Torbjoern Haug

Feasibility Study of Blockchain in Supply Chain

Master's thesis in Mechanical Engineering
Supervisor: Bjørn Andersen
January 2019

Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

Preface

This thesis is the outcome of the course TPK4920 - Project and Quality Management, Master's Thesis, which is the final course and concludes the 5 year Mechanical Engineering master programme at the Norwegian University of Science and Technology. The thesis amounts to a full semester of 30 ECTS, and is normally written in the 10th semester of the degree, during the spring, but this thesis is written during the fall, as the last semester were postponed. Often the master thesis builds upon and is a continuation of the course TPK4920 Project and Quality Management, Specialization Project written the previous semester, but this is not the case for this thesis, and a new topic and field of research were chosen.

I have for a couple of years followed cryptocurrencies and blockchain technology and it is a topic I am interested in, so when I decided to change topic from the Specialization projects, I brought up the topic of blockchain technology, and if it could be of interest to link that up to project supply chain. My supervisor thought it could be interesting, especially since I was interested in the topic.

I am greatly thankful for the willingness and the time provided from the interviewees to share there experience and thoughts with me, thus enabling this thesis, thank you. I would like to thank my supervisor Bjørn Andersen, and I am grateful for his support, guidance, availability and flexibility considering the thesis. I would like to thank my family for all these years, and I would like to thank the Norwegian school system that have enabled me to do a master degree.

Torbjoern Haug
Trondheim, 25. January 2019

II

Abstract

The innovation of blockchain technology is still in its early stages, and as for today most of the opportunities investigated are related to finance, and which opportunities it could provide in other industries are still to be explored. One of the topics that have gotten some attention beside of finance, is supply chain. Even though there are some projects working on solutions considering supply chain as for today, most of them have little to show for yet. This thesis provides a feasibility study of use of blockchain in supply chain, especially related to project supply chains of construction projects. The thesis has two main objectives, where the first is to determine challenges and opportunities in the supply chain of construction projects, as the second is a feasibility analysis of use of blockchain considering the challenges and the opportunities determined from the first objective.

The thesis contains a theoretical framework based on two literature studies, where the first provides a general introduction to supply chain, supply chain management and project supply chain management. As the second gives an introduction and an explanation of blockchain technology, from its invention, features, innovations and its evolution. Additionally, five interviews with experienced employees from the value chain of construction projects were conducted, which the determination of challenges and opportunities were based upon.

Six challenges and opportunities were determined through analysis of the interviews;

1. Could contracts and agreements be deployed and stored on a blockchain?
2. Could blockchain be used to build a system of invoicing to ensure to follow the correct agreement, have a nice flow, at the same time does not give away sensitive information, but the customer gets the transparency and the trackability as they desire?
3. Is it possible to deploy certificates and additional information on the blockchain?
4. Could blockchain be used to track material flow, certificates and addition information considering human rights and environmental aspects of the material?

5. Could blockchain be used to enhance information sharing and reduce information silos?

6. Could blockchain be used to integrate and synchronize the systems in the organization?

From the feasibility analysis off these, number 1 and 3 should be easily met, and the deployment and storing of agreements, certificates and information could be done with the use of "smart contracts", but it is suggested to only store data of importance and not big data when using public blockchains. Further, a private blockchain as the Hyperledger Fabric framework could enable and provide the features needed for a system for invoicing given in 2, and further investigation of the opportunity is recommended. Further investigation of the opportunity presented in number 4 is also recommended, but then with a public blockchain. As for both opportunity 5 and 6, the thesis suggests that blockchain might not be the best solution, as traditional databases most likely could provide better solutions.

Sammendrag

Innovasjonen og utviklingen rundt blockchain teknologi er fortsatt i sin spede begynnelse, og opp til nå så har de fleste mulighetene som har blitt undersøkt vært relatert til finans, og hvilke muligheter den kan muliggjøre i andre industrier og markeder er i stor grad ikke utforsket. Et tema som har fått en del oppmerksomhet ved siden av finans, er supply chain. Selv om det er noen prosjekter som jobber med løsninger relatert til supply chain i dag, så har få av dem mye å vise til enda. Denne masteren er en mulighetsundersøkelse om bruk av bruk av blockchain i supply chain, spesielt relatert til prosjekt supply chain vedrørende større byggprosjekter. Masteroppgaven har to hovedmålsetninger, hvor den første er å utrede utfordringer og muligheter i verdikjeden til byggprosjekter, hvor den andre er en mulighetsanalyse om bruk av blockchain relatert til utfordringene og mulighetene utredet fra første hovedmålsetning.

Masteroppgavens teorigrunnlag bygger på to gjennomførte litteraturstudier, hvor det første gir en generell introduksjon om supply chain, supply chain management og project supply chain management. Mens det andre gir en introduksjon og en forklaring av blockchain teknologi, fra dens oppfinnelse, egenskaper, innovasjon og utvikling. I tillegg, så har det blitt gjennomført fem intervjuer med erfarende ansatte fra verdikjeden til byggprosjekter, som utredningene av utfordringer og muligheter hovedsakelig var basert på.

Seks utfordringer og muligheter ble funnet og inkludert gjennom analysen av intervjuene;

1. Kan kontrakter og avtaler legges til og lagres på et blockchain?

2. Kan blockchain bli benyttet til å bygge et system for fakturering for å sørge for at riktig avtale blir fulgt, bidrar med bra flyt, samtidig som det ikke frigjøres sensitiv informasjon, men kundene får den gjennomsiktigheten og den sporbarheten de ønsker?

3. Er det mulig å legge til sertifiseringer og annen informasjon på et blockchain?

4. Kan blockchain benyttes til å spore materialflyt, sertifiseringer og annen informasjon vedrørende menneskerettigheter og miljøaspekter vedrørende materialet?

5. Kan blockchain benyttes til å forbedre informasjonsdeling og redusere informasjonssiloer?

6. Kan blockchain benyttes til å integrere og synkronisere systemene innad i organisasjonen?

Fra mulighetsanalysen av disse, nummer 1 og 2 burde være enkelt møtt, og tilleggelse og lagring av avtaler, sertifiseringer og informasjon kan bli gjort ved bruk av «smart contracts», men det er foreslått å bare lagre data av viktighet når man benytter offentlige blockchains. Videre, et privat blockchain som Hyperledger Fabric kan muliggjøre de egenskapene som trengs for et system for fakturering som gitt i 2, og videre undersøkelser rundt muligheten er anbefalt. Videre undersøkelser rundt muligheten presentert i 4 er også anbefalt, men med et offentlig blockchain. Mens for mulighetene presentert i 5 og 6, antyder masteroppgaven at blockchain kanskje ikke er den beste løsningen, ettersom tradisjonelle databaser mest sannsynlig kan gi like gode om ikke bedre løsninger.

Content

List of Figures

List of Tables

1 | Introduction

The last couple of years the price, speculation and interest around cryptocurrencies have sky-rocked for then to implode and burst from its all time highs. Through the raise of cryptocurrencies strong opinions from a wide range of people from all areas and occupations in society have been expressed. At the extremes you have those that embraces cryptocurrencies both in terms of ideology as well as a technology that would revolutionize and disrupt the financial system as well as countless of other markets and industries, even society and its governess. On the other extreme you have those that means that cryptocurrencies and everything related to it is completely valueless and compare cryptocurrencies to pyramid scams and ponzi schemes. As well as moderate views between these extremes you have those who not necessary are interested in cryptocurrencies directly but they point out that the technology which cryptocurrencies are build upon is of interest and that they would like to investigate which opportunities or improvements this technology could contribute with in different markets and industries.

Blockchains main use as for today is related to digital money and financial markets and financial instruments, but blockchain is also talked about as a potential contributor with new features, opportunities and allowing mutually mistrusted entities to exchange financial value and interact without relying on trusted third parties, in a diversity of other markets and industries. Such as law, accounting, insurance, supply chain, intellectual property rights, customer loyalty, health care, real estate, etc (Ivan Liljeqvist 2018b, Wüst & Gervais 2018). Through the increased price and interest of cryptocurrencies many projects were funded by investors and speculators through ICOs(Initial coin offerings), as well as organizations that started their own projects to look at the opportunities of the use of blockchain. These projects looks at opportunities and solutions where blockchain could be applied in the markets and the industries mentioned, as well as others, but still most of these projects and their development is in the early stages and few of them have much to show for yet.

The innovation of blockchain technology is still in its early stages, thus, which use cases that could utilize the technology is being explored. Of the markets and industries mentioned above supply chain is one of those area that have gotten much attention. As for today there are different teams and projects developing

systems and solution considering different aspects related to supply chain with implementation of blockchain, but as many of the projects related to blockchain these are also in the early development and few of them have much to show for. The scope of supply chain is both big and complex, and as blockchain is still in its early stages of exploration of its use cases there is challenging to determine where implementation and integration of blockchain solution could be valuable.

1.1 Purpose of the study

The purpose of this study is to look at challenges and opportunities related to supply chain and the procurement process for the value chain of construction projects and discuss if blockchain technology could contribute to solve, improve or utilize these, providing addition value or competitive advantage. Thus, this paper aims to contribute to enlighten challenges and opportunities considering this topic that would be interesting to continue to explore, and were blockchain should not be applied.

1.2 Research questions

How to determine which challenges and opportunities to be discussed? As the author of this paper does not have any experience from the industry, other sources of knowledge were needed to determine challenges and opportunities. Thus, experienced employees from different participants of the value chain of the Norwegian construction industry would be interviewed to provide knowledge and experience to determine challenges and opportunities where the value of using blockchain would be discussed.

In addition to the interviews, two literature studies would be conducted. The first literature study consider the topic of supply chain as well as some aspect of project supply chain. Due to the big scope of supply chain and lack of knowing which topics the interviewees would bring up considering their supply chain and their procurement process the literature study includes a general introduction to many of the areas of supply chain and project supply chain. The second literature study conducted consider blockchain technology and aims to give a general introduction of the innovation of blockchain,provide some explanation

of more technical aspects of the use of cryptography, and the development of blockchain as a technology since its innovation. These literature studies would be used as support for the determination of challenges and opportunities from the interviews, and they would provide the foundation of the discussion considering implementation and integration of blockchain to improve or solve the challenges or utilize the opportunities determined from the interviews.

Two research questions were determined considering this paper, which is given below.

1. Determine challenges and opportunities in the value chain of construction projects and its procurement process where blockchain could be of interest based upon interviews conducted with participants from the industry, with support from the literature studies conducted.

2. Look into the challenges and the opportunities determined by the interviews and discuss if blockchain could provide value, desired features or opportunities which would be interesting to look further into, with potentially opportunities of implementation and integration of blockchain.

1.3 Structure of the thesis

The first chapter introduce the topic, the purpose and the research questions for the thesis. The second part outlines the methodology of the thesis, the method used for the two literature reviews conducted, which consider supply chain and blockchain, and the method used to conduct the interviewees and the analysis of them. The third chapter gives a general introduction of the scope of supply chain management as well as some aspect of project supply, and with the forth chapter giving a both technical and general introduction of blockchain technology, providing the theoretical framework for the interviewees and the discussion in the thesis. In chapter five the results and the analysis of the interviewees are presented, which further is used to determine the challenges and the opportunities, answering research question 1. The determined challenges and opportunities from research question 1 is then in chapter six, according to research question 2. The last chapter is a conclusion of the thesis, where the key findings of the study are presented, as well as limitations and further research.

2 | Methodology

This chapter aims to give the reader an overview of the research methods used and the choices made for this thesis, where the first part of the chapter would present relevant theory, as the following chapter would elaborate upon the methods used, the choices made and their conduction.

2.1 Research design

Rajasekar et al. (2006) define research as a logical and systematic search for new and useful information on a particular topic. As Godwill (2015) defines it as: "The process of arriving at dependable solutions to problems through a planned and systematic collection, analysis, and interpretation of data."

2.1.1 Research paradigm

Research methods can follow different paradigms in which it seeks and obtain valid knowledge. The research paradigm depends on ontology and epistemology. Ontology is the philosophical study of the nature of existence or reality, as epistemology describe how we come to know something, how we know the truth or reality (Kivunja & Kuyini 2017). As ontology consider what the nature of reality is, (Kivunja & Kuyini 2017) ask "Is reality of an objective nature, or the result of individual cognition?". (Easterby-Smith et al. 2012) relates it to be a debate between realism and relativism. In addition to the two, he adds the internal realism and nominalism, which all is shown in the table below.

Ontology	Realism	Internal Realism	Relativism	Nominalism
Truth	Single truth.	Truth exists, but is obscure.	There are many 'truths'.	There is no truth.
Facts	Facts exist and can be revealed.	Facts are concrete, but cannot be accessed directly.	Facts depend on viewpoint of observer.	Facts are all human creations.

Table 2.1: Four different ontologies Easterby-Smith et al. (2012)

Epistemology could be categorized as positivism and constructionism. (Easterby-Smith et al. 2012) even categorize them as strong positivism, positivism, constructionism and strong constructionism, and point out that there is a link between epistemology and ontology, which further could be linked up to methodology, which is shown in the table below.

Ontologies	Realism	Internal Realism	Relativism	Nominalism
Epistemology / *Methodology*	Strong Positivism	Positivism	Constructionism	Strong Constructionism
Aims	Discovery	Exposure	Convergence	Invention
Starting points	Hypotheses	Propositions	Questions	Critique
Designs	Experiment	Large surveys; multi-cases	Cases and surveys	Engagement and reflexivity
Data types	Numbers and facts	Numbers and words	Words and numbers	Discourse and experiences
Analysis/ interpretation	Verification/ falsification	Correlation and regression	Triangulation and comparison	Sense-making; understanding
Outcomes	Confirmation of theories	Theory testing and generation	Theory generation	New insights and actions

Table 2.2: Methodological implications of different epistermologies Easterby-Smith et al. (2012)

2.1.2 Research approach

Research approaches can be categorized as a deductive or an inductive approach. Deductive research moves from general theories or questions to specific situations. In deductive research, the objective is to have a clear theoretical position in terms of ideas, questions or theories before collection data, thus collection data to that specific question or problem. Inductive research does move from a particular or a specific situation to infer to broad ideas or theories. In a inductive approach the data gets collected before you state ideas or theories, but through analysis, the data collected provides ideas or theories (Godwill 2015).

2.1.3 Data gathering

Research methods applied can be quantitative or qualitative or even both. Quantitative research is based on the measurement of quantity or volume. Typical quantitative methods are large-scale surveys, questionnaires or experimental studies which provide quantity or collection of numerical data. Qualitative research on the other hand involves quality and experience. Such methods could be focus groups which attempts to get an in-depth opinion of the participants to evaluate certain qualitative values (Godwill 2015, Rajasekar et al. 2006).

2.1.4 Choice of method

The thesis would try to answer the research questions stated with the experience of the interviewees as well as existing research and literature of the topics. Both in the determination of challenges and opportunities and the discussion of potential use of blockchain related to these, there exists many truths, and the facts depend on the viewpoint of the observer, thereby considering the ontologies would be in the realm of relativism. Which align well with the epistemolgies of constructionism as well as strong constructionism as the thesis asks research questions, provides theory generation but at the same time provides understanding and search new insight, see table 2.1 and 2.2.

The two research questions determined for the thesis use different research approaches. As for the first research question use a inductive approach as the data is collected before stating theories or ideas. The data collected through the interviews are then analyzed to determine challenges and opportunities. The second research question use a deductive approach as general theories or question, to more specific. Even though the specific theories or questions to be solved were not determined at the time of the literature reviews were conducted the topic of the theories and questions to be discussed were given. So, it is not a pure traditional deductive approach, but more so than an inductive approach.

The research will be qualitative in terms of two literature reviews and five interviews to gather data, as the reviews is based on existing literature and the interviews are based on the experience of the interviewees.

2.2 Literature study

Considering the topic of the research questions two main literature reviews were conducted. The first main topic were supply chain and project supply chain and the second were blockchain technology.

Literature reviews can vary in form and themes. The terms 'systematic review' is in some cases used loosely, but as the broadest convection, a systematic approach in literature reviews can be distinguished from a narrative literature review by it uses a structured system of inquiry to find and review publications. However, its more commonly used to refer to a specific type of literature review associated with a specific methodology. Literature reviews could be referred to either "systematic reviews" or "narrative reviews" (Margaret Bearman 2012). "It could be helpful to think of two types of narrative review" Margaret Bearman (2012). The first can be referred to as the traditional narrative or critical review, where the collection off and the critical judgment of the literature mostly are done by the author him self. As for the second more as a narrative approach, but with some systematic elements (Margaret Bearman 2012).

2.2.1 Literature review

Due to the author's limited experience and knowledge to the topic reviewed, the features of a systematic review to be an rigour approach ensures a research process that provides an approach to gather most of the relevant literature, while minimizing the risk of bias, providing a transparent study that enable for replication, a systematic literature review were seen suitable (Educational research review. 2006). Even it may unintentionally lead the research to be too objective at the expense of the creativity and other methods of collection of literature (Easterby-Smith et al. 2012). As for the literature review of blockchain, the literature collected from the systematic literature review were not seen sufficient, so additional collection of literature were conducted.

Gough (2007), Director of the EPPI-Centre, describes a nine-phase process for systematic reviews: This process were used as a guideline for the systematic review of supply chain, as well as for the systematic review of blockchain. The first five phases are related to the research of literature and are included for both the reviews in the sections below, then the findings and presentation of the literature is given in chapter 3 and 4.

1. Establishing the review question
2. Defining inclusion and exclusion criteria
3. Articulating the search strategy, including information sources
4. Screening the articles to see if they meet the inclusion and exclusion criteria
5. Reporting the results of the search strategy, usually through a owchart
6. Extracting relevant data from included studies
7. Assessing the methodological quality or rigour of the included studies
8. Synthesising, either quantitatively or qualitatively, the collective evidence of the included studies
9. Drawing conclusions and communicating these ndings in a manner which is relevant to readership.

2.2.2 Systematic literature review of supply chain

1. ***Review question***
   Provide a general introduction of the theory and the scope of supply chain management, project supply chain management and the procurement process in projects.

2. ***Inclusion and exclusion criteria***
   Literature that describes the theory and the scope of supply chain management, project supply management and the procurement process. Only includes literature from databases were the published literature are accepted as academic literature. Exclude literature in other languages than English. Exclude literature older than 2000.

3. ***Search Strategy***
   As part of the search strategy keywords were defined. These were define considering the topic of the review, then used to conduct literature searches on databases as Oria and Google Scholar. The keywords, its combinations, returns of result and the number of used papers to each search are given below in table 2.3. As the results of the literature search below shows there were not used many combinations of "AND", "OR" or other

operators to narrow the search as well as reduce the overall amount of results. As the review question states above, the review aims to provide literature to give a general introduction of the topic. Thus, simple combinations gave the best results according to the inclusion and exclusion criteria, and were seen sufficient.

Keyword	Returns/Database	Accepted
Supply chain	1 999 684 (Oria)	None
Supply chain management	1 220 0620 (Oria)	4
Supply chain management	2 970 000 (Google scholar)	3
Project supply chain management	354 652 (Oria)	3
Project procurement management	241 498 (Oria)	3
Supply chain and procurement	175 624 (Oria)	1

Table 2.3: Keyword and results of literature search

4. ***Screening***
   The keyword searches got a massive amount of results as seen in 2.3, the first screening of potential interesting articles or books were done through alignment of the title with the keywords, as well as the overall inclusion and exclusion criteria. If an article or a book met these requirements a closer look at the article were conducted by first reading the abstract and potential a quick read to determine if the article or the book met the inclusion and exclusion criteria, if it were considered in alignment with the requirements given for the literature it were included as relevant literature.

5. ***Mapping***

   The literature research provided literature which were seen sufficient for the literature review and covers all the areas of interest. The literature of the topic are well established and well anchored in academic research.

   -Kanskje litt tynt det som står over, må eventuelt endre litt på det!

2.2.3 Systematic literature review of blockchain

1. ***Review question***
   To provide an introduction and explanation of blockchain technology, its innovations and the evolution of the technology.

2. ***Inclusion and exclusion criteria***

   Includes literature which describes and explains blockchain technology in general. Includes literature that discuss blockchain and supply chain. Exclude literature that just mentions blockchain without providing understanding of the technology or relation to supply chain. Exclude literature of a deep technical level and detail of specific and narrow topics within blockchain technology. Exclude literature in any other language than English.

3. ***Search Strategy***
   A similar search strategy as for the previous review were adopted but with other keywords. The keywords define, the combination, results and accepted papers are given in the table below.

Keyword	Returns/Database	Accepted
Blockchain	97 000 (Oria)	1
Blockchain	72 300 (Google Scholar)	3
Blockchain technology	30 000(Google Scholar)	1
Blockchain and supply chain	10 800(Oria)	None
Blockchain and supply chain	9 600(Google Scholar)	3
Hyperledger	2 530(Google Scholar)	3

Table 2.4: Keyword and results of literature search for blockchain

4. ***Screening***
   The results with titles which gave indication of being interesting related to the keywords and topic were further checked out. By reading abstract and some overview of the papers, they were either included or excluded according to the inclusion and exclusion criteria given for the review.

5. ***Mapping***

   Some literature were accepted and were of interest considering the topic of the review. That said, the literature that were accepted were not seen sufficient to cover all the areas of the review topic, especially considering literature of blockchain fundamentals and blockchain technology.

Additional literature for the blockchain review

The systematic literature review in the academic databases of Oria and Google Scholar provided interesting and good papers to the review, but it were not seen sufficient.

Blockchain and blockchain technology were not invented in academia, neither did its main innovations. The main development and innovation of blockchain comes from its developer community of open source cooperation and projects. Thus, respected and recognized literature and sources of information from the blockchain community were included to provide sufficient literature to cover the topics of the review. Examples of additional literature included are a book of Andreas Antonopoulos and white papers from well known projects or protocols, with more.

2.3 Empirical data gathering and data analysis

To determine challenges and opportunities according to research question 1 and to be discussed in research question 2, five interviews were conducted with participants from the industry. Thus, providing a practical perspective to enlighten issues, challenges or opportunities in their supply chain and procurement process. The interviews were conducted and transcribed in Norwegian. A qualitative content analysis were done based on the transcribed data text, where the result from the analysis is given in chapter 5. The analysis with the literature studies makes up the foundation for the determination of research question 1.

2.3.1 Semi-structured interviews

A semi-structured approach were applied for the interview, which enables some structure considering the topic to be discussed, but still enables the interviewee to expand on their answers. The approach gives the interview structure in terms of its framework, but still flexibility as the topic list could be followed based on the interviewees responses, and it enables the interviewee to elaborate and communicate their wider views about the topic and questions discussed (Given 2008). As the purpose of the interviews is to provide practical knowledge from the industry it was essential to enable the interviewees to answer openly and elaborate upon the topics. A interview guide stating the purpose of the study

as well as the topics of the interview were sent to the interviewees well before the interviews. The interview guide is included in the appendix.

2.3.2 Participants

The interviews were established through an inquiry sent to some of the biggest contractors in Norway as well as some potentially interesting participants provided by the authors supervisor. Two of the three companies who agreed to participate come from the contacts provided from the supervisor, and only one of the big contractors agreed to participate upon the inquiry.

Of the five interviews conducted, one of the interviewees is a project manager for a electrical contractor, which often is a subcontractor of construction projects. Another is working in the procurement department of one of the biggest Norwegian construction companies. The remaining three interviewees all works for an electrical wholesale company, one considering souring, one in market planning and the last one in the sells department.

The participants represents different actors in the supply chain for construction projects. Which is of importance for the thesis to get the wider picture of how the different actors operate and their view of the construction industry, and the differences in the procurement process and their place in the supply chain. Three interviews with the wholesale company contributed with views from different departments within the organization.

Even though the interviews are conducted with different actors in the industry, which contributes with practical knowledge with different views, there is important to consider the limitations of the interviews. The interviews consist only of three companies which all represents a specific actor in the industry, which means that only one company in the specific sector is interviewed, thus, views from other actors in that part of the supply chain are not included in the paper.

2.3.3 Method of analysis

An conventional content analysis approach were applied as the analysis method on the transcribed data text from the interviews. "Content analysis is a widely used qualitative research technique. Rather than being a single method, current applications of content analysis show three distinct approaches: conventional, directed, or summative." Hsieh & Shannon (2005). The coding categories are

derived directly from the the text data in a conventional approach. With a direct approach, a guidance for initial codes are establish based on a theory or relevant research findings. A summative content analysis involves counting and comparison, usually of keywords or content, with interpretation of the underlying context (Hsieh & Shannon 2005).

The conventional approach were chosen due to the ability to establish the coding categories from the text data. This were suitable as the purpose of the interviews were to provide additional knowledge to the topic through open questions that the interviewees could elaborate upon. Coding as a method and a tool were seen suitable to reduce subjective bias when analysing the interviews, as all related information give about a topic is included and categorised together, reducing subjective favoritism of information where other opinions and data are neglected. Thus, providing a more objective analysis of the data.

2.3.4 Use of coding

Coding could be performed both manually or by use of electronic methods which have enabled innovative research and coding of data of such a size that a manual approach would take an incredible long time or not even doable (Basit 2003). As the author does not have any former experience or skill with electronic methods and software considering coding, a manual approach were seen most suitable as the transcribed data from the interviews of 35 pages were considered manageable.

17 categories were defined through the first round of coding. A merge of related topics were done to reduce the over all number of categories to 6, where the last category is a combination of topics that did not fit in any of the other categories and were not categorized as a category by itself. Each of these 6 categories were than analysed and the results are presented in chapter 5.

2.4 Quality of the research

Below would some aspects related to the quality of the research both in terms of theory and to the thesis.

2.4.1 Reliability

Reliability consider the data related to the paper in terms of who they are used, collection and analysed. Quantitative research requires a high degree of reliability, through well explained description of methods and experiments used which to provide the data, thus enabling others to reconfirm the data by using the same methods and experiments. Which is not as necessary for qualitative research, as the result relies on the subjective interpretation of the researcher (Johannessen et al. 2015). Kvale (2015) on the other hand argues that the degree of objectivity could be increased by following procedures, such as through a interview guide considering interviews. In this thesis the literature studies and the conduction of interviews as well as the analysis of them have been described as detailed as possible, in terms of choices made, methods used and approach.

2.4.2 Validity

Validity consider if the reserach method used actually do research what it is supposed to do. Thus, it consider the validity and credibility of the data collected according to the research questions and purpose of the thesis (Holme 1996). As for this thesis, the transcribed data text from the interviews were not sent back to the interviewees, so they have not been given the opportunity of commenting or alter their statements from the interviews. The transcribed data have not been seen or been validated by any other than the author.

2.4.3 Generalizability

Even though the interviews are conducted with different actors in the industry, which contributes with practical knowledge with different views, there is important to consider the limitations of the interviews. There were only conducted five interviews, from only three companies in the value chain of construction projects. Due to the limited number of conducted interviews there would surly be many challenges and opportunities throughout the industry and its suppliers that are not expressed.

The interviewees are generally not familiar with blockchain technology, so even though they points out different challenges and opportunities there could have been other opportunities which they do not considering due to their limited knowledge of what the technology potentially could provide and enables.

3 | Supply Chain

In this chapter a general introduction to supply chain, supply chain management and project supply chain management. Thus, providing a fundamental understanding of the topic and context for the interviews and the analysis of those, determination of opportunities and challenges, and further discussion considering these opportunities and challenges. A general explanation of the scope were chosen, since the topics brought up through the interviews which determine the challenges and the opportunities were not known at the time of conduction the literature study.

3.1 Supply chain management

3.1.1 Supply chain

Supply chain management is as the name implies, management of a supply chain. Thus, it is necessary to define supply chain first. A supply chain is the link connecting all the processes, activities and networks from point of origin to point of consumption. These handles the flow of goods and services, funds, and information from the upstream suppliers to the downstream customers. Activities could include sourcing of raw materials and parts, manufacturing, producing, assembling, storing, ordering, tracing, and distribution and delivery to customers, where the final customer is the driving force and the primary purpose of the existence of a supply chain. Therefor, meeting the customers demand is the primary objective. and design and decisions are indirectly or directly related to this objective (Sople 2012, Sanders 2012)

Council of Supply Chain Management Professionals operates with two definitions of supply chain:

1. *Starting with unprocessed raw materials and ending with the final customer using the finished goods, the supply chain links many companies together.*

2. *The material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers and customers are links in the supply chain.*

According to (Mentzer et al. 2001), there seems to be a wider consensus considering the definition of a supply chain compared with the definition of supply chain management. An in their paper they defined a supply chain as: *a set of three or more entities (organizations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer.*

Supply chains are not all alike, (Mentzer et al. 2001) identifies three degrees of complexity: Direct supply chain, extended supply chain and ultimate supply chain. See figure 3.1, below. A direct supply chain consist of a company, a supplier and a customer involved in upstream and/or downstream flows of goods and services, funds, and information. An extended supply chain is a direct supply chain extended to include all suppliers immediate suppliers and customers immediate customer, all involved in the flows of goods and services, funds, and information. "An ultimate supply chain includes all the organizations involved in all the upstream and downstream flows of products, services, finances, and information from the ultimate supplier to the ultimate customer." (Mentzer et al. 2001). (Sople 2012) does not mention ultimate supply chain, but rather includes it as a variation of complexity in the extended supply chain. An important aspect is that the final customer are included in the supply chain. Thus, a retailer are involved in both upstream and downstream flows.

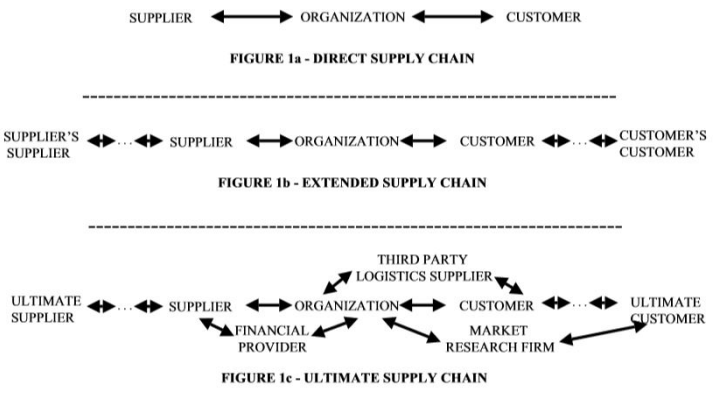

Figure 3.1: Types of Supply Chains (Mentzer et al. 2001)

3.1.2 Supply chain networks

As seen in 3.1, ultimate supply chain can reach a high degree of complexity when including all organizations involved, which could be third parties related to logistics, financial, risk, etc. In addition to this, a company could be part of many supply chains, making cross networks. As retailers which are involved in the sales of many different products from different supply chains, and in addition: "AT&T might find Motorola to be a customer in one supply chain, a partner in another, a supplier in a third, and a competitor in a fourth supply chain."(Mentzer et al. 2001), this example illustrates the complexity that could accrue when multiple supply chains interacts, which explains the network nature that many supply chains possess. (Mentzer et al. 2001)

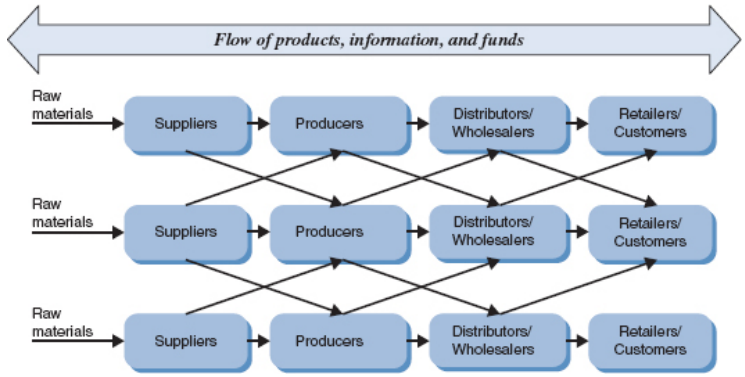

Figure 3.2: Cross networks (Sanders 2012)

3.1.3 Defining supply chain management

Supply chain management is a systematic and strategic coordination of all business functions and processes related to supply chain both within the company and across businesses, thereby improving the long-term performance of the companies and the supply chain (Sople 2012). Mentzer et al. (2001) points out that the term supply chain management historically have had many definitions, therefor they attempted to find a common definition from the literature. Their attempt of a definition:

The systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across

businesses within the supply chain, for the purposes of improving the long-term performance of the individual companies and the supply chain as a whole.

The council of Supply Chain Management Professionals defines Supply Chain Management as following:

Supply chain management encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers. In essence, supply chain management integrates supply and demand management within and across companies.

3.1.4 Supply chain integration

Enterprises today are not necessary competing against another, rather it is one supply chain competing with another supply chain. Thus, the integration of the enterprises involved in the supply chain is of great importance(Sople 2012). Integration are both intra-Oranizational and inter-organizational which bot are essential for a competitive supply chain. "For an organization to be effectively integrated with other members of its supply chain, it must have internal coordination." (Sanders 2012). Therefor, some important aspect of them would be included, starting with some of the main intra-organizational functions, Marketing, Operations, Logistics, and Sourcing.

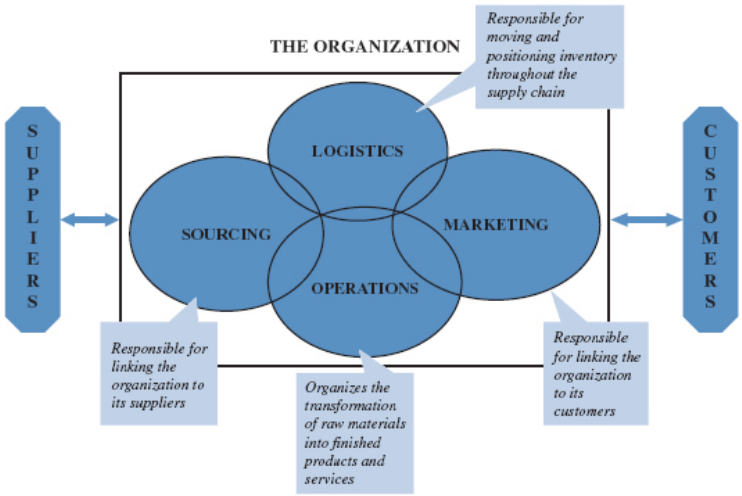

Figure 3.3: Enterprise functions (Sanders 2012)

3.1.5 Marketing

Marketing is the intra-Organizational function which links companies with its customers and downstream supply chain. "It is responsible for identifying customer needs, determining how to create value for customers, and building strong customer relationships." Sanders (2012). Thus, the information provided by marketing has critical importance for the entire organization which has to adapt to customers demand considering time, dependability, communication and convenience. The marketing function has evolved since the 1970's when the main goal were to increase sales, thereby increasing revenue and profit. Competing purely on price is often not sufficient in today's markets, therefor marketing has transformed to include different services related to the customers needs to create value for final customers, which is the main objective of a supply chain. Marketing is responsible of identify customers needs which could become rather complex and vary widely from customer to customer. Some might not even know what they want.

Customers needs could be categorized into three: basic needs, performance needs, and excitement needs. Basic needs are what the customers expects as a minimum and would be extremely dissatisfied if not met. Performance needs

difference one product/service from its competitor and the customer are delighted the better it performs. Excitement needs are performances or aspects with the product/service that customers did not expect but increased their delightment of the product/service. Sales information and customer satisfaction information related to aspects of a product or a service are therefor of great importance to increase value for the final customer, without using unnecessary resources at product aspects or services that does not increase or brings added value for the final customer, thus, increasing total cost (Sanders 2012).

Distribution channels

Distribution channels are of great importance to meet customers needs, expectations and increase satisfaction. Distribution decisions has to be align with customers needs, so service level and satisfaction would be optimized considering cost. Therefor, distribution decisions considering amount, position of Wholesaler, retail, inventory etc, should be determined by customer needs and cost (Sople 2012).

3.1.6 Operations

Operations relates to the production of goods and services within a company in an efficient and cost-effective way. Operations' function is to transform input from suppliers to create goods and services with its available resources as people, equipment, technology, materials and information. In addition to the flow of goods and services flowing downstream from suppliers to operations they also get a flow of information both from suppliers and marketing(upstream flow), which could effect the operations in terms of production output, what to produce, and services to provide (Sanders 2012).

Operations has to determine its production based on which products to produce, services, design, amount, need of customization, need of flexibility with more, often provided by marketing. At the same time the operation function has to have a close communication considering its capabilities and limitations with marketing. Operations must also work close with sourcing to determine material availability, as source of supply, and quality standards, as well as provide sourcing with advocate information to secure consistent supply Sanders (2012).

Product decisions and facility layout are important decisions for being as efficient

and effective as possible, thereby contributing to competitive advantage for the supply chain. These decisions should be align with the overall strategy of the company and based upon all available information to increase value (Sanders 2012).

3.1.7 Sourcing

"Souring is the business function responsible for all activities and processes required to purchase goods and services from suppliers." Sanders (2012). As marketing is the link connecting the company to the downstream supply chain, sourcing is the link connecting the organization to the upstream part of the supply chain. As corporations have turned increasingly towards international sources of supply to look for more efficient and effective coordination of flow of material and services, the sourcing strategy has become increasingly important. Strategic sourcing to build closer relationships with suppliers has been an important aspect considering cost and supply availability (Mentzer et al. 2001).

3.1.8 Logistics

(Asbjørnslett 2003) brings up the danger of presenting supply chain management as the integration of business processes, due to the the origin of supply chain management from the need of integrate business processes to logistics management. Thus, SCM has evolved from logistic management, thereby inherited all aspects of inter-organizational management. The Council of Supply Chain Management Professionals(CSCMP), former The Council of Logistics Management, did in 1998 redefined logistics as part of the SCM. CSCMP defines Logisitics as:

Logistics management is that part of supply chain management that plans, implements, and controls the efficient, effective forward and reverses flow and storage of goods, services and related information between the point of origin and the point of consumption in order to meet customers' requirements.

In addition CSCMP define Logistics Management, considering boundaries and relationships as:
Logistics management activities typically include inbound and outbound transportation management, fleet management, warehousing, materials handling, order fulfillment, logistics network design, inventory management, supply/demand planning, and management of third party logistics services providers. To varying

degrees, the logistics function also includes sourcing and procurement, production planning and scheduling, packaging and assembly, and customer service. It is involved in all levels of planning and execution–strategic, operational and tactical. Logistics management is an integrating function, which coordinates and optimizes all logistics activities, as well as integrates logistics activities with other functions including marketing, sales manufacturing, finance, and information technology.

According to Sople (2012), the key elements of effective logistics includes: product movement, information movement, time and service, cost, and internal integration. Thus, logistics are an important intra-organizational function to integrate internal activities, as well as an essential activity to integrate involved organizations across the supply chain.

3.1.9 Antecedents to SCM

Antecedents to SCM are according to Mentzer et al. (2001) the factors that enhance or embed the implementations of supply chain orientation, which are a systemic and strategic view that enables implementation of supply chain management. As seen in the figure below, Mentzer et al. (2001) point out that the willingness to address trust, commitment, interdependence, organizational compatibility, vision, key processes, leader, and top management support as company antecedents to SCM.

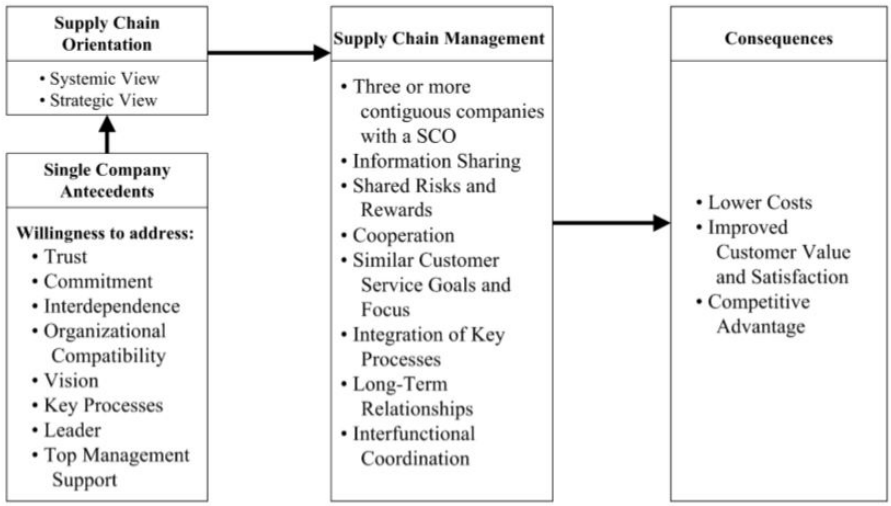

Figure 3.4: Antecedents and SCM activities (Mentzer et al. 2001)

3.1.10 SCM activities and processes

According to Sople (2012), a company can not survive in today's competitive world without the help of its suppliers and their co-operations. Thus, the process of coordinating goods and services, information, and funds across the supply chain becomes essential for the supply chain's competitive advantage, thereby the company's success. Inter-organizational integration is a key aspect of enable the benefits from a well working supply chain. Some SCM activities and processes are shown in figure 3.4 above. Some of them would be described shortly below as others would be explain through the section.

-Coordination:
SCM involves coordination of goods and services both upstream and downstream, this also includes the reverse supply chain, as well as the coordination of the flow of funds related to goods and services, and coordination of various financial arrangements between buyers and suppliers (Sanders 2012).

-Information Sharing:
SCM requires information sharing across the supply chain to increase perfor-

mance related to demand and sales forecasts, production planning, inventory levels, etc. Sharing information enables the entire chain to work in unison and develop more precis forecasts thereby reducing the uncertainty through the supply chain. Thus, reducing the well known Bull-Wipe effect, where the uncertainty of demand increases the further upstream in the supply chain you get. The willingness to make strategic and tactical data available for other participants in the supply chain will further enhance performance (Sanders 2012, Mentzer et al. 2001).

-Cooperation:
SCM requires cooperation across the supply chain businesses to jointly plan, operate, and execute business decisions as one entity. Better collaboration and an align strategy could result in cost cut opportunities and reduce the risks and uncertainties related to unexpected costs. Thus, improving the supply chain as a whole (Sanders 2012).

-Integration of key processes:
"The implementation of SMC needs the Integration of processes from sourcing, operations, logistics, and to distribution across the supply chain."Mentzer et al. (2001).

3.1.11 Competitive supply chain

Competitive advantage refers to activities or processes that a supply chain executes that gives an advantage compered to its competitor's supply chains. According to Sanders (2012), seeking a sustainable competitive advantage has become a top business concern. Competitive advantage can according to them result from two aspects. The first is cost or productivity advantage, where the advantage comes from offering the lowest cost of goods or services, and the second is value advantage, where the advantage comes from providing goods or services with the greatest perceived differential value compared with its competitors.

Cost-productivity advantage can be achieved and improved in several ways, some could be through economic of scale, experience curve, SCM activities and processes, as reduced cost related to coordination, etc. Value advantage on the other hand are much more complex when the value are not determinate by price, but rather the benefits and value provided by the goods and services (Sanders 2012). Time, quality, innovation, reputation, service, responsiveness, reliability,

relationship, security and much more are examples of contributing factors in creating value advantage.

3.1.12 Decisions in supply chain

Ensuring customer satisfaction and optimizing customer value through the supply chain should be the main focus. "To deliver customer value, organizations need to focus on innovation, quality in product and service, maximum utilization of available resources, skill sets of the employees and infrastructure to create the value." Sople (2012). Designing supply chain networks and decisions considering supply chain management are important aspects in optimizing customer value through the supply chain. Increased customer value could be accomplished considering cost, time, quality, service, with more. So why not compete on all dimensions? The issue is trade-offs between different factors. Example, a supply chain can increasing customer value with improving service level and time to marked through flexibility and customization, however, this would increase the cost of production and assembly. Thus, the decisions considering supply chain and design of the supply chain network should be based upon the competitive strategy in service offerings to customers. The competitive strategy should then determine the design of the supply chain network, vendors, production, inventory, distribution, with more.

3.1.13 Supply chain relationship management

As supply chains consists of a series of partnerships, SCM requires partners to build and maintain long-term relationships, which is of great importance for successful integration of SCM activities and processes. Cooperation among the supply chain members is required for effective SCM. Cooperation depends upon trust and willingness from the participants, which could be achieved through long-term relationships. Risk and reward sharing is important for long-term focus and cooperation, and should not be neglected to maintain good relationships (Mentzer et al. 2001).

There is important to acknowledge that all supply chain relationships are not of equal importance. Some members of the supply chain are not of critical importance for the company and the supply chain, and could easily be purchased or potentially solved through contracts. Members that is of critical importance for the company and the competitiveness of the supply chain requires greater attention, and building long-term relationships through partnerships or alliances

could enhance performance. (Sanders 2012)

3.1.14 Sustainable supply chain management

Sustainable supply chain management(SSCM) or green supply chain management, has gotten increased focus in the last decades. The goal is by increasing the focus considering sustainability in supply chain management to reduce environmental and social impact, and not compromising the ability of future generations (Sanders 2012). Paulraj et al. (2017) point out that some researches argues that socially responsible initiatives, such as SSCM, can result in additional costs which then can give firms a competitive disadvantage. They adds that in contrast there are an increasing number of studies that have found positive relationships between environmental responsiveness and performance. Srivastava (2007) supports the statement of the potential opportunities related to SSCM. "Green supply chain management can reduce the ecological impact of industrial activity without sacricing quality, cost, reliability, performance or energy utilization efciency. It involves a paradigm shift, going from end-of-pipe control to meet environmental regulations to the situation of not only minimizing ecological damage, but also leading to overall economic prot. The area throws various challenges to practitioners, academicians and researchers."

Paulraj et al. (2017) examined the links between corporate motives, SSCM pratices, and firm performance. Using a sample of 259 supply chain firms in Germany they found: "Findings of this study contribute to multiple literature researches espousing corporate sustainability and business ethics. This research reveals that moral motives can be a much stronger driver than instrumental motives, and that rms exhibiting a high level of moral concerns for the environment tend to outperform those mainly driven by amoral considerations."

3.2 Project supply chain management

Most of the conducted research and development considering supply chain management have been focused on repetitive and continuous industries and businesses. "Conversely, project industries substantially differ from the stable and continuous supply chains within “goods and service” sectors for a number of specific characteristics: the high complexity and uncertainty in which the production system operates, the transitory site configuration managed by tempo-

rary supply chain network, the high customer influence on the final product, the process fragmentation, and the complex network of stakeholders, which involves multiple organizations and relationships." Aloini et al. (2015). These with a number of cultural factors are some of the rooting causes of the failure to replicate the positive experiences with SCM in other sectors (Aloini et al. 2015). Still, SCM is of importance as the supply chain is the competitive entity. Despite the challenges considering these differences between project based environments and stable and continuous supply chains, there will be a continuous search to enhance "value added", both through cost reduction and improved income (Asbjørnslett 2003).

"The principles of project supply chain management is outlined to be the basis for developing the key describing characteristics of logistics and supply chain management within the project context.The underlying assumptions for the principles is the notion of the project as a business opportunity, with the project supply chains as a competitive entity that may enhance the value of the project, i.e. the business opportunity." Asbjørnslett (2003).

3.2.1 Characteristics

Asbjørnslett (2003) points out five different characteristics that should be of importance for project supply chain management. The first is about project life cycle, and the importance to be aware of the different needs of the two project phases, development and operations. Second consider the supply chain, where development is a one-of-a-kind, as operations are more a repetitive process. Third consider logistics drivers, where development are characterized as a demand chain management and operations at supply chain management. Fourth considering Organizational processes, characterized by agile characteristics in the development phase and lean characteristics in the operations phase. The last looks at service quality, as resilient is of importance for the development phase and robust for the operations phase.

3.2.2 Complexity of projects

In the context of a major project, supply chain can be linear or non-linear. It is considered linear when a material, product or service is sourced from a single supplier, which is more common in the operations management. In a project supply chain a major contractor usually have several subcontracts which again

could have several subcontractors themselves and the process becomes non-linear. Compered with a linear supply chain with defined suppliers and subcontractors performing as specified, the complexity of non-linear supply chains increases the risks of lack of supplier commitment, poor order control, unexpected variations in lead time, and changes induced by suppliers and project members. These non-linear project risks have the potential to generate cumulative negative influences across the project (Basu 2011). The main contractor, subcontractors and sub-subcontractors are themselves often part as customers or suppliers of extended supply chains with more repetitive operations, which further increases the overall complexity of project supply chain networks. In addition, since projects have a defined start and an ending, every new project would have to establish new project supply chains, which does not enable the same opportunity of improving the supply chain over time, as companies with continuous supply chains could. Thus, projects does to a large degree depend on experience to set up their supply chains from the beginning of each project, which could be difficult since every project is different.

3.2.3 Project procurement management

The project procurement management has an huge impact upon the project supply chain. "the NORSOK Collaboration Panel's acknowledgement of the '[inter-organisational] procurement processes as the most important processes among operator, contractors and suppliers'." Asbjørnslett (2003). As the project procurement management processes involve agreements, including contracts and legal documents, these establishes the terms and conditions for the life cycle of the project. Thus, establishing the foundation of the supply chain and the cooperation among the participants through the supply chain. In addition these processes would greatly affect relationships, and could lead to long-term relationships and potential partnerships or alliances (Inc. 2013).

3.2.4 Antecedents in PSCM

Due to the differences between projects and continuous operations, the antecedents would also potentially be different. Aloini et al. (2015) address's a research gap considering antecedents for project supply chain management. Therefor, they aimed to identify the key antecedents of SCM in project-based environment. From isolating a set of 16 antecedents from former SCM research, they analyzed and tested their practical relevance. "The independent connotation of "super-ordinate goals" emphasizes the criticality to achieve com-

mitment and common objectives among project participants, motivating and driving the introduction of the SCM practices. The autonomous factors included in the "rules and procedures — accessibility" cluster represent the formal and technological basis to achieve the dependent antecedents within the "cross-organizational cooperation" cluster. Finally, "cross-organizational cooperation" stresses the importance of sharing of risks and benefits between SC participants as the final (dependent) antecedent to successfully implement SCM practices." Aloini et al. (2015).

3.3 Systems

As SCM consider management of flows of goods and services, information and funds. Systems that enables management of this flows, as tracking, planning, communication, sharing of information, and transfer of funds, makes up the backbone of successful SCM and a competitive supply chain. Many of these systems are build upon information technology(IT), and through this section some elements of the IT systems and what they enables would be described.
Decision support systems(DSS), is an interactive software-based system intended to help decision-makers with useful information from any collection of data to identify and solve problems. In supply chains these DSS are essential in terms of being an information source that helps decision-making consider supply chain plans and strategies. DSS enables control over flows of goods and services, and funds through the supply chain, and consists of a number of systems, tools and technologies, as enterprise resource planning(ERP), distribution resource planning(DRP), EDI, GIS, GPS data, RFID, data warehousing, etc (Sople 2012).

The data warehouse is the company's database which stores all the data and the information that the company and the rest of the supply chain relies upon. The DSS depends on a continuously flow of information from both upstream and downstream to keep updated. To be able to handle the continuous flow of information a communication system is required. Information systems build upon Internet has enabled communication systems required for the flow of information needed for the DSS, the company and the supply chain, which are efficient, effective, at a low cost, and fast (Sople 2012).

3.3.1 Enterprise resource planning(ERP)

"ERP systems provide a single up-to-date database incorporating manufacturing, finance and human resource applications extended to include the tracking of orders and inwards goods, work in progress and the delivery of finished goods. The system is accessible to all departments for the planning and execution of supply chain activities. Thus enterprise resources planning systems integrate (or attempt to integrate) all data and processes of an organization into a single unified system in order to achieve integration." Basu (2011). These large software programs are used for utilization, planning and coordination, and allows for data sharing and communication with the rest of the supply chain. Thus, ERP becomes a useful system for optimization of the supply chain and contributing in the search of competitive advantage.

3.3.2 New business models

Up to now we have seen how IT as a technology, enables systems which enhance performance and integration through the supply chain. In addition, IT and especially internet enabled a range of new business models and the opportunities of interacting with customers in a way never been possible before. Many of the worlds biggest companies today are build on business models enabled through IT and the use of internet. The availability and the speed of internet, and the scalability, effectiveness, efficiency, etc with software has shown its capabilities (Sople 2012). There would be interesting to see if new models of supply chains would develop based on the new opportunities that IT and new innovations would enables.

In this chapter a general introduction and explanation of supply chain, the scope of supply chain management and project supply chain management have been conducted, as well as a introduction of some of the systems applied as support. Being one of the two literature studies providing the theoretical framework for the thesis. The other literature study considering blockchain would be presented in the next chapter.

4 | Blockchain

Blockchain is a relative new technology that has become some of the latest buzzwords with increased publicity for its potential opportunities and its attachment to cryptocurrency, digital money. In this chapter an introduction and explanation of blockchain technology would be given to establish a general understanding of the technology, and of its innovations and features. The chapter would take you from the innovation of blockchain and through its evolution towards new protocols and features. Some parts of the chapter could be a bit technical, especially related to the explanation of cryptography, but it is seen meaningful as cryptography is of such an importance for blockchain technology. This chapter with the previous chapter would provide the theoretical framework for this paper.

4.1 What is blockchain

The innovation of blockchain came with the innovation of the bitcoin protocol by "Satoshi Nakamoto", an alias. Where the blockchain provides
It all started in 2008 with the white paper of the bitcoin protocol, by "Satoshi Nakamoto", an alias, which still is unknown (Nakamoto 2008). One of the main innovations of the bitcoin protocol were the innovation of blockchain. So to provide an introduction and an explanation of blockchain, this paper would start explaining the blockchain through the bitcoin protocol, before following the evolution of blockchain technology. But first, a couple of explanations of blockchain is provided below, as well as a section of cryptography, due to its importance for blockchain technology.

Don and Alex Tapscott explains blockcain as:
"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value"

And Hyperledger (2017):
"In general terms, a blockchain is an immutable transaction ledger, maintained within a distributed network of peer nodes. These nodes each maintain a copy of the ledger by applying transactions that have been validated by a consensus

protocol, grouped into blocks that include a hash that bind each block to the preceding block."

4.2 Cryptography

Before looking at blockchain in bitcoin we need to explain the use of cryptography, which bitcoin and blockchain relies on. Bitcoin use both hash functions and digital signatures. "These mathematical functions are practically irreversible, meaning that they are easy to calculate in one direction and infeasible to calculate in the opposite direction." Antonopoulos (2014). These enables the creation of digital secrets and unforgeable digital signatures (Antonopoulos 2014).

4.2.1 Hash functions

A hash function is a mathematical function with the following three properties:

- Its input can be any string of any size.
- It produces a fixed size output.
- It is efficiently commutable.

It is required that for a hash function to be cryptographically secure it has the following three additional properties:
Collision-resistance: A collision occurs when two distinct inputs produce the same output.
Hiding:Hiding asserts that if given the output of the has function y=H(x), there is no feasible way to figure out what x, was.
Puzzle-friendliness: If a part of the input are suitable random, it is very difficult to find another input that gives the same output. (Arvind Narayanan 2016)

Secure Hash Algorithm 256(SHA256), is the hash function primary used in bitcoin. This hash function can take any length of string as input and returns a 256 bits hash. A collision are theoretical possible, due to the fixed possible outputs of 2^{256}, but with none constraints of inputs, you could do $2^{256} + 1$ distinct inputs, where at least two of these inputs would get the same output, thereby an collision. Even though it is theoretical possible, it is not in practice, with an average of 2^{128} computations to find a collision. "If every computer ever made by humanity was computing since the beginning of the entire universe, up to now, the odds that they would have found a collision is still infinitesimally small.

So small that it's way less than the odds that the Earth will be destroyed by a giant meteor in the next two seconds." Arvind Narayanan (2016). As seen, this hash function is quite secure, and it meets all requirements mentioned above (Arvind Narayanan 2016).

4.2.2 Digital signatures

"We desire two properties from digital signatures that correspond well to the handwritten signature analogy. Firstly, only you can make your signature, but anyone who sees it can verify that it's valid. Secondly, we want the signature to be tied to a particular document so that the signature cannot be used to indicate your agreement or endorsement of a different document." Arvind Narayanan (2016). Bitcoin use Public key cryptography to create a key pair to enable these properties. The key pair consist of a private key and a unique public key derived from the private key. The private key can be used to generate digital signatures for messages or documents. The public key can then validate if the signature is truly sign with the private key without reviling the private key. Such key pairs are used in Bitcoin and possible due to Bitcoin's use of elliptic curve multiplication, a one-way cryptographic function, to generate the public key from the private key. Due to the extreme difficulty of getting back to the private key from the public key, the public key can be shared in public and used to receive bitcoin, more of that later (Antonopoulos 2014).

The figure below illustrates the relationships and generation of a public key and a bitcoin address. The first step is to get a random private key of size 256 bit. There exists different methods of creating secure and random private keys, as calculations determinate by entropy from you moving your mouse. Then generating the public key using the private key as input in the elliptic curve multiplication function. The public key is 512 bits, but can easily be compressed to 257 bits. Thus, we have a key-pair with the properties described above. The public key are used as input in a SHA256 hash function, where the result are used in a RIPEMD160 hash function, which produces the bitcoin address of size 160 bits. It is the bitcoin address which is used to receive bitcoin transactions, but addresses are almost always presented to users in an encoded called "Base58Check", which uses 58 characters with an additional checksum for readability and security. Like this, "19j3z5LpmMGB1tPeNruPghH8Sf47t9cPw6", which is a bitcoin address that received bitcoin in block 547425 (Antonopoulos 2014).

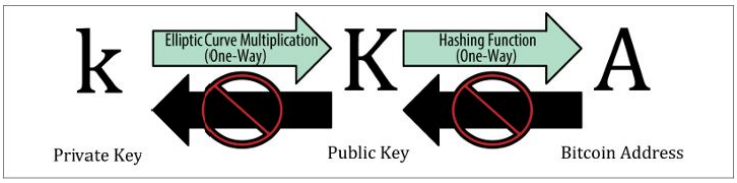

Figure 4.1: The link between a private key, a public key and a bitcoin address (Antonopoulos 2014)

4.3 Design of a blockchain

At the fundamental level a blockchain is a data structure, an ordered, back-linked list of blocks of transactions. Blocks are linked by referring to the previous block in the chain. Thus, the name blockchain, which often visualized as a vertical stack, where blocks are stacks on top of each other with the first block(genesis block) serving as the foundation of the stack. Due to this, the name height is used to address a blocks position in the blockchain Antonopoulos (2014).

4.4 Blocks

A block consist of a block header, containing metadata, and a list of transactions. The first metadata in the block header is a reference to the previous block hash, see figure 4.3. Further the block header contain the metadata; difficulty, timestamp, and nonce, related to mining operation, which would be explained later. The last metadata is the Merkle tree root of the included transactions in the block (Antonopoulos 2014).

A Merkle tree is a binary tree build of hash pointers. The tree is build from bottom up, where the transactions are sorted and hashed, which makes up the foundation of the data structure in the use of Merkle trees in Bitcoin. These transaction hashes are paired in blocks of two and two, and hashed, which makes up the next level of the tree. The process is repeated until a single block is reached, the root of the tree (Arvind Narayanan 2016). To the left in figure 4.2 an illustration of the Merkle tree is shown. To the right in the figure you could see that if some information in the transaction is changed, its hash would also change, and the Merkle tree does not match any more, which would change the

Merkle tree root if calculated. "Merkle trees are used in Bitcoin to summarize all the transactions in a block, producing an overall digital fingerprint of the entire set of transactions, providing a very efficient process to verify whether a transaction is included in a block."Antonopoulos (2014). The purpose of the Merkle tree is to be able to only downloading the block headers and still be assure that all of the data is correct (Buterin 2013).

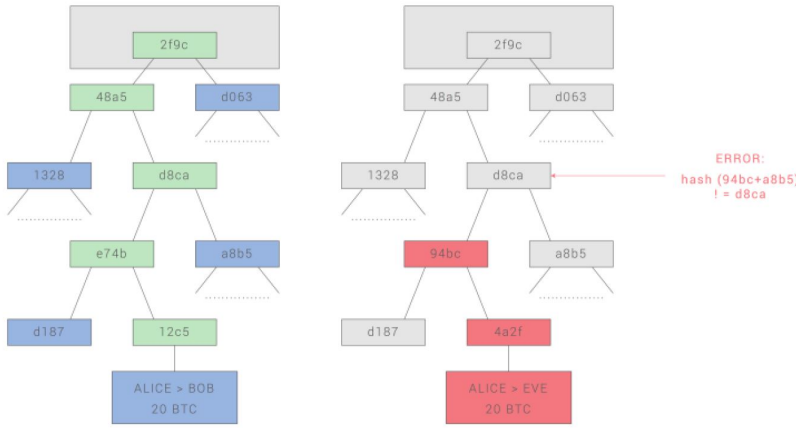

Figure 4.2: *Merkle Tree (Buterin 2013)*

The metadata in the block header is hashed through the SHA256 algorithm twice, and the hash is the primary identifier of the block, a digital fingerprint Antonopoulos (2014). Any change of metadata would change the block hash, so it is easy to validate if a block has been changed. Because any change at all to the transactions would change the Merkle tree root, it would be sufficient to validate the block hash to assure the correctness of the data. Since a block also includes the previous block hash, any changes of the previous block would also change this particular block. Any block since the genesis block has referred to the previous block, and a change in a specific block requires to re-do all the hashing in the following blocks as for the chain to remain valid. This is essential for the security of blockchains and would be further explained in the next section.

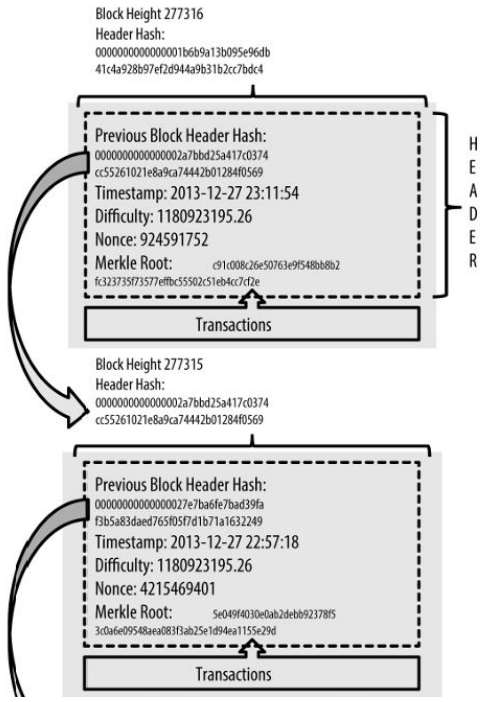

Figure 4.3: *Linking blocks and its metadata (Antonopoulos 2014)*

4.5 Consensus

Bitcoin is not run by a centralized entity or a government, instead it is a network of decentralized nodes. Nodes download and holed the entire blockchain, so, all blocks and all their transactions. In contrast to centralized systems, no permission is needed to run a node, and you can do so from your computer. So, how could a permissionless and decentralized network of nodes without a centralized party agree and trust the chain of blocks. It is done by following agreed rules for the network, consensus algorithm which provide consensus through the network by nodes validating transactions and blocks being in alignment with the rules. The six steps below by Satoshi Nakamoto in (Nakamoto 2008), the original Bitcoin document(white paper), which explains the idea of Bitcoin's consensus algorithm. In addition there is further criteria considering the con-

sensus algorithm as the format of a valid transaction, valid block size and a range of other criteria and rules agreed upon by the network which works as the consensus algorithm.

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

As for today, nodes that does not only validating blocks but also do computation calculations in their effort of creating new blocks are refereed to as miners. Every node could become a miner, but it cases electricity cost and requires capital heavy hardware to be financial profitable, due to the proof-of-work algorithm mentioned in step 3 and 4. In addition there is different light-nodes, these do not contribute in the process of creating and validating blocks, and does only includes block headers and the transactions of interest for the specific light-node. It is often used in Simplified Payment Verification software, which helps set up transactions in a valid matter before broadcasting them to the network (Ivan Liljeqvist 2018b).

4.5.1 Proof-of-work and incentives

In the previous section the block header where introduced, and a digital fingerprint of the block is made by hashing the block headers metadata, which consist of the previous block hash, the mining meta data; timestamp, difficulty and nonce, and the merkle tree root. To enable trust and consensus the proof of work algorithm were implemented. The idea behind the proof of work algorithm is that the block hash must be less than a dynamically adjusted target as a criteria for being validated and accepted by the other nodes. Thus, making

creation of new blocks computationally hard, thereby prevention sybil attackers from remaking the entire blockchain in their favor. Because SHA256 is a one way and completely unpredictable pseudorandom function, the only way to satisfy the target criteria is simply trial and error. Miners could keep hashing by changing the nonce until they or any other miner has found a suitable hash, thus creating a new block and the process repeats (Buterin 2013).

The difficulty in the metadata determines the target for the hash, and it is recalculated by the network every 2016 blocks so new blocks should be created on average every ten minutes. Thus, if the total hashing(computational) power of the network increases, the difficulty would be increases, as well as decreased if the overall hashing power decreases (Buterin 2013).

The implementation of a timestamp was Satoshi Nakamoto's solution of which proves that the data must have existed at the time. Thus, dealing with the issue of people double spending their coins, which is when a owner of some bitcoins tries to sign and include their bitcoins twice, thereby double spending their coins. The timestamp enable participants to agree on a single history of the order in which transactions arrived first, where the first transaction is the one that counts and all attempts of using the same bitcoin is invalid (Nakamoto 2008).

There is no permissions needed to mine bitcoin, those there is no opportunities to punish unfaithful miners, instead there is incentives mechanisms which rewards honest miners playing by the rules, thereby it is in the miners own interest to play by the rules. In any new block mined the creator of that block are allowed to make a reward transaction to an address of their choice. The reward are now at 12.5 bitcoins and the reward is halved every 210 000 blocks, which is approximately ever fourth year. This is new mined bitcoins and the only way of issuing new coins, thus, due to the reduction of rewards every fourth year the total amount of bitcoins that ever would be created is 20,999,999.9769, approximately in 2140. In addition the creator of the block also collect the transaction fees (Arvind Narayanan 2016).

According to step 6 by Satoshi Nakamoto, other miners would if a block is valid continue to mine new blocks using that hash as input in their effort to make new valid blocks, thereby increasing the length of that blockchain. If a miner behave dishonest and create a favorable block with the correct target criteria other miners would see this and would not continue working on this chain, with

the result of the block created of the dishonest miner would not be part of the consensus blockchain. Thus, losing the reward for its effort and cost related to hardware and electricity to find that block. Thus, it is in the miners own interest to play by the rules, so blocks created by the miner is accepted and becomes a part of the consensus blockchain.

"Mining is the invention that makes bitcoin special, a decentralized security mechanism that is the basis for peer-to-peer digital cash. The reward of newly minted coins and transaction fees is an incentive scheme that aligns the actions of miners with the security of the network, while simultaneously implementing the monetary supply."Antonopoulos (2014)

The 51 percent attack is when someone by having more than 50 percent of the hashing power could modify blocks in their favor and still out compete the honest nodes. "To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes." Nakamoto (2008). Thus, more blocks that have been mined after a transaction, confirmations, the more secure, due to all the rework that has to be done for it not to be part of the consensus blockchain. As the longest chain is accepted as the valid chain.

4.6 Forks

The distribution of information through the network is not instant, so if miner A finds a valid hash, but before miner B receive the new broadcaster block, miner B also finds a valid hash and he also starts broadcasting his valid block. In this case different miners would have received the block from A first, and others the block from B. Both blocks are valid and the miners would start mining using the hash from the valid block they received the first. Thus, there is two different copies of the blockchain, which is a fork, which occurs whenever there are two candidate blocks competing to form the longest blockchain. This is resolved when a miner C, which randomly received block B first finds a new valid block and broadcasts this to the network. Due to the consensus algorithm the longest chain, or more precis, the nodes all selects the longest cumulative difficulty chain. Thus, all miners receiving block C would see that the chain with B-C is the longest and would therefor start working on this chain, which then becomes the main chain. Since B-C is the longest and have solved the most difficult computation, no one would continue working on block A, and block A

becomes an "orphan" (Antonopoulos 2014).

Occasionally some from the network would like to make changes to the protocol, to update and or enable new features. Since the bitcoin protocol is a decentralized protocol, you could not force every node to update. It is common to differentiate between two different upgrades, a hard fork and a soft fork. A hard fork is related to changes to the protocol that changes the validating rules of blocks, the consensus algorithm. If every node in the network upgrades, there would be no issue, but if some nodes do upgrade and some does not, a hard fork could lead to a split of the chain and the network. Because some blocks produced by miners that have upgraded would potentially not be approved by nodes that have not upgraded, because the upgrade do support additional features or software which is not in alignment with rules before the upgrade. This would mean that the miners without the upgrade would not accept blocks from the miners that have upgraded. Thus, the miner that have and the miners that have not upgraded would include different blocks in the blockchain, thereby their are two versions of the truth and their are two different blockchains and the network has been split into two. A hard fork is just a upgrade, potentially a big one, but with the opportunity of splitting the network into two separate blockchains. This is why hard forks is rare and carefully planned, so it does not lead to a chain split. If you had one bitcoin before the split, you would after a split have one coin on each of the two blockchains, because they share the same history until the split, so the address with one bitcoin that you controlled before the split does now control one coin each of the two chains (Arvind Narayanan 2016).

Soft forks refers to upgrades that is adding features that make valuation rules stricter or does not change the validation rules at all. Thus, blocks created by miners that have upgraded would be accepted both by miners that have and have not upgraded, and thereby there is no threat of a chain split. If many enough of the networks nodes upgrades the rest of the nodes would be forces to upgrade as well to get their blocks accepted in the main chain (Arvind Narayanan 2016).

4.7 Transactions

Up to now we have talked about the infrastructure and the consensus algorithm of the bitcoin protocol. These structures are design to ensure that transactions can be created, propagated on the network, validated, and finally added to the global ledger of transactions in the blockchain (Antonopoulos 2014). Thus pro-

viding trust and security to transactions without a centralized third party. A decentralized per-to-per cash system.

To send and receive bitcoins, key-pairs are used. A key-pair consist of one public and one private key which enables one key to be shared with the world, the public key, and one private key which proves that you own the public key, and could be proven through a digital signature without revealing the private key. Digital signatures and key-pairs has been explained in more detail in the previous section "Digital Signatures".

A transaction is created by including the coins to send and the bitcoin address to send it to, which is based on the public key, so in that sens it is sent to the public key. Then the transaction is sign using your own private key, which then is broadcast to the network where it is included in the mempool(the queue of unconfirmed transactions) of mining nodes. They would validate the ownership of the coins by verifying the digital signature with the private key corresponding to the public key holding the coins. This is illustrated below, where the coins received are sent as a new transaction and sign with the owners private key (Antonopoulos 2014).

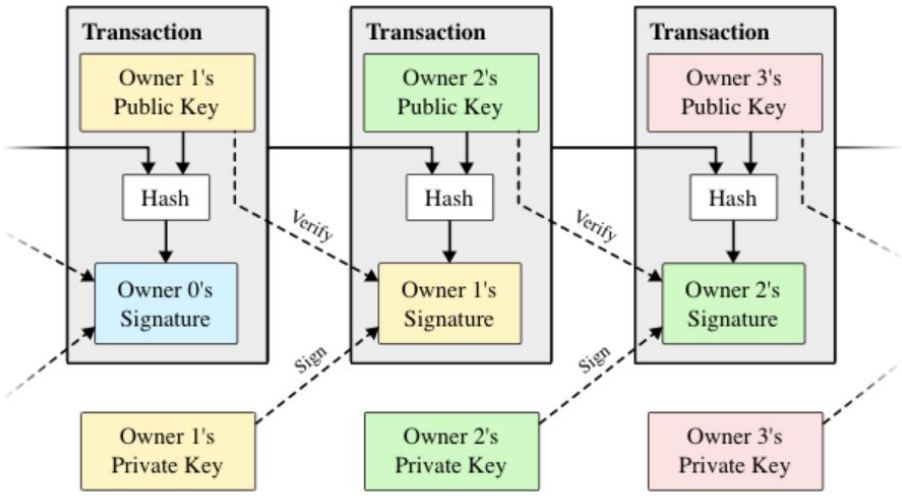

Figure 4.4: Validation of transactions (Nakamoto 2008)

Many likes to think of bitcoins as coins, but the word coins used about bitcoins is actually misleading, because what is referred to as coins are unspent transaction outputs, or UTXO. UTXOs are the outputs from transactions recorded on the blockchain, and is owned by the one or those that have the private key corresponding with the receiving addresses, as they could use these UTXOs to conduct new transactions, which will make new UTXOs. The bitcoin network tracts all (unspent) UTXOs (Antonopoulos 2014). "There are no accounts or balances in bitcoin; there are only unspent transaction outputs (UTXO) scattered in the blockchain." Antonopoulos (2014). In this sense, unspent UTXOs is similar to cash, because a private key could be the owner of many UTXOs as well as using many of these in one transaction. As you use one UTXO as an input in a transaction, this UTXO is spent and therefor no longer valid as an input. So if a transaction of bitcoins, which is only unspent UTXOs as inputs, does not match perfectly with the amount to send, the rest would be sent back as change to the sender, which is a new UTXO, which could be used in a new transaction. Below there is an illustration of a transaction of 7.5 bitcoins. To enable the transaction, a sufficient value of unspent UTXOs have to be included as inputs in the transaction, in this case three inputs. These three UTXOs used as inputs are owned and sign by the sender and a new UTXO of 7.5 bitcoins is available for the recipient, but the three inputs had a total of 8 bitcoins, so the 0.5 bitcoins left are sent back as a new UTXO to the sender, which could be used at a later occasion. In addition the outputs could be a fraction smaller than the inputs in a transaction, this is seen as a fee to the miner which would verify and include the transaction in a block, which is part of the incentive mechanisms for miners (Ivan Liljeqvist 2018b).

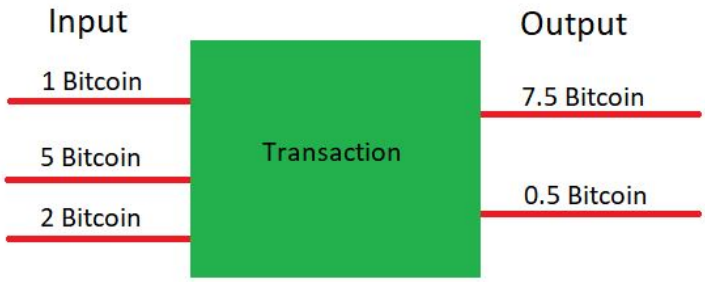

Figure 4.5: Unspent transaction output

4.7.1 Multi-signature

In addition to normal transactions, different scrips with requirements can be used to enable transactions. Multi-signature script is one of these, where a bitcoin address would have a list of potential signers, so not only one private key could provide a signature but N private keys, but the script could require that at least M of N keys has sign the transaction for it to be valid. Multi-signature could be a security mechanism for organizations to secure their funds so not one single key could transfer all the funds out of the organization. For example there could be a 2-of-3 multi-signature, thus, two of the three valid private keys has to sign the transaction for it to become valid (Antonopoulos 2014).

4.8 Blockchain 2.0

The bitcoin transaction script language includes many operators, but there is no loops or complex flow control capabilities. This ensure that the language is not Turing Complete, meaning that the scripts have limited complexity and predictable execution times. It was implemented this way as an security measure, so that infinity loops or other logical failures embedded in a transaction could lead to a denial-of-service attack against the network. Thus, by having a limited language it reduces the vulnerabilities of the network (Antonopoulos 2014).

With the intent of improving upon the concept of scripting, altcoins and on-chain meta-protocols, and develop an environment for developers, Vitalik Buterin and some other developers build a new protocol, Ethereum. Ethereum inherited most of the infrastructure and the consensus algorithms from Bitcoin, but of the changes that was done two were especially important. The first was the implementation of a new programming language with Turning Complete, Solidity. Enabling an abstract foundational layer allowing anyone to write smart contracts and decentralized applications where they can create their own rulers of ownership, transaction formats and state transition functions. The second is that Ethereum instead of using UTXO as Bitcoin, uses objects called "accounts", to account for the state of the blockchain, so it is more like an accounting system. An Ethereum account contains four fields:

- The nonce, a counter used to make sure each transaction can only be

processed once

- The account's current ether balance
- The account's contract code, if present
- The account's storage (empty by default)

Where ether is the currency, fueling Ethereum. There are two main accounts, external owned accounts, controlled with private keys like in Bitcoin, and there are contract accounts, control by their contract code. As for a Turning complete programming language, the introduction of accounts also solves some of the limitations of complexity for Bitcoin (Buterin 2013).

Blockchains as Bitcoin and other blockchains with the same features have been categorized as blockchain 1.0, for the decentralization of money and payments. As the introduction of smart contracts and decentralized application through Ethereum, platforms and protocols with the same abilities and features have been seen as blockchain 2.0, and is for the decentralization of markets more generally, and enables transfer of assets beyond currency. Even though Bitcoin at its "foundational" layer is not supporting these abilities and features, there is possible to build layer two solutions on top of the foundational layer to enable such features (Swan 2015).

4.8.1 Smart contracts

Smart contracts are programs or contracts deployed, stored and run on a blockchain. On Ethereum the contract code is stored in the account's contract code, and since the contact is its own account it could also hold money, enabling programmable money. A smart contract could contain defined functions that allows other accounts, both external and other contract accounts, to interact with the contract. It could also be used for agreements between two counterparties which do not trust each other without having a middleman, to define rules and terms, and it would also enforce those obligations automatically because smart contracts are self-verifying and self-executing (Ivan Liljeqvist 2018c, Min 2018). According to (Swan 2015) there are three elements of smart contracts that make them distinct. First, they are autonomy, when deployed the code in the contract could not be changed, and it is open source, so the code could be reviewed by anyone. Even though it is autonomy and immutable after deployment, the code can have special functions only allowed to be triggered by specific external

accounts, like the creator of the contract. second, they might be self-sufficient in their ability of gathering resources and funds through providing services or issuing equity, and spending them on needed resources, such as processing power and storage. The third element is that they are decentralized, they are distributed and self-executing across the network nodes(Swan 2015). "Contracts do not make anything possible that was previously impossible; rather, they allow common problems to be solved in a way that minimizes the need for trust." Swan (2015)

4.8.2 Decentralized applications

Smart contracts and decentralized applications(DAPPs) are sometimes used interchangeably. According to (Ivan Liljeqvist 2018c), DAPPs are all the infrastructure needed to fill the gap between the users and the blockchain. So, a DAPP could be a game, which runs all the heavy part of the game on a centralized server. The servers would let users connect to the server, as well as connect to different smart contracts on the blockchain to store and secure important information. The DAPP could therefor both be partial centralized and decentralized. So, if the server goes down all the important data about the users, and what they potentially own would still be available on the blockchain, and a new server could then work as the interface and the link between the users and the blockchain. An other example is Steemit, a social media, where steemit.com is a centralized server, working as the interface, but all the data is stored at the steemit blockchain. Thus, even if the server at steemit.com fails, all the data is still stored on the blockchain and could be connected to ones more with a new provider.

(Swan 2015) operates with a slightly stricter definition of a Dapp, "an application that runs on a network in a distributed fashion with participant information securely protected and operation execution decentralized across the network nodes".

4.8.3 DAO and DAC

A "decentralized autonomous organization"(DAO) and "decentralized autonomous corporation"(DAC) is a virtual entity that has a certain set of members or shareholders. These entities have their own set of rules embedded in their code, typically deployed in a smart contract. According to the rules and the govern-

ment, members could allocate its funds and modify its code as well as invoke predetermined smart contracts, perhaps with a 67 % majority. A complex decentralized organization, non-profit or not, could thus be govern through a set of smart contracts in a decentralized manner (Buterin 2013).

4.8.4 Tokens

Each public blockchain has its own coin, Bitcoin has bitcoin, Ethereum has ether, etc. These coins, or cryptocurrencies, are often related to as digital money, but in addition to coins there are tokens. Tokens are a representation of some value or no-value in therms of units, it could be a digital representation of a physical asset, or a direct ownership and representation of digital assets. Tokens could be created on the bitcoin protocol, but if so it has to be at a second layer. On Ethereum or other smart contract platforms tokens and token systems are easily created. Because currency or token systems, fundamentally is a database which is accounting for the ownership, with the ability of transferring X units from A to B if the specified amount is available for the sender, then the accounting system would decrease X units of A's account and add X units at B's account. So, if this logic is implemented in a contract, it is all you need to implement to create a new token system. The balance and ownership can be stored in the contract, and it could also be stored as additional information in the owner's own account. In addition other features could be added to the contract, enabling other use cases for the token Buterin (2013). Tokens could be used as a representation of any wanted asset, "tokenizing". Tokens are created and used as people prefer, and often used in different Dapps as its own cryptocurrency, or as ownership of items (Swan 2015).

Tokens have also been used to finance new projects, so called initial coin offerings(ICOs), where the token is thought to be an utility coin in a Dapp, and the ICO enables people to invest in the project and its development by interacting with a smart contract which transfer tokens corresponding to the funds provided, usually through an user interface provided by the issuer of the token. Thus, projects that never had or could afford an initial public offering provided by the financial system, could achieve crowdfunding much easier and at a much lower cost. By since it is so easy to run a ICO, many have taken advantage of gullible investors by offering tokens with no other initiative than taking there money, scams (Swan 2015).

4.8.5 Blockchain 3.0

Blockchain could be divided into generations of blockchains, where "blockchain 1.0" is referred to as the first blockchains for digital money, then "blockchain 2.0" for digital finance, and "blockchain 3.0" for digital society (Zhao et al. 2016). Blockchain 3.0 refers to the possibilities that blockchain technology could reinvent categories beyond monetary markets, payments, financial services, and economics, but open new possibilities to all industries, even to areas of society and human endeavor. The infrastructure of internet enables global communication of a scope and a scale never seen in history, and with a decentralized technology like blockchain, general decentralized models of cooperation and possibilities could be developed which never were plausible before (Swan 2015).

4.9 Scalability issues

One of the biggest issues with public blockchains today is scalability. Due to different limitations related to verifications and different consensus algorithms, many of the blockchains can today verify and confirm a limited amount of transactions. With todays block size limit and an average creation time of 10 minutes the estimated capacity of the bitcoin network is around 3 to 7 transaction per second(Antonopoulos 2014). The throughput could work to some extent for simpler applications and limited adaption, but to build complex and adapted application based upon blockchain, it requires a completely different level of scale that many of the blockchains can provide today. One of the issues today is that because all the nodes in the network needs to verity all transactions, more nodes thus not increase the transaction output, it rather increases the time needed so every node in the network have processes all transactions. A solution could be to increase the block size, thereby increasing the number of transactions that could be included in one block. The Issue with this is that the size of the blockchain, which includes all transactions ever conducted, would increase even faster. Reducing nodes and increase the block size can and would increase the capabilities of processing more transactions, the issue is that it could become increasingly hard to run a node, which reduces the ability for many to host nodes, thus increasing centralization of the network (Ivan Liljeqvist 2018b).

There are different projects and solutions being worked on to increase and solve the scalability issue. Two such solutions are "lightning network" and "shard-

ing". The lightning network is a second layer solution developed and deployed on Bitcoin. It enables a payment channel of transactions off chain which is anchored to the the foundational layer of the blockchain. It allows to open up a payment channel with one transactions on the foundational layer, then millions of transactions can be executed off chain before another transaction is done on the foundational layer to update the new state of the funds that were locked in the payment channel. The lightning network thus enable a scale of transactions and at a cost that the foundational layer can not provide. The lightning network is deployed and is running on the Bitcoin network, but its use is still moderate, but growing steady (Ivan Liljeqvist 2018b). Sharding on the other hand is not a second layer solution, but rather a design change of the foundational layer. Sharding is still not completely developed or implemented, but it is supposed to be implemented on the Ethereum protocol. As mention above, all nodes in the network has to validate and process every transaction done on the network, limiting the overall capacity for confirming transactions on the network without increasing block size or other solutions which would increase the difficulty to participate as a node. Roughly speaking, sharing presents a solution where the state of the network is split into a bunch of partitions called "shards", which all includes its own transaction history. The idea is that different nodes verify in different shards, thus, all nodes does not need to verify every transaction conducted on the entire network. Each shard is again connected by merkle tree and other solutions, but a further technical explain would not be given here (Jordan 2018).

4.10 Alternative consensus algorithms

The first blockchains used proof of work consensus algorithms, and it is still the most common used, which were explain earlier in this chapter. Other consensus algorithms has been developed to improve or solve different issues. Two of these consensus algorithms are "proof of stake"(POS) and "delegated proof of stake"(DPOS). The proof of stake enables consensus by existing owners of the currency can "stake" the currency as interest-bearing collateral. Where as in proof of work, creation of new blocks and its reward arrives from mining and competition between miner to find the next satisfying block, POS is not bases on computational power, but instead on game theory. Owners of the currency could lock up their currency like a certificate of deposit, and bigger the stake, the higher the probability to be allowed to create the next block, thus receiving the block reward and the additional transaction fees (Antonopoulos 2014).

In DPOS, the currency holder elect who to create new blocks, and the voting power of the holder equals their proportion of the currency. Those who are elected are typically called "validators", and they would conduct all computations of contracts and confirm and validate all transactions into new blocks. The number of validators and how the voting process is executed depends on the consensus algorithm of every protocol that implement DPOS (Ivan Liljeqvist 2018b). These alternative consensus algorithms have both pros and cons compered to proof of work, see table 4.1 below.

	Pros	Cons
POS	-No need of heavy mining investment -No heavy consumption of electricity -No economic of scale for big miners, linear return -Increases transaction throughput -Enable implementations of further solutions for scalability	-No real linkage to the physical world -Those who have more currency get more currency -Less proven consensus algorithm -Relies upon game theory more than simple math through SHA256
DPOS	-Significant increase of transaction throughput -Validators are incentivized to behave and contribute to the community to be elected. -No heavy consumption of electricity -Owner of tokens can influence validators to behave -Only those who wants to be elected to become validators needs to invest in hardware	-No real linkage to the physical world -More centralized (Is it decentralized?) -Less proven consensus algorithm -Only elected validators create new blocks and receive rewards -Relies upon election and not simple math through SHA256

Table 4.1: Pos and cons of proof of stake and delegated proof of stake

4.11 Databases

To store information, and help structure the data, software called databases are used. Some of the most common centralized databases are SQL-databases and no-SQL databases. SQL-databases helps structure the data with adding relationships, as for no-SQL databases just store data as efficient as possible. Most common centralized databases have the abilities of CRUD, which stands

for create, read, update and delete. Where create allows to add new data, read enables to see and read the data, update allows to change or adjust already existing data, and delete enables deletion of data. In addition there is common to have a super user or a few, which could create new users or give additional permissions to existing users in terms of issuing keys which have specific access to one or more of the capabilities, as well as withdraw permissions earlier granted (Ivan Liljeqvist 2018a).

Public blockchains does at its fundamental level, by its distributed ledgers work as a database. But in contrast to centralized databases a blockchain does only allow the features create and read. Thus, the blockchain becomes an append only database. So, you could add ledgers to change states in the blockchain, but you can not change or delete former data. Public blockchains do not operate with super users, and the system is permissionless, allowing everyone to add information by broadcasting transactions and deploying contracts to the network, and it allows everyone to read the data stored, no permissions needed. This enhance transparency and integrity and provides immutability(Ivan Liljeqvist 2018a).

4.12 Permissioned vs permissionless blockchains

Up to now we have discussed bitcoin and other public blockchains, but as the interest of blockchain technology has increased people have looked for other use cases than as for currency and financial instruments. But for many business cases, different needs and a desire of other features has lead to development of private blockchains, often referred to as permissioned blockchains. They are referred to as permissioned blockchains since users are not freely able to join the network, see the recorded history, or issue transactions of their own. Instead these are permissions given to users. This is in contrast to public blockchains as Bitcoin, where no permissions are needed to participant, therefor referred to as permissionless blockchains. By controlling and issuing permissions to users, a permissioned blockchain enables more control and privacy than permissionless blockchains offers today. Permissioned blockchains are due to this also more centralized and does not need to use mining as proof of work as a consensus algorithm. Due to this, these blockchains do not require a protocol currency, and the creation of new blocks could be performed centrally enabling a high transaction throughput, solving the issue of scalability. So, private blockchains offer more control, privacy, and transaction throughput by giving up some of

the decentralized nature of public blockchains(Dob 2018, Ivan Liljeqvist 2018a).

Private blockchains both have some of the features of more traditional systems and information handling as well as some of the features of public blockchains, thus enabling some degree of a hybrid system. As for today there are especially to main projects working with and developing private blockchain, these are the Ethereum Enterprise Alliance, which uses the foundation of the public blockchain Ethereum in a private and permissioned way, and the other is Hyperledger, which is a development community as Ethereum Enterprise Alliance of over 250 supporting organizations, where IBM have been one of the main contributors. One of Hyperledger main projects is Hyperledger Fabric, and would be roughly explained below as an example of a permissioned blockchain (Hyperledger 2017).

4.13 Hyperledger Fabric

Hyperledger Fabric(HLF) is an open source permissioned blockchain, design for use in enterprise contexts. HLF support smart contracts, but under the name chaincode, and it does support general-purpose programming languages such as Java, Go and Node.js, rather than a constrained domain-specific languages such as Solidity in Ethereum. Thus, many companies would already have programmers with the skill needed to develop chaincode without learning an additional programming language specifically for this task (Hyperledger 2017). In addition, HLF introduce pluggable consensus, this means that the participants can agree upon their consensus algorithms determined on the degree of trust or need of security for the protocol. As both permissionless and permissioned blockchains today operate with hard-coded consensus, "One-size-fits-all". Thus, HLF provides an additional solution, and with HLF architecture, which would be looked into below, with increased flexibility HLF could be tailored to a specific use case and trust model (Androulaki et al. 2018). Which enables some other features than other distributed ledger or blockchain platforms (Hyperledger 2017).

4.13.1 Architecture

The Membership service provider(MSP) is a special node or nodes that issues public key certificates, specific x.509 certificates, which is certificates used over

the internet. These are used for authentication and authorization, and the MSP maintains the identities of all nodes in the system (Ivan Liljeqvist 2018a). In HLF, the MSP provides and maintains the identities of three different nodes in the system; clients, peers, and orderers.

- "Clients submit transactions proposals for execution, help the execution phase, and, finally, broadcast transactions for ordering."Androulaki et al. (2018).

- Peers execute transaction proposals and validate transactions. They also hold and maintain the blockchain ledger and the "world state" in red in figure 4.6, as well as the "chaincode"(yellow). The world state is a database more like the account state in Ethereum compared to Bitcoin, and is a summary of all ownership of the addresses/accounts in the system, all the states. This enable fast reading of data and unnecessary to go through the hole blockchain to validate the correctness of the data, which can be the case in the UTXO system of Bitcoin. (Ivan Liljeqvist 2018a).

- Orderers, or ordering service nodes, establishes the total order of all transactions in HLF, where the transaction contains state updates with cryptographic signatures from the peers that have calculated them, then timestamps them by adding them into blocks. (Androulaki et al. 2018)

The transaction flow is shown below, if the client has the permissions needed to conduct this transaction, it would be accepted and a response would be sent back to the sender which then broadcasts the verified transaction to the orderer for ordering. The client is here represented as an application, but peers could also submit transactions. The figure below just illustrates the execution and transaction flow of one transaction in one node.

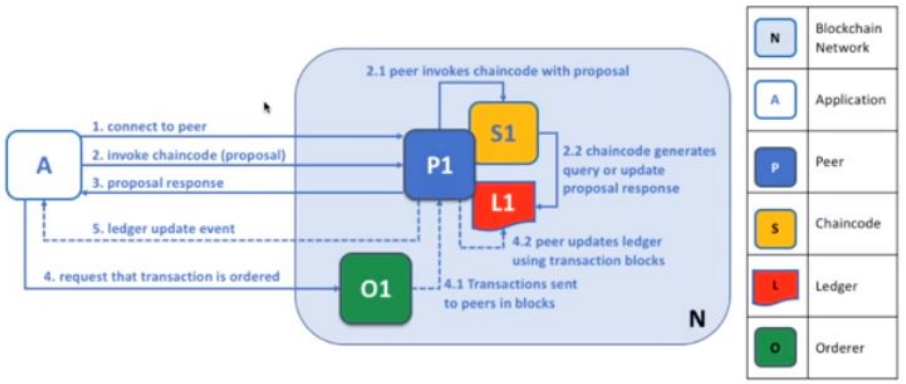

Figure 4.6: HLF transaction flow (Ivan Liljeqvist 2018a)

Since peers does the validation and the computations and the the orderer order and timesteamp the transactions, HLF enables parallel computing which is not possible in other blockchains discussed. This enables efficient processing and increased transaction throughput for the HLF ledger compared to other blockchains discussed. Androulaki et al. (2018) points out that since it is possible to run a physical node with multiple roles, HFL could operate as a traditional per-to-per blockchain if preferred.

4.13.2 Channels

Blockchains discussed up to now consist of one network at the fundamental level, HFL do support multiple blockchains connected to the same MSP, which could be seen as sub-networks, but would be referred to as channels here, with different members granted and identified by the MSP (Androulaki et al. 2018). Each channel have its own ledger and chaincode, which are hold by the peers of the channel. The use of channels enables confidentiality and privacy within the network, and could be beneficial in business use cases as it is only the members of the channel with permissions from the MSP that could read and conduct transactions in the channel. One peer could also be a member of multiple channels, thus holding the ledger and the chaincode for each of the channels (Ivan Liljeqvist 2018a). Thus, channels contributes with further flexibility of the HLF blockchain. A illustration is given in the figure below, which shows a HLF network where the MSP maintain and holds all the identities, and clients,

orderers and peers interact. The peers hold different ledgers of chaincode, since they are members of different channels. Peers could also submit transactions, which leads to peer-to-peer gossip with the orderes, as shown in the figure.

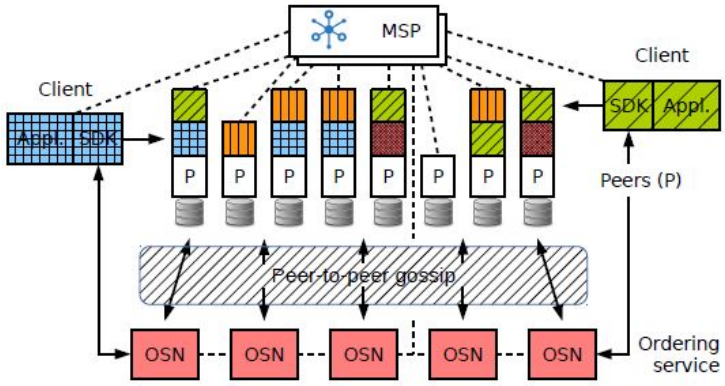

Figure 4.7: A Fabric network with federated MSPs and running multiple (differently shaded and colored) chaincodes, selectively installed on peers according to policy. (Androulaki et al. 2018)

Through the chapter an introduction and an explanation of Bitcoin and its invention of blockchain technology have been given, followed by the evolution of blockchain through new protocols enabling new features, both other public blockchains such as Bitcoin, but also private blockchain such as the Hyperledger Fabric framework. This chapter provides the second of the two literature studies conducted in the thesis, which makes up the final theoretical framework of the thesis. Thus, the next chapter of the thesis would try to answer research question 1 by determine challenges and opportunities based upon analysis of the conducted interviews, with the support of the theory provided from the literature studies if needed.

5 | Challenges and Opportunities

In this chapter the results from the analysis of the coding conducted on the transcribed interviews would be presented in the six categories established through the coding. The results from the coding were further used to determine challenges and opportunities, which are presented in the end of this chapter and provides the answer of research question 1.

5.1 General about the purchasing process

This section mainly considering the procurement process, another section would be dedicated to documentation, agreements and contracts. But since they in a large degree overlap the topic would also overlap at times.

The nature of the procurement process differs between the contractor companies and the wholesaler. As the contractors purchases all needed material and services specifically to given projects, in real time, without any warehouse, the wholesaler manages a big warehouse and do supply contractors and suppliers directly. The wholesaler does normal purchases given by prognoses based on traditional sales data. But if they participate in a tender for a delivery to a project, they often negotiate better prices from the suppliers, and if they win, they would use the standard agreement negotiated with the customer and include improved terms for this project, as well as include the additional data into the calculation of new prognoses. As for the contractors, they do purchase material, but they also purchase services and hire subcontractors. Common for the main contractor and the subcontractor are that they do purchase all the material for the project directly to the project, with the specification needed of the material in that project. The main contractor often has big orders of standardized material as rebars, and the procurement of material usually counts for 10 % of the project cost. These orders are usually purchased locally with the use of a framework agreement negotiated centrally to develop partnership with suppliers, but they do have the opportunity of obtain offers from other suppliers and potentially use them instead. The subcontractor usually orders

more complex material and do contact a few of its suppliers and compared the different offers they get based on functionality and price for each project.

The purchasing and hiring of subcontractors is the main purchase for the main contractor, and is not regulated through framework agreements, and the accumulated amount is often around 60 % of the project cost. This process is critical both in terms of cost and in terms of ensuring strategically partners in subcontractors to successfully deliver the project. Subcontractors from a wide range of disciplines are needed in a project, and for the main contractor, 40-50 different subcontractors could be involved in a project. A tender is sent out to the market, incoming offers would be evaluated, and to be considered as a subcontractor they must fulfill different criteria's and requirements. Normally 2-3 of the subcontractors would be summoned for a clarification meeting. According to the main contractor interviewee, this meeting is potentially the most import meeting during the purchasing process. "Because during the meeting we try to be as open as possible, and through the meeting we would ensure that the contractor actually have understood us, what to price, and ensure that they have included all of our requirements. This process provides us with a lot of knowledge and often ends up in a contract."

Based upon the interviews conducted the procurement processes seems to vary due to different business models, complexity and the nature of the service and material to be purchased. From the main contractor's point of view, the biggest challenge they currently face considering the procurement process is internal and is related to employees working with procurement lack competence. Specificity related to law, and the ability and the competence of negotiate agreements. As 70 % of the money flow goes through procurement, this has an incredible impact on the project. In addition, he adds that the decentralized organization structure of the company's regional branches both has its positive and negative effects, and one of the negative effects could be the loss of negotiate more agreements centrally. The wholesaler is also working to increase their efficiency and improve their agreements by going together with the Swedish, Danish and the Dutch branches of the company to negotiate with common suppliers.

5.2 Material flow

Topics and aspects around the flow of material and products were discussed in all the interviews expect in the interview with the sourcing person. This section

would as well as looking at the material flow also relate to the information and documentation of the material and products, even though topics around both information and documentation would be discussed in later sections, so there might be some overlapping. An interesting aspect is that the contractors are the end consumer of the material and the products used in projects, as the project is handed over to the principal all together, and the wholesaler is further upstream in the supply chain as a deliver of material and products.

The contractors interviewed does not operate their own warehouse and consume incoming material just in time at the building site. The wholesaler is one of the suppliers delivering material just in time on building sites. Therefor the physical flow of material becomes logistics about amount, where to deliver, time of delivery, changes, flexibility, etc, which have to be agreed upon through an agreement and communication between the company delivering and the contractor. The wholesaler is part of the transportation and delivery of the material flow as mentioned, but as they are operating a warehouse the management of material flow becomes a core operation and service they provide. The marked person from the wholesaler is managing this operation, he said that they always try to adapt, and the goal is to have a healthy store of stock and provide a service degree of delivery as high as possible. It is done by managing incoming flow of material and outgoing flow of material based upon empirical data. All available information and historical data are used as input in a software used to calculate prognoses, which also take into account lead time, delivery time, etc, to optimize material planning and the material flow. New orders are sent consecutively according to the prognoses. He further adds that project orders that often could be significant can impact the degree of delivery, and he points out that information about the delivery time and the amount of project orders often are revealed a bit late, thus impacting the prognoses and thereby the safety stock which eventually could affect the service degree of delivery. "It is not the price that wins the market, but material availability".

The main contractor mentioned that it would been interesting to see if some purchases of material that gets directly shipped from the producer to the contractor could be done without an unnecessary cost increasing wholesaler, but how this effect the price and logistics has to be taken into account to determine if it is cost efficient or not, he adds. This were also mentioned as a great concern by the interviewees from the wholesaler, as their place in the supply chain are threatened.

As for now the topic of practical and physical flow of material has been looked into, another aspect of the material flow are the requirements of the material. The main contractor elaborated upon the requirements for material used in construction projects. Material are purchased by the company themselves or by their subcontractors according to the contract. The quality requirements of the material are established according to Norwegian standards and common requirements in the specific disciplines, so everything is in alignment with Norwegian laws. The requirements also reflect the requirements set by the main contractor's principal. The requirement considering the accountability of the material used do vary. As all chemical material used in the specific project are accounted for in a system according to the requirements from the principal, this is not the case for material as wood, rebars, etc, so the suppliers are committed to deliver the material according to the standards and requirements stated in the contract. He adds that they do not have the time and the resources to check 100 % of the material they get at the building site. "So, we have to trust the suppliers to deliver according to the agreement, but we can not know if they actually do, I don't necessary think so. We have had a few cases with issues related to lack of quality". As for today they do not know much about the material received at the building site, and there is an enormous amount of value delivered to Norwegian building sites from all over the world. But when they have an agreement in Norway they often feel quite safe, but they do not know where their suppliers buy their materials from, and the main contractor lose control over the origin of the material quite fast as they start digging upstream. "Today we protect ourselves through legal contracts, thus being covered in causes where there could be non acceptable things going on, because we cannot know everything". He added that it might be here there could be interesting to look at the opportunities of blockchain, related to the flow of material.

For the subcontractor the important aspect is that he as a project manager in electro engineering that he could trust the truthfulness of the certificates from his suppliers, if not they would have curious issues, and as for now he has never seen any issues with the certificates, which is the strength of curious suppliers according to him. The process of getting approved products to be sold through the wholesaler is comprehensive and requires sufficient documentation and must meet all Norwegian requirements and standards. More about this in the next section, but the process is demanding, and it might be therefor the interviewees from the wholesalers does not share the need or considers the opportunities of tracking the documentation of the material, because they already has a well working system for this, and the system enable all their customers to visit their

web shop where they get access to all the documentation and specifications the wholesaler have on the products. At the same time the sales person point out that their customers are becoming more demanding and requires more transparency and information upstream in the supply chain.

In addition the sales person reflects upon the increased focus on environmental issues, and adds that it is interesting if blockchain could be used as a tool of tracking environmental footprints through the supply chain, but the same time she adds that they might not be interested in giving a completely record back to their suppliers and origin, because they would like to be a part of the value chain. The interviewee from the main contractor totally agree upon the importance of environmental focus and adds that they are increasing their effort considering the topic, and there is an increasing demand for information considering the environmental footprint related to the project. It is challenging according to him to estimate this properly today, but increased information about the origin of the material used during the project would at least help.

As for an implementation of blockchain to track the material flow and the related information could be interesting according to the main contractor, but they would have to look further at the opportunity, both because of the technological challenges and look if it actually is cost effective and contribute with comparative advantage for them as a company. First he would like to ask if this actually is information they need, and would a requirement considering this reduce qualified suppliers, thus decrease overall opportunities and increase cost? He continues that if he was a public builder/customer and a system which could track the material flow the answer would been yes, but more likely he thinks it would have been a requirement. He thinks that it would be more likely to be adopted as a requirement from the public instead of first being implemented at the contractor level. Then everyone would have to implement such a system and it would not lead to any potential extra cost.

5.3 Agreements, documentation and certificates

Agreements and contracts are the basis for the interviewed companies and the legal documents between them and other entities both upstream and downstream. They do set the terms and the requirements for the business cooperation, it also includes most of the requirements for documentation and certifications needed, and consider where and how this should be handed over, therefor through this

section the documentation systems would be discussed as well as the agreements and the contracts.

If the main contractor wins a tender competition for a construction project, they would start their purchasing process as described in section 1. As for the procurement of material they could use a framework agreement prepared and negotiated centrally with a strategic supplier. These framework agreements are typically two years legal agreements, often fixed unit cost, but they include clauses which allows them to obtain other offers at large projects. The agreement includes mutual trust and all terms related to the flow of required documentation. The subcontractor interviewed has many of the same terms and requirements as the main contractor considering procurement of material, but they do not have standardized framework agreements as their procurement are customized especially to a specific project, so they consider incoming offers for every project and if accepted they would make a contract with the specific terms and requirements considering the procurement of the material and delivery. One of the suppliers for the subcontractor is the wholesaler interviewed. They have customer agreements with its customers, which includes all the terms and requirements needed for both parties, as payment terms, price, logistics, etc. As for project offers mentioned with the subcontractor, this is and additional contract with own terms and requirements but based upon the framework of the customer agreement. The sales person from the wholesaler points out that it would be potentially interesting to look at the opportunities for having contracts and agreements on a blockchain.

The most comprehensive contracts for the main contractor are done with its subcontractors, where most of the contracts are done after the main contractor have got the project, but if a project is big and complex, they could make agreements with strategical subcontractors to assist with expertise related to engineering and pricing of an offer. There are additional legal requirements for subcontractors that are going to work at the building site during the project duration, both as a subcontractor and as the main contractor. As for the main contractor it includes security responsibility, solidarity responsibilities and tax issues considering its subcontractors and its employees. As for the subcontractors there are restrictions by law that the lowest level of subcontractors is level two, which mean that the subcontractor themselves could add their own subcontractor, but not further. The interviewee tells that some public principals does not allow any levels bellow subcontractor, due to the challenges of monitoring the complex structure of many levels of subcontractors.

The agreements between the wholesaler and their suppliers are negotiated by the sourcing department with support and collaboration from the market and product department. According to the sourcing interviewee they like profiling themselves as a souring and service partner as a company, where the sourcing part is to negotiate on behalf of their customers. The agreements are a legally contract working as a framework for our cooperation. The agreement consists of terms and requirements, especially considering commercial and mercantile terms, and how to handle different processes. He adds that it is a requirement that the agreement is signed before any of their products are allowed to be stored at our warehouse, in that sense this is the first step to start a cooperation. As for now they have 600 registered supplier agreements and a total of around 100 000 products registered in their system, where 80-90 % are negotiated locally in Norway and the rest with their branches of the company in neighbor countries. In addition, they usually renegotiate the top 50-100 supply agreements every second year.

Before the wholesaler will sell or provide a stack of a product, they would have to registrar the product with all related documentation and specification considering that article. All the necessary information is put into what they call "master data" and would be available to customers at their web shop. So, for the wholesaler all necessary documentation necessary is obtain through the Norwegian EFO database or from the supplier at the registration of the product in their systems. If there have been any sales through a project agreement there would potentially be extra documentation considering engineering etc, and this would then be provided in addition to the available information about the products in the web shop.

As for the contractors that purchase all their material and services to a specific project, new agreements and contracts are established for every project. Most of the documentation is received through and related to an agreement. According to the main contractor the contract is related to the company and require documentation considering certifications, insurances, potentially open book, different pre-qualifications, etc. Then there is a different system and additional information considering HSE at the building site, where the subcontractors that are going to work at the site has to provide documentation of every single employee of theirs that would be at the site during the project duration and would be provided an ID-card. Then there is the documentation of material, where the degree of documentation varies from discipline to discipline. So, most of the

documentation is provided related to agreements and contracts, for both the contractors. But both the contractor interviewees point out the importance of the operation and maintenance documentation that would be handed over to their principals at project delivery, where all necessary information and documentation needed for the owner should be included.

In common with all the companies interviewed is that there is a significant flow of documentation, but they all operate with several systems where different documentation are stored. Integration between the systems could be costly, but several systems might be inefficient and the same documentation could be stored in several systems and could bring issues if information gets updated in just one or a few systems and not in all, which could cause issues when the information is not in sync through the organization.

5.4 Information sharing and communication

A large amount of information, certificates and documentation are shared through the process towards a contract. But it is not the main focus for this section, it is more focused on the information sharing and communication related to day by day activities, even though these does intervene as well, so some overlap with the previous section could accrue.

Even though this is related to the agreement and the contract, the increased requirements consider open book and the desire of transparency from customers, especially public actors, have increased the degree of information sharing.

The type of information needed vary for the different interviewees. For the project manager from the subcontractor the information considering changes in delivery is almost as important as getting the delivery at all, and this communication is usually very good. The sales person, the marked person and the main contractor have also mention information considering delivery, and with a slightly different view and thereby different issues. Both the sales person and the marked person from the wholesaler point out the issue of late information considering volume, delivery time and potentially changes in delivery time. Which results in challenges considering managing and planning of logistics, as well as for material planning, where late information results in less accurate prognoses and reduced stock of products which again could cause reduced service of delivery for other customers. As for the contractor it is more that the information of

what actually to buy gets revealed and becomes ready quite late, which further causes limited time to purchase, thus limiting the opportunities to negotiate the best deal possible.

The sales person mentions that as a wholesaler, they should communicate information upstream in the value chain, which often is challenging due to few partner agreements and much silos. She adds that the industry is conservative, and people fear information sharing. The marked person shared the same view, that there is a high degree of information silos through the supply chain, thus securing business secretes. "People are almost afraid to ask for information", the marked person. The sourcing person pointed out that the suppliers would like as much information as possible, and as a wholesaler they would provide and share sales data and inform about markets campaigns, but not the details considering the sales. They would not like to provide all available information because they do not know the supplier's intentions and agendas with all these data. As many of the suppliers are big and serves many off their competitors it gets more complicated, he would like to see more statistical data showing that it is beneficial for them to share more information. It seems that the lack of trust is causing the unwillingness of sharing more information, thus contributing to silos. That said, the marked person did also add that they are now starting to share their accuracy of prognoses and estimates with their suppliers, so through better collaboration with suppliers they hope to be able to improve their prognoses and their material planning, which would increase service degree and improve the warehouse.

Trust seems to be an important factor for the willingness of sharing additional information. The contractor interviewee supports this view, he tells that they might be more willing to share information with strategical partners, based on trust, compared to a new established partner, even though they both have the same requirements through the contract.

According to the interviewees the communication channels seems to work well across the participants in the supply chain. The subcontractor expresses good communication and relations both to its suppliers and to its principals, the same as for the marked person of the wholesaler and adds a strength of theirs is relative few persons are involved in the communication channels, which enables a good and precis information flow. There is therefor interesting that the sales person in the same company mentions too many communication channels as a challenge, which makes it hard to track if everyone follows the agreements in the

contract. Even though the sourcing department have their main responsibilities considering agreements and contracts, they are an important communication channel for the suppliers to the organization. Issues related to defects and reclamation is often taken through communication channels without the need of including agreements and contracts.

5.5 Invoice flow

The process and the handling of invoices were a topic in 4 of 5 interviews and considering all the companies. Common for them all is that the process and the handling of invoices is rooted in the terms and the requirements of contracts and agreements. The payment deadlines follow the norm in their industry and is 45 and 60 days for contractors and wholesalers respectively. There is a wide range of payment systems used in the industry, but some standardized format of sending and receiving invoices makes it possible to integrate some information flow, which is managed in their own account system.

The sales interviewee from the wholesaler thinks that the flow of invoices is an interesting topic for blockchain, and she thinks it would potentially be opportunities of improving today's process and handling. According to her it is often related to invoices where different issues reveal themselves. There should also be pointed out that there are differences in the company's business model. The sourcing interviewee in the wholesaler stated that it is a complex industry, where they work in different customer segments, with 4000-6000 customer agreements. In addition, there is different frameworks considering projects and suppliers, so it becomes a complex price structure, which vary from country, customer, project, and a wide range of services and costs. So, the scope of invoices can seem to be in a different magnitude for the wholesaler compared with the contractors, even though the amount and further invoicing for the contractors as well can become significant and complex.

The interviewee from sales said that in every project they are a part of they end up discussing invoicing flow, time and terms, also related to the framework agreement. The number of invoices becomes significant, which the customer does not appreciate and would like as few as possible, at the same time they would like them to be transparent and clear. Thus, the specifications and attachments increase to enlighten the invoices. She adds that they on the other hand would not have collected invoices, because they do not want to finance their customers.

Therefor they invoice continuously, as some of their customers also appreciates, because they would like to further invoice their customers, which they collect and organize before they invoice, so the structure of invoicing becomes complex.

She adds that there are increasing demands and requirements of open book and transparency from the customer. They want to see what each process cost, so what we usually invoiced as one invoice is now divided into freight, services and cost related to price, with a known added profit percentage. Thus, one invoice has become three. Further she says that they always could fit cost allocation in nice tables, but it is invoicing, where it gets divided, optionally a collected invoice, without losing information, tracking and transparency. When the invoice flow could be 1000 order lines which again are priced according to a set of rules, standard agreements or project agreements. In addition, there is special cases where we as a wholesaler is further invoicing weeks after the order is delivered. The ability to track the invoices is essential considering return of material, as for today the customer has to search through our web shop to find their order, so they would be reimbursed according to their agreement. Again, the customer requests tracking of the invoice, which is challenging for us day to day.

She further elaborates with how they could ensure that they follow the correct agreement, have a nice flow, at the same time as they do not give away sensitive information, but the customer gets the transparency and the trackability as they desire. Could this be links to all agreements to ensure correct invoicing, simplify and increase efficiency of the invoice flow, reduce mistakes, increase trackability and transparency. It would also be interesting to link it to transportation data, thus having documentation and trackability all the way?

5.6 Additional topics

This section looks at some of the topics discussed through the interviews that could be of interest but were not given its own section or fitted the topics in the previous sections. One of the topics were technology and digitization which were mentioned in one way or another in all the interviews. General for them all is that they have gone through a process of digitization to enhance efficiency, reduce cost, and support and contribute with additional value for the companies. There were pointed out by a couple of the interviewees that the industry is conservative, and implementation of technology and digitization take a long time. One of the interviewees from the wholesaler says that they as a strategy

should have "Digital Courage". The wholesaler has done big investments in their digitization of metadata, centralizing the data and increasing access for all in the organization and for customers, common for them all is to work toward a better integration of digital systems. In addition, the interviewee from the main contractor mentions that they have worked much with and well on their way of implementing 3D-modeling and BIM. Both that the industry is conservative as well as they show willingness of implementation of new technology when contributing with addition value, even though changes and the willingness comes slowly it is interesting considering potential use of blockchain in one form or another, because without any willingness or openness for a specific technology, an implementation of the technology would be as good as impossible, as well as it shows that the process of adaptation and then implementation could take some time.

Hacking were another topic, where the market interviewee brings up that they have been exposed of attempts of hacking. The motive behind is not clear, but he thinks it is related to espionage, where sensitive business secrets could be sold to potential competitors, or he thinks it is related to hackers that would lock up valuable business information which they then demand ransom to unlock. Regardless the motive, it shows that security of businesses information, especially sensitive information must be taken seriously.

The last topic to be mention in this section is considering competition. The sourcing person from the wholesaler points out that it is for them a challenge that they at all times are challenged by new actors and new channels of competitions. Especially since a comprehensive process of accept and include new products for sale, where international enterprises could speed up this process in multiple countries. New competitors is a common challenge, but new channels of competition driven by globalization and new technology is of great interest.

5.7 Summary of challenges and opportunities

In this section the challenges and the opportunities to be discussed in the discussion chapter would be determined based upon the opportunities and the challenges highlighted from the results and analysis of the interviews, as well as of interest and in alignment with the topic of the literature studies conducted about supply chain and blockchain.

5.7.1 Negotiation

In section 5.1 the interviewee from the main contractor address that one of their biggest challenges considering their procurement process is their employees lack of competence especially related to law, and the ability and the competence of negotiate agreements. Since 70 % of the money flow goes through purchases of material and subcontractors the opportunities considering this challenge is profound. Even though this is the case, blockchain is a database and could not enhance employee's competence related to law and negotiation, so, blockchain is not suited to deal with this challenge.

5.7.2 Invoice flow

The process and the topic of invoicing were mention by many of the interviewees, especially the sales person from the wholesaler sees opportunity of improving this process. See section 5.5 for addition information about the results and analysis of the process and topic of invoicing. It would be interesting to look at the opportunity of using blockchain to potentially ensure that they follow the correct agreement, have a nice flow, at the same time as they do not give away sensitive information, but the customer gets the transparency and the trackability as they desire. As well a look at the opportunity of linking this to all agreements to ensure correct invoicing, simplify and increase efficiency of the invoice flow, reduce mistakes, increase trackability and transparency. As for this to work, it requires that contracts and agreements could be deployed on the blockchain, to enable a link between the invoicing and the agreements they are based upon. Therefor, the possibility of deploying contracts and agreements would be discussed before potentially looking at the opportunity of using blockchain for the invoicing process.

5.7.3 Material flow

The main contractor pointed out that they do not know much about the material received at the building site, but by having an agreement in Norway they feel pretty safe, but he admits that they do not know which suppliers and from where their suppliers uses, and they lose control over the origin of the material quite fast as they start digging upstream. At the same time some of the interviewees tells that their customers are getting more demanding and requires more transparency and information upstream in the supply chain. So, could the

material flow and addition important information and certifications be tracked, thus enhance transparency and trust in the material flowing downstream? As well as it is mentioned as an opportunity one of the interviewees from the wholesaler also express concerns related to how this could affect their position in the value chain. The main contractor which do see the use case of it also elaborate upon if this is information actually needed from their perspective as an contractor, but as the customer he sees the potentially value of it. Because he do not know if the tacking of the material flow could create addition value for them as a contractor he thinks that it might rather become a requirement from their customers or by law.

The subcontractor also point out that if they can not rely upon the certificates they have huge issues. The environmental element in this could also be added and tracked, but in terms of ensuring the correct certificates and right conditions related to human rights etc, as well as enabling better tracking and information about the environmental foot print of the material.

Even though there were some different views, especially consider how it should work, it would be interesting to look if blockchain at all could be suitable for tracking the material flow as well as necessary information considering the material. In this case it should also be possible to deploy certificates to a blockchain, as well as addition information to the flow of the material.

5.7.4 Information sharing and communication

From the section 5.4 considering information sharing and communication contributed with a couple of interesting aspects. First, it seems that the communication works well, but could as well work better at times, but this seems to be related to the correct channels of communication and the timing of the communication and relationships between the participants. Better communication channels could at least better some of the issues mentioned in the interviewees, but this would not be considered further in this paper, as blockchain do work as a database, and should not be used as a communication channel, even though communication through transactions should be possible it does not give any sense and potential improvements of communication should be solved with different tools or methods.

That said, it could be interesting to look if blockchain potentially could assist as a tool for enhance information sharing. Especially based upon the interviews

from the wholesaler, where they pointed out that the industry is conservative and there is a high degree of information silos, and it seems people are scared and shows unwillingness to share information due lack of trust, and the uncertainty and the lack of control considering the intentions of those to share information with. It would be interesting to look if blockchain could be used as a tool to enhance trust and reduce uncertainty, thus potentially contribute to a higher degree of information sharing, and less information silos.

5.7.5 synchronization of systems

In all the companies interviewed there is a significant flow of documentation, but they all operate with several systems where different documentation is stored. Integration between the systems could be costly, potentially inefficient and the same documentation could be stored in several systems and could bring issues if information gets updated in just one or a few systems and not in all, which could cause issues when the information is not in sync through the systems. It would therefor be interesting to look into if blockchain could be used to improve the current system.

5.7.6 Security of sensitive information

Security would not be discussed as a specific topic or opportunity in the discussion chapter, but it is of great importance, and should be taken seriously and included in the discussion for all IT systems and handling of sensitive information.

5.7.7 Results for research question 1

The challenges and the opportunities determined through this chapter are presented below, and provides the answer of research question 1 of the thesis.

1. Could contracts and agreements be deployed and stored on a blockchain?
2. Could blockchain be used to build a system of invoicing to ensure to follow the correct agreement, have a nice flow, at the same time does not give away sensitive information, but the customer gets the transparency and the trackability as they desire?
3. Is it possible to deploy certificates and additional information on the blockchain?

4. Could blockchain be used to track material flow, certificates and addition information considering human rights and environmental aspects of the material?

5. Could blockchain be used to enhance information sharing and reduce information silos?

6. Could blockchain be used to integrate and synchronize the systems in the organization?

6 | Feasibility Analysis

In this chapter the challenges and the opportunities determined through research question 1 would be further discussed. These would be discussed with the help of the literature studies conducted about supply chain and blockchain and potential addition information if needed. The main goal is to highlight and discuss the challenges and the opportunities, and the goal with the discussion is not to find a working solution but rather determine if there is interesting to further look into the opportunities of blockchain for that specific use case or not. Below you could see the six challenges and the opportunities which would be discussed in this chapter.

1. Could contracts and agreements be deployed and stored on a blockchain?

2. Could blockchain be used to build a system of invoicing to ensure to follow the correct agreement, have a nice flow, at the same time does not give away sensitive information, but the customer gets the transparency and the trackability as they desire?

3. Is it possible to deploy certificates and additional information on the blockchain?

4. Could blockchain be used to track material flow, certificates and addition information considering human rights and environmental aspects of the material?

5. Could blockchain be used to enhance information sharing and reduce information silos?

6. Could blockchain be used to integrate and synchronize the systems in the organization?

The flow chart by Wüst & Gervais (2018), shown in the figure below, have been used as a guideline and assistants when seen fitted for the discussion of the challenges and the opportunities.

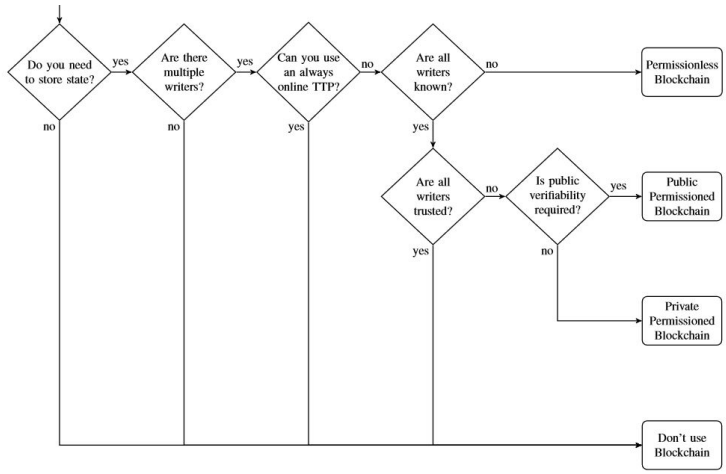

Figure 6.1: Fig. 1: A flow chart to determine whether a blockchain is the appropriate technical solution to solve a problem (TTP stands for trusted third party) (Wüst & Gervais 2018)

6.1 Agreements and contracts

Could contracts and agreements be deployed on a blockchain?
smart contracts was an innovation and implementation on the Ethereum protocol, which are programs or contracts deployed, stored and run on a blockchain. It is further explained in section 4.7.1 "smart contracts". As for today there are many both permissionless and permissioned blockchains that do support smart contracts, whether they call it "smart contracts" or "chaincode" as in Ethereum and in Hyperledger Fabric respectively. Thus, contracts and agreements could easily be deployed, stored and run on a blockchain as long as that protocol supports "smart contract" features.

In addition to just store the contracts and the agreements the features often related to "smart contracts" enables the opportunity to build functionability related to the contracts and the agreements, which could be functions giving specific information or functions that interact with the contracts and agreements with build in logic. There could also be restrictions considering who that could interact with specific functions, in a permissionless protocol this restric-

tions could be linked to given addresses as for a permissioned blockchain could be given permissions given from the MSP.

6.2 Invoicing

Could blockchain be used to build a system of invoicing to ensure to follow the correct agreement, have a nice flow, at the same time does not give away sensitive information, but the customer gets the transparency and the trackability as they desire?

Lets first go through the flow chart given by Wüst & Gervais (2018) in figure 6.1 to determine if there is any major reasons for excluding blockchain as a potential solution or part of a solution in making the invoicing process in alignment with the wanted features given in the use case.

-Do you need to store the state? The contracts and the agreements, and the addition logic around them which enable interaction with them need to be stored. To employ these should not be of any issue as long as a blockchain with "smart contract" features are chosen, which were discussed in the previous opportunity. Invoices would also be needed to be stored in form of conducted transactions which would be stored in the blockchain ledger.

-Are there multiple writers? Specifically how many writers needed depends on how the system should work, but two or more should have access to the blockchain, and different permissions could be given in terms of the need to interact with the "smart contracts", or potential add functions enabling deactivation of the use of the contracts and the agreements. In this case it depends on how the system is structured, and how it works, but since the contracts, the agreements and the invoices is sensitive information it could already here look like a permissioned blockchain is more suited then a permissionless blockchain, if any blockchain solution at all.

-Is there need of any trusted third party? It should be possible to build a system without a trusted third party, and a blockchain would potentially enhance trust, as all contracts and logic used in the smart contracts and interacted with to conduct transactions in terms of invoices would be open for those with granted permissions, if a permissioned blockchain is seen more fitted than a

permissionless blockchain.

-Are all writers known? Yes, so a permissionless blockchain is not needed in this regard, as well as the need of privacy and confidentially is easier enabled with a permissioned blockchain. But it should be said that permissionless blockchain could potentially provide better solutions and features that supports privacy and confidentiality to a greater extent in the future.

-Are all the writers trusted? Most of the writers should be trusted, but a blockchain could further enhance trust, as well as providing a trusted ledger were mistakes could not be deleted or changed, but rather a new transaction have to be conducted to correct it. Thus, all history would be available due to the blockchains nature of immutability.

-Is public verification required? It should not be required, as accounting would not be a part of the discussion and a potential system at this time.

So based on the guideline from Wüst & Gervais (2018) a private/permissioned blockchain seems most suitable and interesting to look at. So lets discuss other aspects of a potential use of blockchain for this specific case.

6.2.1 Proposal for a system

To use a private/permissioned blockchain a new blockchain has to be created and run. For this proposal the Hyperledger Fabric(HLF) framework seems most suitable, as this is one of the permissioned blockchains with the most backing and furthest development, as well as it is open source, so the framework and the necessary code is easily available. HLF is further explained in section 4.12. Since this use case mostly is based upon the interviewee done with the wholesaler, I would use them as the example for the proposal.

The HLF is flexible when it comes to consensus algorithms, and does not require any native currency or mining if it is not seen necessary, but tokens could easily be created by contracts deployed in the chaincode if wanted or needed. What is needed is a MSP which would maintain and hold the permissions of the participants in the blockchain, which has to be trusted and agreed upon by the participants of the blockchain. In addition some of the participants would nodes in terms of a peer, holding the chaincode and the ledger, and orderers, ordering the transaction, timestamp them and put them into blocks, or as both

a peer and an orderer at the same time. There would also be possible to give other participants access as a client, with specific permissions to participate in the blockchain without holding the ledger or ordering new blocks. It would be natural that both the wholesaler and their customers could be peers, potential also enabling the system of invoicing towards the wholesalers suppliers as well, which also could participates as peers and orderers.

So, if there is both customers and suppliers participating in the blockchain this would lead them all to see the flow of invoicing of everyone else. Thus, violating the desire of keeping sensitive information confidential, and not suited for the wholesaler which would share all its agreements and prices in their invoicing of their customers both to their suppliers and other customers. This could be solved through the use of the supported feature of channels in the HLF framework. Channels is multiple blockchains inside the same network with the same MSP, explain in section 4.12.

How specifically the structure of channels should be implemented depends on the need and desire of the participants, but the wholesaler could establish a channel with a specific customer, which then work as its own blockchain with its own chaincode(smart contracts) and ledger which only is available for the participants of that channel which is given by permission by the MSP. The agreements, the contracts and the interacting logic could be stored and hold in the chaincode by the channels peers, and the invoices could be conducted transactions done by interacting with the agreements in the chaincode. By establishing channels the wholesaler and the customer enables privacy and confidentiality, as other participants in the network whether they are other customer or suppliers can not see the chaincode or the ledger stored by the peers in this channel.

So, lets say that a HLF is constructed with multiple channels to provide privacy and confidentiality, but how could it ensure that the invoicing is following the correct agreement? The agreement and the contracts between the wholesaler and the customer would be deployed as chaincode as already stated before. But what if a new agreement are negotiated between the parties, whether it should be a new standard agreement or a special agreement considering a up coming project? There would not be possible to delete a previous contract, since every transaction and contract deployed on the blockchain is immutable. So, when an agreement is deployed on the blockchain it could not be changed, so new agreements would have to be deployed to update. To ensure to follow the correct agreement an addition function or functions could be implemented in all agree-

ments which allow one or two participants to deactivate the agreement, maybe the participants of the agreement would have it like two or more have to invoke that specific function to make the agreement deactivate. By deactivating the previous agreement and deploying the new agreement, the new invoicing should be in alignment with the new agreement. How this should and could be done depends both on a technical solution as well as the desire of the participants and would not be discussed further here, as this paper do not aim at presenting a final solution.

By issuing invoices by conduction transactions in interaction with the chaincode it provides transparency as all the logic in the interaction with the chaincode and the broadcasted transaction is open and could easily be validated by the participants in that channel, as well as it is being timestamped at the time it is included in a block, which gives it accountability in terms of procedure and time. Every peer holds a copy of the blockchain history, so any changes done to the blockchain would both be detected in terms of the other peers and their copy of the ledger, as well as the changes has changed the hashes of the continuous blocks, making them invalid. Because transaction both are timestamped and immutable stored in the blockchain ledger could enable the customers with the transparency and the trackability as they desire. The HLF framework also allows the customers customer to become a client with specific permissions granted so they could take part as a participants in the channel, if desired.

To enable a nice flow in the invoicing process would rely upon a well design system where everything seems to flow without any big issues as well as easily interacted with from a human perspective. It is important to remember what blockchain is and where it is. Blockchain is a database which enables logic in its smart contracts, here chaincode, so this system is the backend, handling data and logic. As the HLF framework is flexible and would in for this use case be build up by multiple channels it could by design enable further invoicing from the suppliers of the wholesaler to its customers where that is needed. It could also enable any combination of a channels seemed suitable for that specific customer or project, as well as the agreements and the addition logic, in that sense a nice flow of invoicing could be achieved by design and code to provide the desired flow of invoicing.

Even though the design and logic in the chaincode potentially could contribute to a well working system with a nice flow it would still be the back-end. In-

teracting with the back-end is often technical and is in most cases not the preferred choice of interaction from a human perspective. The HLF framework also support application program interface(API) which allow to build a front-end more suited for human interaction but through the API interacts with the blockchain. This could potentially be to the wholesalers web shop or it API could be used to retrieve invoices or other data from the blockchain directly into the wholesalers or customers accounting program. Thus, humans could interact with the front-end but actually interacting with the blockchain without noticing (Ivan Liljeqvist 2018a).

Security is becoming a crucial aspect of any system handling core business operations and sensitive data. The positive aspect with the HLF framework is that it is build on blockchain technology which includes security in its fundamental layer as well as the HLF framework is developed in cooperation with many skillful developers from respected organizations which have contributed to secure solutions, without I could verify this at such a technical data science level. As negative aspects there is three logical point of attack. First would be to in one way or another be able to take control over one of the participants permissions thus giving the attacker the same access as that participant. The positive side is that since the blockchain is immutable the attacker could not change previous transactions, but could read or interact and conduct new transactions according to the permissions he have gotten control over. Second would be to infiltrate the MSP to be able to take control over the granted permissions or give itself the wanted permissions. Third would be to physical get into the server where the blockchain ledger is stored, thus be able to retrieve sensitive data, but even though the attack would physical change the data in the blockchain ledger other copies of the ledger would be stored by the other peers in the network, as well as the cryptographical hash would be changes, thus, the blockchain would still be immutable as long as not all the servers where the ledger is stored is attacked at the same time.

6.2.2 Normal databases

Up to now we have looked at the opportunity and a proposal of potential use of blockchain for this research question, but even though such a system could work it does not mean that it is the right solution. As for today the system is build by using more traditional databases in a centralized manner. Traditional databases are much more efficient and the knowledge and competence are easier available

as for today (Ivan Liljeqvist 2018a). But what a blockchain solution lose in efficiency and in increased complexity it do provide additional transparency, trackability, immutability and trust. Which system to prefer depends therefor upon the design of the system and the desire of its participants. This paper do not aim to conclude which of these approaches is the most suitable but rather points out potential opportunities which would need further research to enlighten.

6.3 Certificates and addition information

Is it possible to deploy certificates and additional information on the blockchain?

As for contracts and agreements, certificates could also be deployed on a blockchain as a "smart contract". Addition code can also be added to the deployment to provide addition logic to the certificate as well as enabling interaction with the certificate according to the functionality the code attached to the certificate deployed allows. By using a blockchain, the timestamp as well as the immutability of the blockchain would provide the proof of existence of that certificate at that specific time as it was deployed. Even though you could prove the time of deployment the information deployed would have to contain some information that could be verified to prove that the certificate deployed are valid and not faked.

The Norwegian company DNV-GL has established a private blockchain where they store all their management systems, products and supply chain certificates, where every certificates are tagged and traceable, allowing anyone to obtain instant confirmation that a certificate is valid and up to date. When they issue a certificate, the data is digitized and a digital identity is assigned to each certificate (DNV-GL 2018). "The certificate data is in parallel managed in our production system. In total, this creates an immutable transaction, secure and highly transparent, making it easy to uncover fraud as the technology will expose any outdated or forged certificates." DNV-GL (2018)

Information could also be deployed as smart contracts on blockchains which supports smart contracts. That does not mean that any information could or should be deployed on a blockchain, because public permissionless blockchains are design to validate transactions and store the state of values in the smart contracts with coded logic to interact with the contract. So, even that you can

fill contracts with information this would in most blockchain becomes extremely inefficient and expensive, since when deploying a contract every line of code included in the transaction that deploys the contract would accumulate a needed fee so the miners and the nodes of the network would include the transaction with the contract into a new block, thus becoming a part of the blockchain. So, as for today addition information can be stored on the blockchain, but in terms of public permissionless blockchains the information to add should be limited to absolute necessary and valuable information.

It should also be said that there are projects working to provide storing of data in the same sense as cloud storage provided today by Amazon, etc, but just in a decentralized fashion linked up to a blockchain. One example of such a project is FileCoin, which potentially could provide storage of big data for a fee, which could be linked up to a blockchain as for security, payment and interaction.

6.4 Material flow

Could blockchain be used to track material flow, certificates and addition information considering human rights and environmental aspects of the material?

-Do you need to store the state? In order to track the material flow its state how to be stored and potential information as certificates, human rights data and environmental data could also be attached to the flow and stored in the ledger.

-Are there multiple writers? Yes, as the material flow down the supply chain it would be multiple writers.

-Is there need of any trusted third party? The use case for the blockchain as for this use case is to track the material flow without any needed trusted third party, where the blockchain could contribute with trust as the material flow through the supply chain.

-Are all writers known? This could depend on what kind of material being tracked or the scope of material being tracked, but in many cases all writers would not be known.

-Are all the writers trusted? In a complex flow of material in a global marked all writers could not necessary be trusted.

According to (Wüst & Gervais 2018) flow chart to determine if any blockchain is needed it shows that a blockchain could be a suitable solution, and due to the potential unknown writers a permissionless blockchain could be the best fit.

In a construction project, the material flow would arrive from a significant number of suppliers in a complex supply chain network from its origin to its end. In these cases a permissioned based blockchain where all the participants have to be known and granted permissions to interact with the blockchain would most likely prove difficult, as well as every project often requires and has different suppliers. A permissionless blockchain would enable any supplier to interact with the blockchain, thus, when considering material flow for construction projects a permissionless blockchain might present the best solution. That said, in other circumstances where the material flow are more constant and the suppliers and other participants are known a permissioned blockchain could be interesting.

Blockchain both provide security and immutability, and if all suppliers in the supply chain interact with the blockchain and provides information considering tracking, certificates and additional data the blockchain would provide provenance, trackability as well as transparency of the material flow. This would require that certificates and additional information could be deployed and stored on the blockchain, and as discussed in the previous section, this is not a problem, and some companies are already doing so, but the amount of data should be limited to a certain degree if stored at the main layer of a public blockchain due to cost.

If a permissionless blockchain is just the participants would have to have some ability of control, track and attach important information to the material. By tokenizing the specific material, which means a digital representation of the material in terms of a token, see section 4.8.4 "tokens" for further explanation of tokens. By having the material represented as a token you could transfer the ownership of that token to your customer, which then would provide a tracking of the material. By using smart contracts with functions that enable attachment of data but requires that you are the owner of the token to interact, it would provide control of who that could attach information to the token, such as certificates, data about human rights, data about environmental footprint, or any other data. This is just one suggestion of enabling control, tracking and

attachment of information to a specific material.

Even though the blockchain provides a secure and immutable store of information it can not ensure that suppliers or other participants do provide reliable data to the blockchain. Wüst & Gervais (2018) says that there are projects researching possibilities of implementing hardware with sensors that could provide trusted and reliable data directly from the physical world to the digital world of blockchain. Even though this could increase the trust of the included data there would still be possibilities of influencing or attacking the data before included into the blockchain. So, even if you use a blockchain you can not necessary control the data broadcasted to the blockchain by participants, but when the data is broadcasted to the blockchain it is final and immutable. So, if something would occur a year or ten years after the broadcasting, it would still be securely stored and immutable on the blockchain, and the suppliers would not be able to adapt and change their information according to what has occurred.

Blockchain could be used to track material flow by participants interacting and providing data of the flow of the material as well as attaching additional information of importance considering the material to be stored on the blockchain. So, how to design a system where all the participants can contribute, interact and manage the tracking of material flow? This question is fare from easy and there are challenges considering have to interact, controlling how and who to interact, provide privacy and confidentiality if desires with many more which have to be addressed when developing a system for this. But how to design such a system is not the aim of the thesis, but there are projects working on topics considering supply chain which works with these challenges. These projects works with permissioned as well as permissionless blockchains, mostly with smart contracts on Ethereum, or other protocols that support smart contracts. They also work on new second layer solutions that could provide addition features that as for now can not be provided at the main layer of Ethereum. Another blockchain protocol that should be mentioned is Vechain, which have much focus related to blockchain opportunities within supply chain, and is one of the leading projects through some partnerships when it comes to tracking of material (team 2018).

Brody (2017) argues that implementation and use of blockchain technology as part of the supply chain do not have to be really expensive and by using API and plugging into your existing infrastructure such as ERP systems you could enable tracking as well as better data to further improve their supply chain.

6.5 Information sharing

Could blockchain be used to enhance information sharing and reduce information silos?
-Do you need to store the state? To share information the information that is going to be shared would have to be stored on the blockchain.

-Are there multiple writers? yes, there would at least be two participants that would have to write transactions to contribute with information to be shared on the blockchain.
-Is there need of any trusted third party? No, there is no need of a trusted third party.
-Are all writers known? Yes, all writers are known.
-Are all the writers trusted? They are trusted to some degree.
-Is public verification required? No, there is no need or requirements of public verification.
The questions from the flow chart in determine if a blockchain is needed for that specific use case brings up some interesting elements. With the use of a permissoned blockchain as the hyperledger Fabric, privacy and confidentiality would be accomplished so not everyone can see the information that is shared, but what does blockchain brings which could not be accomplished with traditional databases? In the case of sharing plain data, transactions as blockchain often is used for is not necessary, but transactions would be be conducted just to add information to the blockchain for sharing that information with the other participants. A blockchain would provide a timestamp and provide an immutable blockchain, storing all the information ever shared in that blockchain. So, what about trust, would it enable increased trust between the participants? Not necessary, as pointed out by some of the interviewees, the trust issue is often related to the lack of control of what the counterpart you share information with would use this information to, even potentially against your interest. Whether the information is shared through a traditional database or through a blockchain would not provide additional control of the intentions and use of the information used. Where blockchain could enhance trust is considering transfer of value.

Even though it should be possible to build a system for information sharing between participants in the supply chain based on blockchain, blockchain is not specifically made to store large amount of data, but rather verify and ensure safe and trusted transaction based on consensus between the participants of the

blockchain. As for this use case as presented in the research question it is not clear in which way a blockchain based solution would enhance information sharing, which is not possible to enhance with traditional databases, which is more efficient, less complex and where knowledge and competence are easier available.

6.6 Synchronize systems

Could blockchain be used to integrate and synchronize the systems in the organization?
-Do you need to store the state? Would need to store all data and the states given in the systems to integrate.

-Are there multiple writers? There could be multiple writer inside the organization, but no one outside the organization.

-Is there need of any trusted third party? No, this should be a system implemented within the organization without a trusted third party.

-Are all writers known? Yes, all writers are known.

-Are the writers trusted? Yes, all writers are trusted, as they all would be part of the organization.

A permissioned blockchain as hyperledger Fabric would provide a synchronized system where all the nodes running in the organization have its own copy of the ledger that is synchronized and up to date with the rest of the nodes, thus would a permissioned blockchain provide synchronization of the systems as well as only those with permissions from the MSP could interact with the system and read its information and code. That said, what the blockchain provides and achieves is to work as a traditional database, without providing any of the features and the positive abilities a blockchain could provide beyond a traditional database. So, why use a blockchain when a traditional database could be used to integrate and synchronize the internal systems which is much more efficient, simple, and available knowledge and competence compared to blockchain? (Ivan Liljeqvist 2018a)

This chapter have discussed if blockchain could provide the features required

to meet the needs and the desires enabling a system or utilizing the opportunity, according to or presented in each of the six challenges and opportunities determined in research question 1. Based upon the discussion of each of these challenges and opportunities, number 1 and 3 of these are seen doable, as further investigation and research considering 2 and 4 are recommended, and the challenges and opportunities presented in 5 and 6 are not suggested to further investigation.

7 | Conclusion

This chapter provides a conclusion where the two research questions stated for this thesis would be answered. It also includes suggestions of further research.

7.1 Research question 1

Through the process of determine challenges and opportunities some of them could of obvious reasons not benefit or even integrate any use of blockchain, so these were therefor filtered out and not included. A total of six challenges and opportunities were seen as interesting to further discuss the opportunities of implementation and integration of blockchain. These are given below, and provides the answer of research question 1.

1. Could contracts and agreements be deployed and stored on a blockchain?
2. Could blockchain be used to build a system of invoicing to ensure to follow the correct agreement, have a nice flow, at the same time does not give away sensitive information, but the customer gets the transparency and the trackability as they desire?
3. Is it possible to deploy certificates and additional information on the blockchain?
4. Could blockchain be used to track material flow, certificates and addition information considering human rights and environmental aspects of the material?
5. Could blockchain be used to enhance information sharing and reduce information silos?
6. Could blockchain be used to integrate and synchronize the systems in the organization?

7.2 Research question 2

The answer of research question 2 would be presented in this section, and would provide the thesis recommendations considering further investigation of the op-

portunities of use of blockchain in the six challenges and opportunities determined in research question 1.

-Could contracts and agreements be deployed and stored on a blockchain? Contracts and agreements can be deployed, stored and run on a blockchain with the use of smart contracts, both on public and private blockchains, but the blockchain protocol have to support smart contract features. Additional functionality enabling interaction and logic can also be attached to contracts and agreements at deployment.

-Could blockchain be used to build a system of invoicing to ensure to follow the correct agreement, have a nice flow, at the same time does not give away sensitive information, but the customer gets the transparency and the trackability as they desire? Since all the participants are known a permissioned blockchain were seen most suitable, such as the Hyperledger Fabric framework. By deploying and storing agreements on the blockchain with attached functionality providing logic and interaction the system could provide a nice flow of invoicing and ensure that the correct agreement is followed. Every participant in the blockchain hold a copy of the ledger or granted permission to the blockchain and could therefor confirm that the correct agreement are used.

As all invoices issued as an transaction through interaction with the agreement, then included in a new block and becomes a part of the blockchain, both all issued invoices and agreements are stored securely and immutable on the blockchain, providing transparency and trackability of every invoice issued and every agreement deployed to the blockchain. Hyperledger Fabric enables channels, which is multiple blockchains within the same setup of Hyperledger Fabric, this would provide the opportunities to control and grant permissioned to specific participant for that channel, thus enabling privacy and confidentiality of sensitive data.

Since the Hyperledger Fabric framework could provide the features necessary and desired for such a system, the thesis would recommend that further investigation and research of such a system would be interesting.

-Is it possible to deploy certificates and additional information on the blockchain? Certificates and information could be deployed and stored on the blockchain providing prove of existence and immutability, just like with contracts and agreements. By using smart contracts when deploying certificates and information

you can attach functionality that enable interaction and logic. Even though you can deploy and store information on the blockchain, a public blockchain should not be used to store big data, since when broadcasting a smart contract or a transaction to the network you would have to pay a fee related to the size of the deployment, to be included in the blockchain. So, massive storage of information on a public blockchain would become extremely expansive, so you should limit it to information of importance.

-Could blockchain be used to track material flow, certificates and addition information considering human rights and environmental aspects of the material? Tracking of material related to a project where all participants upstream are known would be challenging, so a permissionless blockchain seems most suitable. With a permissionless blockchain, a public blockchain, all participants could interact with the blockchain and contribute. So, how to track and control who that could attach addition information? One way could be by tokenizing the specific material, thus making a digital representation of the material, which can be owned, and by using smart contracts addition functionality could be added so only the owner of the token(the material) can attach information to the token, or other smart contracts linked to the token. Further the owner of the material could send the token as a transaction to the new owner, thus tracking the material flow.

So, even though there are challenges and uncertainties of how such a system should be design, how it should work, and issues related to control the correctness of the information provided by the suppliers. A blockchain could provide tracking of the material flow, as well as provide attachment of addition information, stored securely and immutable. This thesis does therefor recommend further research and investigation of the opportunity to track the material flow with the use of blockchain technology.

-Could blockchain be used to enhance information sharing and reduce information silos? A blockchain can be used to share and store information, but as all participants are known and the cost of storing much data on a public blockchain a permissioned blockchain would be more suitable, which would enable to share information without broadcasting the information openly for any to see.

Even though a blockchain could provide sharing and storing of information does not mean that it would enhance information sharing and reduce information silos. If the issue is related to the lack of trust in what other participants

would use the information for, a blockchain would not provide any insurance or control of the information shared compared to a traditional database. Since a traditional database is much more efficient, have more available competence and knowledge, and less complex than a blockchain, but still could provide and enables the same result of information sharing. Thus, as for this specific use case I would not suggest to further explore a blockchain solution, as traditional databases are as good or even a better solution.

-Could blockchain be used to integrate and synchronize the systems in the organization? A permissioned blockchain as hyperledger Fabric would provide a synchronized system, where information would be kept inside the organization and not open for the public. But it would require nodes internal in the organization which all have its own copy of the blockchain, and since there is no other participants than internal participants what you actually get is a blockchain which work as a traditional database. So, why not use a traditional database to integrate and synchronize the systems in the organization as they are both more efficient, available, less complex and provides the same features of giving participants specific access. Thus, I would suggest to not further explore the opportunities of using blockchain to be used to integrate and synchronize systems internal in a organization.

7.3 Further research

Further research related to the opportunities of blockchain as a system for invoicing and tracking material as pointed out in the paper. Both in terms of theory as well as practical solution and design of such systems.

It would also be interesting to see if a system which do not only enable invoicing, but also includes payment of the received invoices and then connect this through accounting. Thus, you would enable invoicing, payment and merging these in accounting all in one system.

As blockchain technology still is in its early days general research considering the technology, new innovation and opportunities of the technologies in other industries and use cases would be interesting. Thus, contribute with a better understanding of the technology as well as providing more academic literature, as most of the innovation and development of blockchain are done in open source projects outside academia.

Conducting similar research as this thesis with additional interviews both considering the topic of supply chain as well as in other industries to look at opportunities which would provide more knowledge of potential use cases of blockchain, or not.

Bibliography

Aloini, D., Dulmin, R., Mininno, V. & Ponticelli, S. (2015), 'Key antecedents and practices for supply chain management adoption in project contexts', International Journal of Project Management **33**(6), 1301–1316.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. et al. (2018), Hyperledger fabric: a distributed operating system for permissioned blockchains, in 'Proceedings of the Thirteenth EuroSys Conference', ACM, p. 30.

Antonopoulos, A. M. (2014), 'Mastering bitcoin'.

Arvind Narayanan, Joseph Bonneau, E. F. A. M. S. G. (2016), 'Bitcoin and cryptocurrency technologies'.

Asbjørnslett, B. E. (2003), 'Project supply chain management: From agile to lean'.
URL: *http://hdl.handle.net/11250/240611*

Basit, T. (2003), 'Manual or electronic? the role of coding in qualitative data analysis', Educational research **45**(2), 143–154.

Basu, R. (2011), 'Managing project supply chains'.

Brody, P. (2017), 'How blockchain is revolutionizing supply chain management', Ernst Young .

Buterin, V. (2013), 'Ethereum white paper'.
URL: *https://github.com/ethereum/wiki/wiki/White-Paper*

de Araújo, M. C. B., Alencar, L. H. & de Miranda Mota, C. M. (2017), 'Project procurement management: A structured literature review', International Journal of Project Management **35**(3), 353–377.

DNV-GL (2018), 'Certificates in the blockchain'. Accessed: 2019-19-01.
URL: *https://www.dnvgl.com/assurance/certificates-in-the-blockchain.html*

Dob, D. (2018), 'Permissioned vs permissionless blockchains: Understanding the differences, url = https://blockonomi.com/permissioned-vs-permissionless-blockchains/, urldate = 2018-12-27'.

Easterby-Smith, M., Thorpe, R. & Jackson, P. R. (2012), Management research, Sage.

Educational research review. (2006).

Given, L. M. (2008), The Sage encyclopedia of qualitative research methods, Sage Publications.

Godwill, E. A. (2015), 'Fundamentals of research methodology : a holistic guide for research completion, management, validation and ethics'.

Gough, D. (2007), 'Weight of evidence: A framework for the appraisal of the quality and relevance of evidence', Research Papers in Education **22**(2), 213–228.

Holme, I. M. (1996), 'Metodevalg og metodebruk'.

Hsieh, H.-F. & Shannon, S. (2005), 'Three approaches to qualitative content analysis', Qualitative Health Research **15**(9), 1277–1288.
URL: *http://search.proquest.com/docview/220263705/*

Hyperledger (2017), 'Introduction: Hyperledger fabric, url = https://hyperledger-fabric.readthedocs.io/en/release-1.2/whatis.html, urldate = 2018-12-27'.

Inc., P. M. I. (2013), Project procurement management, in 'Guide to the Project Management Body of Knowledge (PMBOK® Guide)', 5th edition edn, Project Management Institute, Inc. (PMI), pp. 1–4.
URL: *https://app.knovel.com/hotlink/pdf/rcid:kpGPMBKPM1/id:kt00BRQGU1/guide-project-management/project-procurement-management?kpromoter=Summon*

Ivan Liljeqvist, F. M. (2018a), 'Blockchain business masterclass'.
URL: *https://ivanontech.teachable.com/*

Ivan Liljeqvist, F. M. (2018b), 'Deep fundamentals'.
URL: *https://ivanontech.teachable.com/*

Ivan Liljeqvist, F. M. (2018c), 'Smart contract programming'.
URL: *https://ivanontech.teachable.com/*

Johannessen, A., Tufte, P. A. & Christoffersen, L. (2015), 'Introduksjon til samfunnsvitenskapelig metode'.

Jordan, R. (2018), 'How to scale ethereum: Sharding explained, url = https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce, urldate = 2018-12-25'.

Kivunja, C. & Kuyini, A. B. (2017), 'Understanding and applying research paradigms in educational contexts.', International Journal of Higher Education **6**(5), 26–41.

Kvale, S. (2015), 'Det kvalitative forskningsintervju'.

Margaret Bearman, Calvin D. Smith, A. C. S. S. C. B. M. H.-W. D. L. N. (2012), 'Systematic review methodology in higher education', Higher Education Research Development **31**(5), 625–640.

Mentzer, J. T., Dewitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D. & Zacharia, Z. G. (2001), 'Defining supply chain management', Journal of Business Logistics **22**(2), 1–25.

Min, H. (2018), 'Blockchain technology for enhancing supply chain resilience', Business Horizons .

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'.

Paulraj, A., Chen, I. & Blome, C. (2017), 'Motives and performance outcomes of sustainable supply chain management practices: A multi-theoretical perspective', Journal of Business Ethics **145**(2), 239–258.

Pheng, L. S. (2018), Project Procurement Management, Springer Singapore, Singapore, pp. 177–193.
URL: *https://doi.org/10.1007/978-981-10-6992-5*$_1$2

Rajasekar, S., Philominathan, P. & Chinnathambi, V. (2006), 'Research methodology', arXiv preprint physics/0601009 .

Sanders, N. R. (2012), 'Supply chain management : a global perspective'.

Sople, V. V. (2012), 'Supply chain management'.

Srivastava, S. K. (2007), 'Green supply-chain management: A state-of-the-art literature review', International Journal of Management Reviews **9**(1), 53–80.
URL: *https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-2370.2007.00202.x*

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

Sweeney, E., Grant, D. B. & Mangan, D. J. (2018), 'Strategic adoption of logistics and supply chain management', International Journal of Operations Production Management **38**(3), 852–873.

team, V. (2018), 'Development plan and whitepaper'.

Wüst, K. & Gervais, A. (2018), Do you need a blockchain?, in '2018 Crypto Valley Conference on Blockchain Technology (CVCBT)', IEEE, pp. 45–54.

Zhao, J. L., Fan, S. & Yan, J. (2016), 'Overview of business innovations and research opportunities in blockchain and introduction to the special issue'.

A | Appendix

A.1 Interview guide

Before the interviews an introduction of the topic and purpose of the thesis were sent, as well as this interview guide with these topics shown below.

• Introduction of the topic by Torbjørn Haug

• Purchasing process.
• Documentation through the supply chain.
• Suppliers.
• Procurement to project or generally to the company.
• Overview of purchases.
• Time to get a complete overview of the origin and documentation of components.
• Falsification of certifications.

• Which aspects of your supply chain and your procurement process do you think works well today?
• Which challenges or opportunities do you see in your supply chain and procurement process?