advise all customers to buy their products from a member on the blockchain or the authenticity cannot be confirmed.

With this said, without the unique identity and the 1-1 link, there is nothing that ensures that the physical product matches the digital representation on the blockchain. Blockchain stores information, but it does not verify if that information is correct or not. Thus, it can store false information as well as it stores correct information. Therefore, the need for and value of a blockchain decreases if the 1-1 link between the product and the blockchain is nonexistent, especially if the main purpose is to use it for authentication purposes. This is highlighted by an expert by saying *"If [SKF] cannot tag their products, there is nothing they can do"*.

5.4.2 Entering and Storing Information on a Blockchain

Given the immutability of blockchain, a critical aspect is to ensure that the data put on the blockchain is correct. Because, if the wrong information is put on the blockchain, it will stay there. The problem of incorrect information does not exist in the Bitcoin network since it is self-referring, i.e. outgoing transactions can only be created by referring to previously incoming transactions. Therefore, incorrect information cannot exist within Bitcoin to begin with. However, if blockchain would be applied in a supply chain like SKF's, new products such as bearings would be added to the network by the manufacturer when they were produced. This could lead to that incorrect information is added to the blockchain. For example, an actor conducts a transaction of 30 bearings on the blockchain to the next actor, but only sends 25 by mistake in reality. The actor receiving the bearings does not notice this and accept the blockchain transaction, which leads to that the information on the blockchain is incorrect. In such a situation, the point of entry for products become very critical and leaves no room for error. SKF intentions can be trusted here, but in a large supply chain that is not fully digitalized the human element will always exist and be a risk. Like one of the experts said: *"At some point, there is always a person involved in the process, so sometimes the human element will be there. And we have a saying called garbage in, garbage out. Therefore it will always be a trust risk, although it becomes smaller with blockchain."*.

Potentially, sensors and information systems could be used in automated processes to update events and transactions on the blockchain in order to minimize entry errors. Smart contracts could here host potential to enable automation of information writing to the blockchain, if standardized protocols are developed that adds events to the blockchain depending on the information from sensors and information systems. While SKF's production and information systems might be ready for blockchain implementation, it seems more unlikely that all the actors within their supply chain are. The level of digitalization among the actors varies a lot, which can make the implementation of blockchain in a supply chain network difficult.

5.4.3 Blockchain and Supply Chain Size

If different private blockchains are created within the same industry, it could become a challenge to actors within that industry. If SKF would start a private blockchain with all their resellers and customers, problems can arise if a competitor starts another similar private blockchain. Since the resellers usually buy products from several companies to offer a broad product sortiment or limit supplier power, they would have to be a part of each and every blockchain in order to be able to buy the products. This could possibly lead to lower value for both resellers and customers if transaction costs increase due to this complexity. Further, SKF would potentially sell smaller volumes when resellers choose to only buy from one company. A private blockchain containing only SKF and their supply chain would therefore potentially

be effective in the beginning, due to higher security and trustworthiness within the network, but could lose value in the long run if competitors did the same. If SKF instead would collaborate with their competitors and create an industry-wide blockchain, another complexity arises. One of the main benefits with blockchain is that it enhances transparency, but in this case it could be viewed as a challenge. With the transparency, everything would become visible to everyone within the industry. For example, the amount of sold bearings and what stock the different customers are keeping would be visible to the competitors which probably is not desirable. Further, other questions emerge regarding what company would be the owner and in control of the blockchain, who would pay for the implementation and what actors should be nodes. Coordinating on these matters would be difficult for one supply chain alone, but for a whole industry it would be even harder. This is highlighted by one expert, saying *"There are a lot of private blockchains within the same industry where everyone wants to create their own but no one want to join someone else's."*.

Another challenge with blockchain in supply chains is inherent in the sheer size of the specific supply chain. As Vidal and Goetschalckx (1997) describes, a global supply chain is more difficult to manage due to several factors such as different currencies and taxation systems, but also because it involves more actors. This is supported by Manners-Bell (2014), who argues that the risks associated with a global supply chain increases the bigger it gets due to the higher number of participants. Thus, a blockchain containing a large number of actors is more difficult to manage than a network containing only a few actors. Since SKF have production factories in 24 countries, are present in 130 countries with around 17 000 resellers and have customers all over the world, the number of actors required to be a part of the blockchain network quickly becomes gigantic. In section *4.2 Examples of Blockchain Projects* it can be seen that among the studied projects, blockchain is used in smaller networks than an extensive supply chain such as SKF's. All of the blockchains described involves up to only a few hundred actors, making them relatively easy to coordinate compared to the number of actors that SKF would need to collaborate with. The exception is Stena Steel that would have had around 5100 actors in their blockchain if it was realized. One of the reasons that their pilot study was not implemented was the difficulty to demand every participant in the supply chain to be a part of the blockchain. This gives an indication of how hard it would be for an even bigger supply chain like SKF's, and strengthens the theory of how complexities in supply chains magnify when the amount of actors increase.

The blockchain network of a supply chain must probably end somewhere. Even if SKF wanted to extend their blockchain outside of their supply chain and include every end customer, that would be extremely difficult just considering the total number and varying level of digitalization of customers. If end customers are not members of the blockchain, it means that some sort of exit transaction is needed in the end of the supply chain when a bearing is bought by an end customer. This to prevent the possibility for the last actor in the supply chain to use the digital representation twice. However, since it is highly unlikely that all end customers

are aware of the blockchain, there is a risk that the bearing could be sold while the digital representation remained with the reseller on the blockchain. This means that it is possible for the last actor to both purchase and sell fake bearings outside of the blockchain until a customer that is aware of the blockchain comes along, and demands that the genuine digital representation is sold through an exit transaction on the blockchain. Hence, even with the blockchain it is possible for actors to sell fake products. To avoid it would put extreme pressure on SKF to make customers aware that authentic bearings only can be bought through the blockchain. This is again unreasonable due to the high number of customers and the large variety of digitalization between them.

The situation does however change slightly if there exists a unique tag and a solid 1-1 link between the bearing and the blockchain. It would then be possible to verify which digital representation a bearing corresponds to, and to verify that it was genuine. But as long as customers are unaware, of both the blockchain and that they have bought counterfeit bearings, counterfeiters can still sell their products. It would simply be hard to reach the counterfeiting problem just by implementing a blockchain, since the problem today exists outside SKF's supply chain. However, if counterfeiters sell their products through actors that are members of the blockchain, the transparency could potentially make it harder for these actors to cheat the system. As blockchain members, they could still potentially use their digital representations multiple times, but it would be harder to hide if sales of bearings in a region remained high when those actors themselves bought smaller amounts from SKF. Also, since an actor that is a part of the blockchain would be demanded to buy their products through the blockchain, counterfeit products could only enter the supply chain if an actor intentionally purchased fake goods. Unlike today, where authorized resellers on rare occasions could buy counterfeit bearings on the aftermarket by mistake.

6

Conclusion

This final chapter summarizes the answer to the general research question which has been discussed in the previous analysis and discussion. Arguments are first made as to why the technology is suitable, after which the arguments against suitability is presented and an overall conclusion is then reached together with future potential for the technology. This is followed by a section regarding potential future research, before concluding with a section presenting the practical implications for SKF.

6.1 Conclusion of Thesis

Blockchain has undoubtedly many benefits that are attractive for extensive industrial supply chains and some that could help to mitigate the problem of counterfeiting. While automation is already an ongoing process in many supply chains today and a bit of a challenge, blockchain implementation could help to accelerate this process. Automated transactions could help to ensure that the correct information was uploaded on the blockchain. With automation and standardization, deviations could more easily be spotted and make it harder to cheat the system like in the case of counterfeiting. Counterfeiting could also be mitigated by the transparency, distribution and immutability of blockchain. The transparency would allow for traceability within the supply chain as well as making it impossible to change transactions without the network noticing. The distribution and immutability of transactions stored on the blockchain could enable auditing of past transactions and have them serve as evidence in case of disputes.

Despite the above mentioned reasons for why blockchain is suitable to use in a supply chain, there are several contradictory reasons for why it is not. Since blockchain was invented to remove a central party, decentralize power and increase the trust in a network, it is most suitable when there is no central party that is trusted or desired. Therefore, a blockchain might not be needed if the manufacturer of physical products can be a trusted central party in the extensive industrial supply chain surrounding it, since they have the information required to authenticate the products. Further, a potential blockchain for an extensive supply chain would likely be private in its

design, causing it to lose some of the attributes and capabilities that the original blockchain provided. When this happens, the point of implementing blockchain in the first place would potentially be lost and other digital technologies might be better suited for preventing counterfeiting.

Without a tag containing a unique identity and an irrevocable 1-1 link to the blockchain, there is nothing that ensures that the physical product matches the digital representation. Thus, blockchain could not be used to securely authenticate products and therefore loses some of its value. Furthermore, to ensure that blockchain benefits could be fully utilized, the information on the blockchain needs to be correct at all times. Therefore, point of entry is critical when the blockchain is supposed to represent a physical state. Automation could help to remove the human element and ensure information validity, but in an extensive supply chain, the level of digitalization will vary and make a blockchain implementation difficult. Finally, to coordinate a large amount of actors within a supply chain to create a blockchain is difficult. Creating a blockchain that stretches across a whole industry will add even more complexities. In an extensive supply chain it would be challenging to make every actor a member of the blockchain and to make end customers aware of it. Therefore, it can be argued that it would still be possible for counterfeiters to sell bearings outside of the blockchain. If the problem with counterfeiting lies outside of the supply chain, a blockchain cannot help to stop counterfeiting in full.

At first sight, it is easy to believe that blockchain can help with the two main aspect of preventing counterfeiting of physical products; namely to make it harder to sell the counterfeits and to improve authentication of products. However, learning more about the technology leads to the realization of the difficulties of using it to prevent counterfeiting. The challenges with using blockchain in an extensive supply chain slowly starts to outgrow the benefits. Instead, it becomes clear that blockchain might be too complicated and unnecessary to implement in such a supply chain as of today and other digital technologies such as a distributed database might be more suitable. Blockchain do however host a huge potential to create value for supply chains and help to prevent counterfeiting if the difficulties presented are mitigated and future technological development make implementation easier.

A concluding remark should be made that many of blockchain's benefits are an outcome of the setting they were originally applied in, and might be removed when blockchain becomes private in its design. Thus, it is highly important to consider what aspects of blockchain are desired and if these would still be achieved in the intended environment, so that the original point of blockchain implementation is not lost.

To conclude, the answer of the general research question of this thesis is that blockchain is not suitable to use in an extensive supply chain to prevent counterfeiting of physical products today.

6.2 Future Research

This thesis have shown the challenges with implementing blockchain in a supply chain, and also raised questions regarding if blockchain can be helpful to prevent counterfeiting of physical products or not. It also aimed to lift questions that companies working in extensive supply chains need to ask themselves before implementing a blockchain solution in their network. However, given that this thesis had a limited time to conduct research in, not all leads could be followed, and this leaves room for more investigation to be done by other researchers. For example, there are many blockchain projects existing around the world that this thesis did not have time to look into. By synthesizing experiences from these, new insights could be drawn about blockchain application in supply chains. More research could also be conducted on the problem of linking physical products to digital representations and how this can be useful. Business models should also be researched to see if incentives can be created for people outside of the supply chain to participate in its blockchain and thereby make it a public blockchain, ensuring higher security. Coordinating actors and activities in a decentralized system to achieve a common purpose is a relatively new phenomenon, and how this can be done in an efficient way is another subject that needs further exploring.

6.3 Practical Implications for SKF

SKF's original inquiry was to develop an understanding about blockchain and whether it could help them to mitigate the problem of counterfeiting through authentication of products or by providing secure traceability of products in their supply chain. If blockchain would have shown potential for this purpose, they might have pursued a future investment in the technology. Therefore, guidelines on how SKF can use the analysis and conclusion of this thesis to move forward is presented below.

Since SKF sell physical products, complexities arises when a blockchain, which is digital, is supposed to be used to authenticate the products. First, there is the problem of creating a unique identity by marking or tagging a product in a way that can be maintained throughout the supply chain. Second, even if such identity tags could be created, that information would need to be stored on the blockchain so that the blockchain could be used for authentication. Today, it is however hard to see how this could be done in a way that is better and more secure than any other verification tool. Therefore, from an authentication point of view, blockchain does not seem to be an all mighty solution worth pursuing for SKF as of today.

However, blockchain have potential from other perspectives to mitigate the counterfeiting problem. The transparency and immutability aspects in a blockchain network show potential to provide the secure traceability in the supply chain that SKF initially sought after. With an implemented blockchain and well established

standards for transactions within the supply chain, deviations from these transaction standards could more easily be discovered than what they can today so that suspected counterfeit activities could be investigated. However, since the problem today exists *mainly* outside SKF's supply chain, it would need to be further investigated as to if the blockchain could help to spot suspicious activities better than what today's operations can. Since it also seems likely that a potential blockchain implementation would be private in its design, some attributes and capabilities might be lost. Therefore, it is important to investigate if there exists other digital solutions that can provide the same level of traceability within SKF's supply chain as such a blockchain solution potentially could. Along with these two considerations, SKF must evaluate the challenges presented in the analysis to see whether it is reasonable to believe that a blockchain could be implemented throughout their supply chain or not.

To conclude, it can be said that blockchain have a large potential to do good in supply chains, not just from an anti-counterfeiting perspective. The technology is however young and will continue to develop going forward. As of today, blockchain is not suitable to use in a supply chain to prevent counterfeiting of physical products, but SKF should continue to observe the technology as it matures and to see if it will meet the needs they have in their operations. The wait could be long however. As one of the experts said - *I think you will have to think that it is not before in 30 years that we will see maturity, solutions that are ready for a larger distribution. I don't think we will see them sooner than in 30 years. I think it is so long until we see them that I will probably retire before the first real solutions can be distributed.*

References

Abeyratne, S. A. and R. P. Monfared (2016). "Blockchain ready manufacturing supply chain using distributed ledger". In: *International Journal of Research in Engineering and Technology* 5.9, pp. 1–10.

Alicke, K., J. Rachor, and A. Seyfert (2016). *Supply Chain 4.0 – the next-generation digital supply chain*. URL: `https://www.mckinsey.com/business-functions/operations/our-insights/supply-chain-40--the-next-generation-digital-supply-chain`. [2019-03-20].

Appelbaum, D. and S.S. Smith (2018). "Blockchain Basics and Hands-on Guidance: Taking the Next Step toward Implementation and Adoption". In: *The CPA Journal* 88.6, pp. 28–37.

Bai, X. et al. (2008). "Anti-fake label and security identification system based on multiple luminescent quantum dots". In: *2008 2nd International Conference on Anti-counterfeiting, Security and Identification*. IEEE, pp. 45–47.

Berman, B. (2008). "Strategies to detect and reduce counterfeiting activity". In: *Business Horizons* 51.3, pp. 191–199.

Bitcoin.org (2019). *Bitcoin Developer Guide*. URL: `https://bitcoin.org/en/developer-guide`. [2019-03-15].

Blockgeeks (2018). *What is Ethereum Gas: Step-By-Step Guide*. URL: `https://blockgeeks.com/guides/ethereum-gas-step-by-step-guide/#What_is_Ethereum_Gas_Step-By-Step_Guide`. [2019-03-21].

Bryman, A. and E. Bell (2015). *Business Research Methods*. Oxford University Press, USA.

Bussmann, O. (2017). "BankThink A public or private blockchain? New Ethereum project could mean both". In: *American Banker.[Retrieved from] https://www.americanbanker.com/opinion/a-public-or-private-blockchain-new-ethereum-project-could-mean-both*.

Cachin, C. and M. Vukoli (2017). "Blockchain consensus protocols in the wild". In: *arXiv preprint arXiv:1707.01873*.

Cargill (2017). *Honeysuckle White® brand leads the way in food transparency, delivering a farm-to-table Thanksgiving featuring first-ever traceable turkeys*. URL: `https://www.cargill.com/2017/honeysuckle-white-brand-leads-the-way-in-food-transparency`. [2019-03-20].

Chang, Y., E. Iakovou, and W. Shi (2019). "Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities". In: *arXiv preprint arXiv:1901.02715*.

Chen, L. et al. (2016). "Use of CdS quantum dot-functionalized cellulose nanocrystal films for anti-counterfeiting applications". In: *Nanoscale* 8.27, pp. 13288–13296.

Christidis, K. and M. Devetsikiotis (2016). "Blockchains and smart contracts for the internet of things". In: *IEEE Access* 4, pp. 2292–2303.

Christopher, M. (2016). *Logistics & supply chain management*. Pearson UK.

Crosby, M. et al. (2016). "Blockchain technology: Beyond bitcoin". In: *Applied Innovation* 2.6-10, p. 71.

D'Aliessi, M. (2016). *How Does the Blockchain Work? Blockchain technology explained in simple words*. URL: https://medium.com/s/story/how-does-the-blockchain-work-98c8cd01d2ae. [2019-02-22].

Eisenhardt, K. M. and M. E. Graebner (2007). "Theory building from cases: Opportunities and challenges". In: *Academy of management journal* 50.1, pp. 25–32.

Everledger (2019). *Emerging technology solutions for real world challenges*. URL: https://www.everledger.io. [2019-03-18].

Gartner (2019). *IT Glossary*. URL: https://www.gartner.com/it-glossary/. [2019-03-15].

Gill, P., A. J. Jeffreys, and D. J. Werrett (1985). "Forensic application of DNA 'fingerprints'". In: *Nature* 318.6046, p. 577.

Gobble, M. M. (2018). "Digitalization, Digitization, and Innovation". In: *Research-Technology Management* 61.4, pp. 56–59.

Google (2019). *"blockchain"*. URL: https://trends.google.com/trends/explore?date=2015-03-12\%202019-04-12&q=blockchain. [2019-04-12].

Green, R. T. and T. Smith (2002). "Countering brand counterfeiters". In: *Journal of international Marketing* 10.4, pp. 89–106.

Gunasekaran, A. and E. WT. Ngai (2007). "Managing digital enterprise". In: *International Journal of Business Information Systems* 2.3, pp. 266–275.

Harvey, M.G. (1987). "Industrial product counterfeiting: problems and proposed solutions". In: *Journal of Business & Industrial Marketing* 2.4, pp. 5–13.

IBM (2017). *Walmart, JD.com, IBM and Tsinghua University Launch a Blockchain Food Safety Alliance in China*. URL: https://www-03.ibm.com/press/us/en/pressrelease/53487.wss. [2019-03-19].

— (2018). *Maersk and IBM Introduce TradeLens Blockchain Shipping Solution*. URL: https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution. [2019-02-06].

ISEAL Alliance (2016). "Chain of Custody: Models and Definitions". In: *ISEAL Alliance: London, UK*.

Jeffreys, A. J., V. Wilson, and S. L. Thein (1985). "Individual-specific 'fingerprints' of human DNA". In: *Nature* 316.6023, p. 76.

Jung, L. et al. (2016). *DNA marking of previously undistinguished items for traceability*. US Patent 9,266,370 B2.

Klötzer, C. and A. Pflaum (2017). "Toward the development of a maturity model for digitalization within the manufacturing industry's supply chain". In:

Konstantopoulos, G. (2017). *Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake*. URL: https://medium.com/loom-network/under-

standing-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb. [2019-02-22].

Korpela, K., J. Hallikas, and T. Dahlberg (2017). "Digital supply chain transformation toward blockchain integration". In: *proceedings of the 50th Hawaii international conference on system sciences*.

Lantmäteriet (2016). *Framtidens husköp i blockkedjan*. URL: https://www.lantmateriet.se/contentassets/ee30ed78dcdb4dd698cf454001369cf8/blockkedjan-framtidens-huskop.pdf.

Manners-Bell, J. (2014). *Supply Chain Risk: Understanding Emerging Threats to Global Supply Chains*. Kogan Page Publishers.

Martinez, J. (2018). *Understanding Proof-of-Work, Part 1: Demystifying Solving a Block*. URL: https://medium.com/@julianrmartinez43/understanding-proof-of-work-part-1-586d7ee6b014. [2019-02-22].

Massessi, D. (2018). *Blockchain Public / Private Key Cryptography In A Nutshell*. URL: https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c. [2019-02-22].

Mattsson, L-G. (2003). "Reorganization of distribution in globalization of markets: the dynamic context of supply chain management". In: *Supply Chain Management: An International Journal* 8.5, pp. 416–426.

Murphy, C. J. (2002). *Peer reviewed: optical sensing with quantum dots*.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. URL: https://bitcoin.org/bitcoin.pdf.

— (2009). "Bitcoin v0. 1 released". In: *The Mail Archive* 9.

Noy, C. (2008). "Sampling knowledge: The hermeneutics of snowball sampling in qualitative research". In: *International Journal of social research methodology* 11.4, pp. 327–344.

OECD (2007). *The economic impact of counterfeiting and piracy: Executive summary*. OECD Publishing.

OECD/EUIPO (2016). *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact*. Paris: OECD Publishing.

Peck, M. E. (2017). "Blockchains: How they work and why they'll change the world". In: *IEEE spectrum* 54.10, pp. 26–35.

Provenance (2019). *Reinforcing organic certification in the digital age*. URL: https://www.provenance.org/case-studies/soil-association. [2019-03-20].

Selectamark Security Systems (2019). *SelectaDNA Technology*. URL: https://www.selectadna.co.uk/. [2019-04-17].

Shultz, C. J. II and B Saporito (1996). "Protecting intellectual property: strategies and recommendations to deter counterfeiting and brand piracy in global markets". In: *The Columbia Journal of World Business* 31.1, pp. 18–28.

Sillaber, C. and B. Waltl (2017). "Life cycle of smart contracts in blockchain ecosystems". In: *Datenschutz und Datensicherheit-DuD* 41.8, pp. 497–500.

Singhal, B., G. Dhameja, and P. Sekhar Panda (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Berkley, CA: Apress.

SKF (2019). *About SKF*. URL: https://www.skf.com/se/our-company/index.html. [2019-04-23].

Spekman, R. and E.W. Davis (2016). "The extended enterprise: a decade later". In: *International Journal of Physical Distribution & Logistics Management* 46.1, pp. 43–61.

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

Szabo, N. (1997). "Formalizing and securing relationships on public networks". In: *First Monday* 2.9.

Tilson, D., K. Lyytinen, and C. Sörensen (2010). "Digital Infrastructures: The Missing IS Research Agenda". In: *Information Systems Research* 21.4, pp. 748–759.

Tradelens.com (2019). *TradeLens Documentation*. URL: `https://docs.tradelens.com/`. [2019-04-17].

Tuyls, P. and L. Batina (2006). "RFID-tags for anti-counterfeiting". In: *Cryptographers' Track at the RSA Conference*. Springer, pp. 115–131.

Vidal, C. J. and M. Goetschalckx (1997). "Strategic production-distribution models: A critical review with emphasis on global supply chain models". In: *European journal of operational research* 98.1, pp. 1–18.

White, M. (2018). *Digitizing global trade with maersk and IBM*. URL: `https://www.ibm.com/blogs/blockchain/2018/01/digitizing-global-trade-maersk-ibm/`. [2019-02-06].

WTO (2019). *Glossary: Counterfeit Definition*. URL: `https://www.wto.org/english/thewto_e/glossary_e/counterfeit_e.htm`. [2019-02-01].

Yahoo (2019). *Bitcoin USD (BTC-USD)*. URL: `https://finance.yahoo.com/quote/BTC-USD`. [2019-04-23].