Chair of Industrial Logistics

Master's Thesis

# A Quantitative Evaluation Model for Distributed Ledger Technologies to increase Transparency in the Supply Chain

Jakob Gmoser, BSc

March 2022

MONTANUNIVERSITÄT LEOBEN
www.unileoben.ac.at

# EIDESSTATTLICHE ERKLÄRUNG

Ich erkläre an Eides statt, dass ich diese Arbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt, und mich auch sonst keiner unerlaubten Hilfsmittel bedient habe.

Ich erkläre, dass ich die Richtlinien des Senats der Montanuniversität Leoben zu "Gute wissenschaftliche Praxis" gelesen, verstanden und befolgt habe.

Weiters erkläre ich, dass die elektronische und gedruckte Version der eingereichten wissenschaftlichen Abschlussarbeit formal und inhaltlich identisch sind.

Datum 23.02.2022

J. Gmoser

Unterschrift Verfasser/in
Jakob Gmoser

# Acknowledgement

A big thank you goes to my supervisors, Priv.-Doz. Dr. Manuel Woschank, MSc and Dipl.-Ing. Philipp Miklautsch, BSc, who supported me throughout the whole process of this thesis with valuable input and countless feedback loops.

Furthermore, I would like to acknowledge my friends (colleagues) from block42 – Blockchain Company, for all the valuable talks on and off the record. - ttfm

Of course, I also would especially like to thank my parents, without you this whole Montanuniversität adventure simply wouldn't have been possible. Furthermore, I am beyond grateful to my whole family, my friends and my girlfriend, Sarah, who all supported me along the way and stood behind me, no matter what.

# Kurzfassung

Mit der Einführung von Bitcoin im Jahr 2009 wurde eine Revolution in Gang gesetzt, und die Blockchain-Technologie gewann immer mehr an Aufmerksamkeit. Zunächst war sie nur auf den Finanzsektor beschränkt, doch in den letzten Jahren wurde das immense Potenzial dieser Technologie auch in anderen Geschäftsbereichen wie der Supply Chain Branche erkannt. In diesen Jahren hat sich auch die Technologie weiterentwickelt, und jetzt ist nicht nur die Blockchain-Technologie interessant, sondern der viel mehr umfassende Begriff der Distributed-Ledger-Technologien (DLT). Zu den charakteristischen Merkmalen dieser Technologie gehört es beispielsweise, Vertrauen zwischen sich unbekannten Parteien aufzubauen und Anwendungen mit Transparenz für alle Parteien zu versehen. Aufgrund dieser Eigenschaften werden DLTs als große Chance für die Erhöhung der Transparenz und Rückverfolgbarkeit in Supply Chain Anwendungen gesehen.
Derzeit befinden sich DLTs in einem sehr schnellen Entwicklungsstadium, und die Forschung an der Schnittstelle zwischen DLTs und Anwendungen in der Supply Chain befindet sich noch in einer sehr frühen Phase. Da viele Optionen zur Auswahl stehen und DLT-Designs verschiedene Stärken und Schwächen für den jeweiligen Anwendungsfall mit sich bringen, ist der Prozess der Auswahl des richtigen DLT-Designs für den Gesamterfolg der Anwendung sehr wichtig. Gerade dieser Teil wird in aktuellen Forschungsartikeln nur unzureichend abgedeckt, da sich die aktuelle Forschung unter anderem größtenteils noch immer nur auf die Blockchain-Technologie konzentriert.
Das Ziel dieser Arbeit ist es, diese Lücke zu schließen, indem sie DLTs über die Blockchain-Technologie hinaus abdeckt und den Auswahlprozess eines geeigneten DLT-Designs für eine Supply-Chain-Anwendung umfassend behandelt. Ziel ist es, ein quantitatives Bewertungsmodell zu entwickeln, das von Organisationen angewendet werden kann, die eine DLT-Lösung in ihre Supply Chain Prozesse implementieren wollen. Das Modell wird auf der Grundlage einer systematischen Literaturrecherche, der Ergebnisse von qualitativen Experteninterviews und schließlich durch die Bewertung verschiedener DLT-Designs mit Hilfe einer quantitativen Umfrage unter Industrieexperten entwickelt. Einschränkungen könnten sich durch den sich schnell entwickelnden Stand der DLT ergeben und dadurch, dass nur eine begrenzte Anzahl von Experten für die wichtigsten Teile dieses Modells befragt wurde.

# Abstract

With the inception of Bitcoin in the year 2009 a revolution was kicked-off, and blockchain technology gained more and more traction. First, it was limited to the financial sector only, but in the recent years the immense potential of this technology was also recognized across other business sectors, such as the supply chain industry. The technology evolved, and now it is not only blockchain technology which is interesting for such applications, but the much broader term of distributed ledger technologies (DLTs). Inherent characteristics of such technologies are for example to build trust among various parties that do not trust each other and it can bring transparency into applications in ways which are never seen before. Because of these characteristics, DLTs are seen as a big opportunity for increasing the transparency and traceability in supply chain applications.

Currently the development of DLTs is in a very fast evolving state and research on the intersection of DLTs and supply chain applications is in an early state. As there are many options to choose from, and DLT designs bring various strengths and weaknesses to the specific use case, the process of selecting the right DLT design is very important for the overall success of the application. This part, specifically, is covered badly in current research articles, as the current research is still for the most part focused on blockchain technology only and often times no consideration was given to the selection process of an appropriate DLT design.

The goal of this thesis is to fill this gap by covering DLTs beyond blockchain technology and to comprehensively cover the selection process of an appropriate DLT design for a supply chain application. The aim is to develop a quantitative evaluation model, which can be applied by organisations wanting to implement a DLT solution in their supply chain operations. The model will be developed based on a systematic literature review, the results of qualitative expert interviews and lastly by rating different DLT designs with the help of a quantitative survey conducted with domain experts. Limitations could arise through the fast evolving state of DLTs, and through the process of interviewing a only a limited amount of experts for the most important parts of this model.

# Contents

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| DLT | Distributed Ledger Technology |
| MUL 4.0 | Montanuniversität 4.0 research project |
| SCM | Supply Chain Management |
| blockDAG | block-structured directed acyclic graph |
| TDAG | transaction-based directed acyclic graph |
| PoW | Proof-of-Work |
| PoS | Proof-of-Stake |
| BTC | Bitcoin |
| PoA | Proof-of-Authority |
| DAG | Directed Acyclic Graph |
| EVM | Ethereum Virtual Machine |
| IoT | Internet-of-Things |
| GPS | Global Positioning System |
| PoC | Proof-of-Concept |
| ETH | Ether |
| B2B | Business-to-Business |
| B2C | Business-to-Consumer |

# 1 Introduction

There are a lot of stakeholders involved in a typical supply chain. Each participant is not only dependent on the product of the subsequent party but also on the information he receives about the product, like the material composition and simulation data. Moreover, there are evolving regulatory measures which ensure that organisations need to know how their suppliers treat the product and which working environment they provide. Therefore, transparency and traceability play a big role in supply chains and are creating special demands on information systems.

## 1.1 Initial Situation and Problem Statement

There is no doubt that information is an important resource nowadays. Especially when it comes to data about very specific and complex products. But in order for supply chains to utilize their full potential, some information needs to be shared across many different actors. There is also a lot of outside pressure nowadays on the companies to share information about their supply chain from governments, consumers, and other stakeholders.[1] Moreover, greater supply chain transparency is demanded from a regulatory perspective in order to prevent consumers from certain unseen threats or to positively influence working conditions.[2] The use of innovative information technologies is providing the possibility to share data to different stakeholders in a supply chain.[3]It is important to find the right balance between privacy for each company and the sharing of information in a supply chain in order to provide transparency and traceability to the end consumer. Distributed ledger technologies, the most famous example of which is blockchain technology, can provide a possibility for sharing product relevant information across a supply chain. As those technologies are known for their strengths, being immutability and transparency, DLTs could fill these needs in a supply chain. Research on DLTs and especially their influence on information systems for supply chains is scarce. There are certain challenges in place when designing and developing a DLT application for a specific use case, as there are lots of different DLT designs to choose from, each with a different set of configurations of their characteristics. Moreover, the characteristics are often interdependent with each

[1] Bateman and Bonanni 2019.
[2] Bowman and Bateman 2019.
[3] Patterson et al. 2003.

other which results in trade-offs that need to be considered. Therefore, it is one of the key challenges to select the right DLT concept and design and configure it correctly to exactly meet the demands of the specific use case.[4]

## 1.2 Objective and Research Question

The aim of this thesis is to develop a quantitative evaluation model for selecting a DLT design, according to the needs of a supply chain. This model is then to be tested in the scope of the MUL 4.0 research project where it is the aim to digitize the value chain in the metal processing industry. With the help of the evaluation model, a suitable DLT concept for this project should be selected.

Only by clearly formulating a research question, a defined focus for this thesis can be established. Subsequently, the criteria for the systematic literature review will be dependent on the quality of the research question.[5]
The objective of this thesis is the development of a quantitative model for evaluating distributed ledger technologies with regard to requirements on transparency and traceability in supply chains. The actual research question can therefore be split into two parts:

- Which specifications and requirements are important to consider when it comes to transparency and traceability applications in supply chains?
- How well do different DLT designs perform regarding the specifications and requirements of different supply chains?

## 1.3 Expected Outcome and Limitations

The expected outcome of this thesis is a list of specifications and requirements which are considered in DLT applications in the supply chain industry. Moreover, a selection of different DLT networks with their most important characteristics which will be quantified will be covered. Based on this data, a quantitative model will be developed with the goal of selecting an appropriate DLT design for a given supply chain use case. It is expected to figure out a selection of DLTs or one specific DLT which fits best for the application given by the Montanuniversität 4.0 (MUL 4.0) research project. In the future, this model should be available for organisations who are considering an application including a DLT implementation in order to improve the transparency and traceability in their supply chain operations.

[4] Kannengießer et al. 2019, p. 1.
[5] Denyer and Tranfield 2009, p. 681.

This thesis is proposing a possible method for the selection of a specific DLT design based on the concrete requirements of a supply chain application. The quantitative evaluation model will be designed in a general way. Whereas the needs regarding transparency and traceability in a supply chain could be slightly different for various industry sectors, the need for an adaption of the model to a specific industry could be present. Moreover, it is worth mentioning that the research regarding DLT and especially its application outside of the finance industry is still in its infancy but in a fast-evolving state. This could render specific aspects regarding DLT characteristics and their possibilities outdated within a reasonable matter of time, while the core principles and outcomes will stay the same. Technical implementation details of specific DLTs will not be covered and also an implementation of the software within the research project is not part of the thesis.

## 1.4 Structure of the Thesis

The second chapter of the thesis will cover the role of transparency and traceability in supply chains. After the introduction of the important terminology and definitions regarding this topic, the need and the importance of transparency in supply chains will be covered. Subsequently, the current regulatory landscape regarding supply chain transparency will be taken care of. As a next step, information systems and their use in supply chain management are described, since they play an important role for transparency as well as traceability of products in a supply chain. The first part is concluded by gathering the challenges in supply chain management which are omnipresent and have an actual context. The third part will introduce the theory behind DLTs. In this part, all important aspects of this technology will be covered, starting by explaining the terms and definitions that are needed. Since the concept of DLT only works out because of advanced concepts of cryptography, the most important cryptography principles are covered afterward. Furthermore, the distinction between private and public DLTs is made, which also brings up the importance of consensus mechanisms. As an example for many DLT concepts, the two most known, Blockchain and directed acyclic graphs, will be described hereafter. It is also essential to speak about the programmability of distributed ledger technologies, which will be the closing point of the second part. For these introductory chapters, which are laying out a basic understanding of supply chains and distributed ledger technologies, essential books and book chapters were used as the main literature.

After laying the foundations in the first three chapters, the fourth chapter is investigating the possibility of using distributed ledger technologies to facilitate transparency and traceability in supply chains. This chapter starts with an introduction and by covering a selection of already available and relevant case studies of DLT usage in supply chain applications. Therefore, a systematic literature review will be conducted in order to find the main requirements and parameters which are important for describing a DLT application for the supply chain domain. Moreover, in order to research certain DLT designs, freely available information from blog posts or whitepapers is used as literature in this chapter. To be able to develop a quantitative evaluation model for the selection of DLT designs based on these parameters, qualitative expert interviews are conducted to refine the list of parameters. On this basis, a quantitative survey is created, to rate the performance of certain DLT designs regarding the refined list of parameters. In the end, all findings are brought together and a quantitative evaluation model is developed.

The thesis will be concluded with a case study within the scope of the MUL 4.0 project. With the help of the model, which is generated in chapter 4, a selection of distributed ledger technologies will be conducted for the case in order to test the model in a real-world use case and gather additional feedback. In this chapter additional information and resources from the ongoing MUL 4.0 project were also considered. A graphical overview of the structure of the thesis can be seen in figure 1.1.

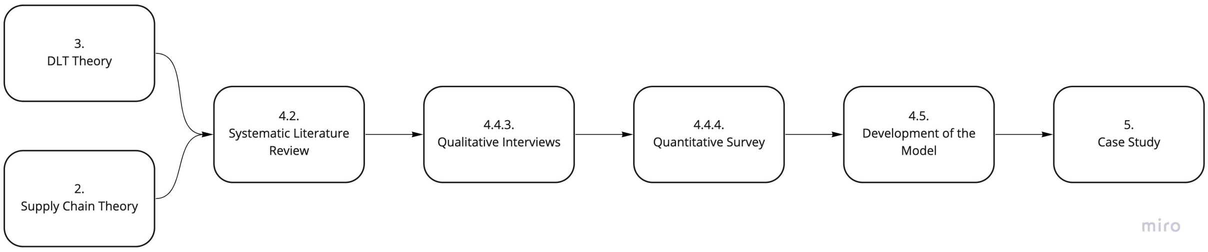



Figure 1.1: Structure of the thesis

# 2 Transparency and Traceability in Supply Chains

This chapter will introduce the terms and definitions regarding logistics, supply chains, and supply chain management in this thesis. Moreover, the focus will be laid on the role of transparency along the supply chain and the possibility to follow the trace of goods in a supply chain. Especially in this regard, the information flow in the supply chain plays an important role. Moreover, it is also beneficial to have an overview of current regulations and how those influence the supply chain landscape. The chapter is closed with an analysis of challenges that supply chain management has to deal with inherently but also due to actual developments.

## 2.1 Supply Chain Terminology and Definitions

Logistics is a term that first appeared already in the 19th century in particular in the military industry. In this context, logistics described the planning of replenishments and how troops should move from one location to another. In the years afterward the term slowly evolved out of the military context and was also used in other industries. These days, nearly every industrial enterprise has departments specialised on logistics or supply chain operations.[6]

But logistics not only evolved in its application areas but also in the operations that are within the scope of this term. In the modern era, there are many different definitions of the term logistics, but there are several elements which most authors agree on:[7]

**Logistic processes** are all transport and warehousing processes as well as loading/unloading, storing and removing from stock and commissioning goods.
**Logistic objects** can be tangible assets, material and products in industrial operation, but also intangible assets.
A **logistic system** serves the implementation of several logistic processes and has the structure of a network. It consists of vertices, like for example warehouses, and edges,

[6] Arnold 2008, p. 3.
[7] Arnold 2008, p. 3.

which can for example be possible transport routes. The borders of a logistic system can be defined according to different perspectives. Each logistic system can be split up in smaller subsystems but is also a part of a bigger super-system.[8]

With these basic things in mind logistics can be defined as follows:

> *Logistics is the design of logistic systems as well as the control of the logistic processes which are taking place within this system.*[9]

However, what is missing in this definition are three key characteristics which are also worth considering as well:[10]

- Information is not only playing a part as an object in logistics, but is also an important prerequisite to control the processes. Every logistics system needs an information and communication system, because it can be the case that the objects which need to be controlled are far away from the controlling instance.
- Moreover, logistics means a holistic view of the entire system and its processes, not only a single aspect of it.
- Logistics is interdisciplinary. It is a combination of economics, engineering, and informatics.

By now, there should already be a comprehensive understanding of what logistics is and how it is defined. The logistic system of one enterprise can also be called the logistic chain of this enterprise. It encompasses the overall flow of goods from the suppliers to the enterprise, flow within the enterprise, and from the enterprise to the customer. This can be seen as a sequence of transport-, warehousing-, and production processes.[11] Expanding the scope of this logistic chain a little bit further one can speak of a supply chain. A supply chain comprises several production- and sales levels along the way from the extraction of raw materials until the sale to the end consumer. In its most minimal form, a supply chain could be a direct relation from production to the consumer of the product, which could be the case on a farm for example.[12] In figure 2.1 another example of a supply chain can be seen, with two parties who are supplying to a producer some sort of goods. These goods are then delivered to a distributor where they are distributed to two different retailers. The supply chain ends with the consumer buying the goods at one of the retailers.

[8] Arnold 2008, p. 3.
[9] Arnold 2008, p. 3.
[10] Arnold 2008, p. 3.
[11] Arnold 2008, p. 3.
[12] Zsifkovits 2012, p. 61.

> *"A supply chain is a network of business processes and instances, which are procuring raw materials, transforming them into intermediate and end products and distributing them to customers."*[13]

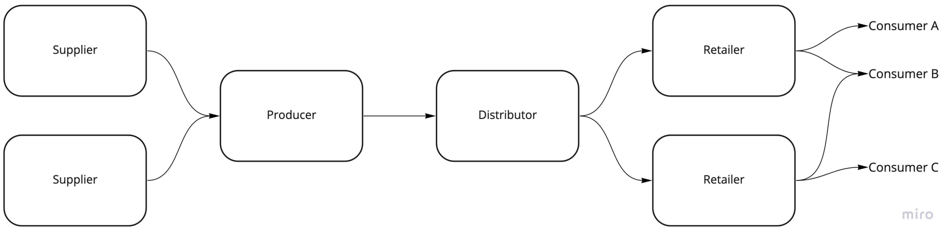



Figure 2.1: Example of how a supply chain could look like (Based on: Zsifkovits 2012)

In order to keep all the processes and operations running as smoothly as possible in such complex supply chain networks, supply chain management (SCM) is needed. SCM is targeting optimisation potentials not only within one enterprise but also on interfaces with other companies within the scope of the overall supply chain network. The main aim of supply chain management, is to reduce transaction costs along the whole supply chain.[14]

In regards to supply chain management, there are four competition factors that are of special importance: Costs, time, quality, and flexibility.[15]

- **Costs:** Costs are a key parameter in a supply chain and are concerning especially stock levels, transport, and investments. High stock levels, for example, ensure a steady supply. But a lot of capital is needed to sustain high stock levels.
- **Time:** Most activities in SCM aim to lower the time needed. The most common metric for time in logistics is lead time.
- **Quality:** In order to cater to the customers' wishes, quality is an important parameter to consider. It can be measured for example by keeping count of the products that were rejected or need to be reworked.
- **Flexibility:** Organisations should be adaptable and versatile within a supply chain to the ever-changing circumstances.

In this chapter, the terms logistics and supply chain management were defined. With the development of the industries and the thinking in terms of supply chain networks, supply chain transparency among partners also gained more and more attention. Getting into the details of the phenomenon of supply chain transparency and all it brings with it is the focus of the next chapter.

[13] Zsifkovits 2012, p. 61.
[14] Werner 2008, p. 7.
[15] Werner 2008, p. 26.

## 2.2 Transparency in Supply Chains

In this section, transparency and the role it plays in supply chain operations and management will be covered. Moreover, the often mistakenly interchanged terms of transparency and traceability will be defined.

As a starting point, transparency, in general, can be roughly defined as the "disclosure of information". In the context of disclosing environmental information of enterprises, it started to get attention from the 1960s, and was initially started by right-to-know movements in the US and other industrialized democracies. From that point on, the most notable field where transparency played a role was sustainability, but of course not limited to that. Over the years, transparency has evolved itself from being a phenomenon on the sidelines to a big pillar in today's society. With this development, transparency received more attention for making global value chains greener.[16]

> *"Transparency of a netchain is the extent to which all the netchain's stakeholders have a shared understanding of, and access to, the product-related Information that they request, without loss, noise, delay and distortion."*[17]

In this definition *netchains* are a directed network of supply chain actors which are cooperating with the common goal of bringing a product to the customers.[18] But throughout the literature, it is, unfortunately, the case that definitions of supply chain transparency are very inconsistent and many authors focus solely on one aspect of transparency.[19]

Transparency can be measured along two dimensions: The **scope of the supply chain transparency measures** and the **progress regarding certain milestones** which are needed to reach full transparency. How such a categorisation could look like can be seen in figure 2.2.[20]
In the context of global value chains, completely new infrastructures and intermediaries are emerging in order to work with information and make it available to stakeholders inside and outside these value chains. There are four ideal types of transparency which are in most cases occurring in a more or less mixed form in practical value chains:[21]

- **Management transparency:** Management transparency refers to the disclosure of information by the upstream economic actors in value chains for the downstream actors in chains. As an example, total quality management can be named.

[16] Mol 2015.
[17] Camps et al. 2004.
[18] Camps et al. 2004, p. 290.
[19] Egels-Zandén et al. 2015.
[20] Bateman and Bonanni 2019.
[21] Mol 2015, p.2.

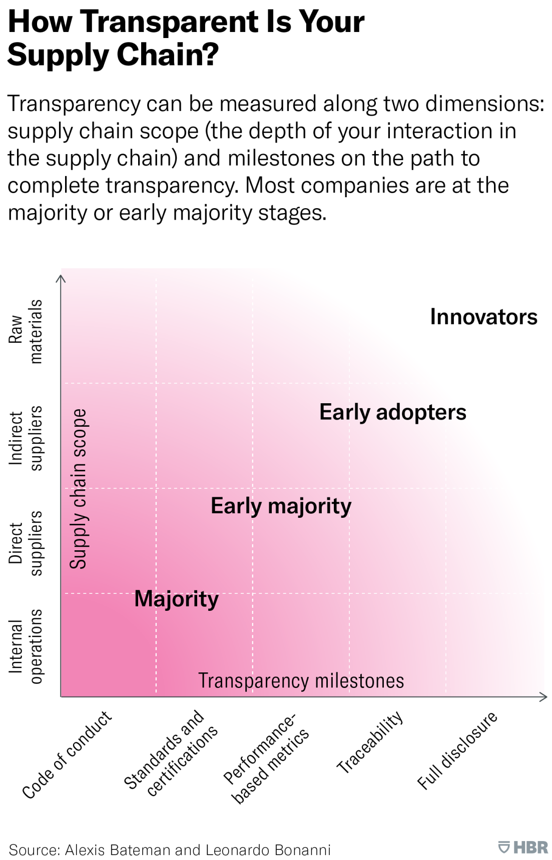



Figure 2.2: Two dimensions of supply chain transparency (Source: Bateman and Bonanni 2019)

- **Regulatory transparency:** As the name would suggest this means the disclosure of information from economic actors in value chains for regulatory and inspection bodies. For example, the EU tracking and tracing system would fall into this category. More details on the current regulatory landscape will be provided in chapter 2.3.

- **Consumer transparency:** Hereby meant is the disclosure of information by economic actors but also through certification bodies. The information is disclosed mainly to consumers and certification bodies. One example of this type of transparency would be all sorts of eco-labels and certifications.

- **Public transparency:** In public transparency, it is all about disclosure of information, again by economic actors in the value chain and certification bodies, but in this case, the information is disclosed for the greater public domain, not only consumers. A public carbon disclosure project could be named as an example.

But there are also certain troubles which come along with transparency and it's goals, especially regarding the latter two forms of transparency, consumer and public transparency. First of all, it is quite complicated and cost-intensive for organisations to take certain measurements, audits or reporting processes. Such actions and activities are more easily fulfilled by larger actors in more developed nations. All of these prerequisites present a big hurdle to smaller companies located in less developed economies and make it difficult to fulfill transparency requirements. Moreover, already when it comes to negotiating and designing transparency infrastructures and guidelines, larger and more powerful actors are having a bigger influence. Furthermore, in order for transparency to provide massive value, the following two conditions have to be met:[22]

- Those meant to be using the disclosed information must have access to that information.
- Actors whose information is disclosed need to be responsive and vulnerable to possible accusations.

This again could bring possible drawbacks with it. Firstly, because consumers and the public in developing countries may have very limited access and understanding of disclosed information. Secondly, it could it be the case, that an organisation discloses information in an unnecessarily complex way, aggregates the information in ways that are not suitable or abstracts away important parts of information.[23]

Moreover, it is hard to precisely distinguish between transparency and surveillance. Nearly every form of transparency can be also used with other intentions as a means of surveillance and control. As is the case with codes of conduct in transnational companies which protect health and safety conditions, but also bring a great amount of monitoring, surveillance, and control of workers with them.[24]

Another possible drawback of increased transparency can be recognised in the growing amount of information that is being shared. The more supply chain transparency is being demanded, the more data needs to be shared, which can quickly turn into an "information jungle". While for some supply chains this can be an unintended side effect, there are certainly institutions that use this overload of information for their own purposes. What's missing here are trusted parties who are acting as information validators and certifiers in order to distinguish true from false information. But still, and this applies on a much more general level, transparency can only be achieved when the quality and reliability of the information is proven and guaranteed. The disclosed information needs to be valid at all in order to make an influence in transparency.[25] Therefore, knowing which information is needed by the supply chain actors is a prerequisite for transparency.[26]

[22] Mol 2015, p. 5.
[23] Mol 2015, p. 5.
[24] Mol 2015, p. 5.
[25] Mol 2015, p. 5.
[26] Camps et al. 2004, p. 290.

In contrast to transparency, traceability can be very broadly defined as the ability to trace the history, application, or location of an object. This can relate to the origins of materials and parts, the processing history, and/or the distribution and location of the product or service after delivery.[27] Traceability can be seen as a tool to answer questions regarding a product, like who, what, when, where, and why.[28] The relationship could be formulated like this: Traceability enables transparency through the means of tracing and tracking.[29]

One company that has been often mentioned regarding its supply chain transparency efforts is Patagonia. They have a section on their website publishing data about their own sites, which are operated by Patagonia[30], and also a section where they disclose farms, factories, and mills they work closely with.[31] Due to the dynamic characteristics of a supply chain, there should always be an ongoing process in order to work towards a more transparent supply chain. In the end, this is better not only in regards to sustainability but also in performance.[32] This can also be seen as there are four major reasons for increased use of traceability technologies:[33]

- Technology Push: New technologies & integration in standard software
- Regulatory Push: Regulations will be covered in detail in section 2.3
- Industry Pull: More efficiency & more stability regarding processes
- Customer Pull: Requirements like a certificate of origin

It can be seen there are many perspectives and views on supply chain transparency and in the end, it comes down to the questions that are being asked. Because definitely not all information needs to be disclosed to other parties, but only that which is of special importance to external parties.[34] What is also important to consider is the role that the end-consumer plays, when it comes to supply chain transparency. According to a study of MIT Sloan Institute, consumers are willing to pay up to 10% more for a product from a company which provides greater supply chain transparency.[35] Another topic that is getting more important in this space is regulations. In certain areas where it is especially important to ask questions, governments are creating regulations around them. In the

[27] *ISO9000:2015(en)* 2022.
[28] Aung and Chang 2014.
[29] Sunny et al. 2020.
[30] **https://www.patagonia.com/where-we-do-business/owned-and-operated.html**; **23.02.2022**.
[31] **https://www.patagonia.com/factories-farms-mills/**; **23.02.2022**.
[32] Bateman and Bonanni 2019.
[33] Engelhardt-Nowitzki and Lackner 2006.
[34] Bowman and Bateman 2019.
[35] Bateman and Bonanni 2019.

next chapter, more focus will be laid on the point of regulatory transparency, what this means in detail and how the regulations look in practice currently.

## 2.3 Regulations

As already mentioned briefly, there is also a regulatory view on transparency and there are ever more guidelines emerging which companies have to adhere to. This section will give an overview of the current regulatory landscape.
There are certain industries, where consumers and regulatory bodies demand more visibility for the products. These industries are most certainly also under some kind of regulations regarding supply chain transparency, like for example the food and apparel industry.[36] But what is important to note regarding regulations is that they are bound to one specific country or region. For example, there is the California Supply Chain Transparency Act and the U.K. Modern Slavery Act, which is valid in a certain geographical area.[37]

The California Supply Chain Transparency Act encompasses all companies which are doing business in California, have annual worldwide gross receipts exceeding $100 million, and are identified as manufacturers or retailers on their California State tax returns. In order to follow the law, companies have to make public disclosures on their websites regarding five topic areas: Verification, Audit, Certification, Internal Accountability, and Training. The disclosure of information should be done in a way that provides context to the consumers but in any case, companies are not obliged to share any confidential or trade secret information.[38]

The U.K. Modern Slavery Act was introduced in 2015 and requires all large businesses to make a statement in which they describe all the steps and measures they take in order to prevent modern slavery in their business and their supply chains. It is also required that the business take serious and effective steps to identify and root out contemporary slavery.[39]

Germany recently passed a law, which will require companies with more than 3.000 employees to perform steps of supply chain due diligence. This includes measures like having the obligation to identify, prevent and address human rights conditions and environmental issues not only in their own production but also at their direct suppliers. This will be valid from 2023 on and starting already in 2024 it will be extended to companies with

[36] Bowman and Bateman 2019.
[37] Bowman and Bateman 2019.
[38] Harris 2015.
[39] Office 2021.

1.000 employees and more.[40]

In Norway, recently a Transparency Act passed the parliament which amends companies to do assessments not only regarding human rights practices on their in-house operations but also on their supply chain partners. Interestingly, the formulation of the law leaves the review and critical inquiry about reporting to the customers, expecting them to be able to read and understand those reports. The fear of being "named and shamed" should be enough reason for companies to follow the regulation and do due diligence.[41]

In 2017 a new French law was introduced called the "Duty of vigilance law" which requires French companies with more than 5000 employees to publish a so-called annual vigilance plan. This plan has to include several measures to identify risks and prevent severe impacts on human rights and the environment. The scope for this plan is not only the company itself and its subsidiaries but also its subcontractors and suppliers.[42]

Another European country which is adopting a supply chain transparency law is the Netherlands. The child labour due diligence law already passed in May 2019, but will likely become effective in the course of the year 2022, which also means that the final details of the law are not yet known. But what is already clear is that it will affect companies which are registered in the Netherlands as well as companies from abroad who are selling goods and delivering services to Dutch customers. The affected companies will have to conduct due diligence in regards to child labour in their own activities and their supply chain.[43]

In general, there are also talks about a proposal for an EU-wide supply chain act, since the start of 2020. But this proposal has already been delayed three times over the last years and the new expected launch date will be at the end of February 2022.[44]
In this chapter, the regulatory landscape regarding supply chain transparency was covered and the details of different laws in various countries were summarised. Obviously, there is no claim to completeness, as it is not viable in the scope of this thesis to cover all regulations. What has been prevalent when researching this topic, is that in the last few years, governments started to introduce supply chain transparency laws, predominantly regarding human rights and the environment. In the foreseeable future, it's definitely imaginable that more countries introduce such laws and that existing laws get extended beyond current limitations. Another important development of the last several years

[40] Thomson 2021.
[41] *Beyond Supply Chain Transparency Laws* 2016; Thomson 2021.
[42] *France's Duty of Vigilance Law* n.d.
[43] amfori 2020.
[44] Rosenberger 2022.

within supply chain management has been the advent of digitalisation within the use of information systems. This will be covered in the next chapter.

## 2.4 Handling Information in Supply Chains

There are two kinds of objects to be handled in a supply chain: Physical goods and information. Therefore, the processes regarding the information flow are of great importance in logistics and this field is called information logistics.[45] Information logistics is focused on the information that is necessary for planning and controlling the flow of material goods, the financial flows, and the utilization of personnel and equipment. However, an important differentiation to the flow of material is, that information does not flow only downstream in the supply chain, but is oscillating between different stages in the supply chain, going forward but also backward. Moreover, information logistics has an extended set of stakeholders, compared to material logistics. These are external stakeholders, which are not taking part in the physical supply chain, but are dependent on some information, like for example tax authorities, customs, insurances etc.[46]

The trends going towards cross-organisational, global supply chain networks, combined with an ever-growing speed of innovation as well as the high dynamism and volatility of the markets are leading to high complexity in managing the material and information flows. Especially information and communication systems are subject to new and increased requirements coming from all these circumstances:[47]

- **Displaying real-time data:** Up-to-date and consistent information has to be available at all times no matter where the user is located.
- **Reliability and accuracy:** Information and information systems are the backbone of every supply chain and they have to operate in a reliable and failure-proof manner.
- **Integration in global supply chains:** Supply chain management must be able to connect heterogeneous information systems. Therefore, interface standards and coordinated processes are needed in order to guarantee interoperability.
- **Provisioning of relevant information:** The demands of the customer are at the core of it and the offering of specially processed information are new fields of business.

Innovative information technologies are providing the possibilities to cover exactly those requirements. With such information systems, more accurate and up-to-date information

[45] Zsifkovits 2012, p. 245.
[46] Zsifkovits 2012, p.246.
[47] Zsifkovits 2012, pp. 246-247.

can be delivered which are leading to better visibility throughout the supply chain. Some may say, that information technology is the single most important factor for improvement in supply chain management.[48]
Especially when looking at traceability systems in supply chains, there are already a lot of emerging technologies in an operational state. But the problem currently with all these systems is that nearly all of them are of a centralized nature, which could lead to new problems regarding trust and availability.[49]

Although distributed systems like blockchain technology and other new inventions are praised as a solution to supply chain transparency, there are a lot of other factors that come into play. One single technological innovation cannot be the solution to such a challenge. A viable solution must not only be built upon the right technology, it must also include the right people and information.[50]

The management of the information flow in supply chains is a big challenge in SCM. The next chapter will continue in more detail on the topic of challenges in SCM.

## 2.5 Challenges in Supply Chain Management

Following, an overview of general challenges in supply chain management as well as some actual developments which are bringing totally new challenges with it is given.
First of all, logistics and supply chain management have changed heavily in the last couple of years. Whereas earlier, processes and departments were all seen in an isolated fashion and worked towards their own goals, it is now the case that processes need to be seen over the whole supply chain in order to be and stay competitive. Moreover, supply chain networks are getting more and more complex in their structures and organisation which results in higher requirements regarding coordination and cooperation along the supply chain and its various participants. Furthermore, this brings with it ever-growing challenges regarding the management of such networks and the data and information which needs to be handled. This may raise the need for even more innovation happening on the side of information systems in the supply chain domain.[51]

But extending beyond the classical challenges in supply chains, there are also challenges arising from actual developments in the world. Göpfert and Wellbrock did an exhaustive review of several studies regarding the future of logistics and supply chain management

[48] Patterson et al. 2003.
[49] Feng Tian 2017.
[50] Bateman and Bonanni 2019.
[51] Arnold 2008, p. 459.

and identified a total of 10 challenges:[52]

- Climate change
- Rise of globalisation
- New emerging markets (eg. Brazil, Russia, India, China)
- Threat of espionage, crime and terrorism
- Rise in demand for locally produced products
- Demand for more individualisation regarding customer requirements
- Growing complexity regarding inter-organisational data exchange
- Rise in infrastructural bottlenecks
- Increased significance of logistics service
- Rising transport costs

A section on challenges in supply chain management written in the year 2022 would most probably be incomplete without mentioning the worldwide COVID-19 crisis. COVID-19 and its implications on global supply chains are much more wide-ranging than anything previously encountered.[53] There are certain production challenges arising due to this crisis, mainly driven by suppliers' challenges like port congestion, decreases in freight capacity, and shortages of truck drivers. Global supply chains are facing delays and inventory shortages due to the impacts of COVID-19. Moreover, end-users consumers will continue to insist on the cheap prices they are already used to, but on the other side, businesses will need to relocate some of their efforts to higher-cost markets. This would put firms under constant pressure to improve their supply chain resilience.[54][55] Also in this case it was pointed out that the use of technology can help with streamlining the manufacturing processes.[56]

This chapter covered the theoretical basics regarding the definitions and terms in a supply chain management domain and aimed for painting a clear picture about what supply chain transparency actually means. In order to see how supply chain transparency is supported from a legislation perspective, the current regulatory landscape was also briefly covered. Lastly, this chapter dealt with the important role of information in supply chain management and how this information can be handled, before closing the chapter with an overview of the challenges that current supply chain executives are facing.

[52] Göpfert and Wellbrock 2012.
[53] Butt 2021, p. 2.
[54] Xu et al. 2020, p. 154.
[55] Butt 2021, p. 16.
[56] Butt 2021, p. 18.

# 3 Distributed Ledger Technologies

DLTs are a rather new concept which only got more attention from the year 2008 on when Satoshi Nakamoto (a pseudonym for a to-date unknown person or group of people) published the Bitcoin whitepaper. Bitcoin is combining and applying several innovations in computer science in order to solve fundamental problems of digital currencies, like the double-spending problem. The concept behind the operating principle of Bitcoin is called blockchain technology and in the following years, this technology was identified as a subcategory of the much broader term of distributed ledger technologies.[57]

This chapter will start by defining the term distributed ledger technologies (DLTs) and differentiating it from traditional databases. Furthermore, the different forms of DLT and how to structure them properly, according to current knowledge, will be covered. Subsequently, the cryptographic core concepts that make distributed ledger technology work are explained. Another big differentiation that can be made among DLT networks is between private and public networks which also underlines the importance of various consensus mechanisms, which are responsible for the network of nodes to find a common decision. Furthermore, two DLT concepts that are of further significance for the following parts of this thesis will be covered, the blockchain and transaction-based acyclic graphs. This chapter will be concluded with a small exhibit about smart contracts, which are allowing programmability to distributed ledger technology and are therefore opening up a lot of possibilities for various use cases and applications to be built.

## 3.1 Distributed Ledger Terminology and Definitions

As already mentioned briefly in the introduction to this thesis, data is one of the most important resources nowadays, with it being even more valuable than oil.[58] By providing such a huge value, it has also become important how the data is stored. For the storage of data, some types of databases are needed, which are mostly organized as relational databases. Meaning, there are clearly defined tables with dependencies between these tables. Usually, databases allow four different operations, also known as CRUD (create, read, update, delete) operations. Data can be created in the database, it can be read,

[57] Nakamoto 2008.
[58] *The world's most valuable resource is no longer oil, but data | The Economist* 2021.

updated, or deleted if it is not needed any more. Each operation on the database is called a transaction.[59]

Generally, three types of databases can be distinguished: centralized databases, decentralized databases, and distributed databases, as visualized in 3.1 As the name already says, centralized databases are located on a single central storage device. There is only one single authority which controls the system and all users of this system are dependent on this one party to maintain the database. This is also known as the client-server model, with one server storing the data and many clients accessing the data. Centralized databases can be easily maintained but have drawbacks regarding availability and performance.[60]

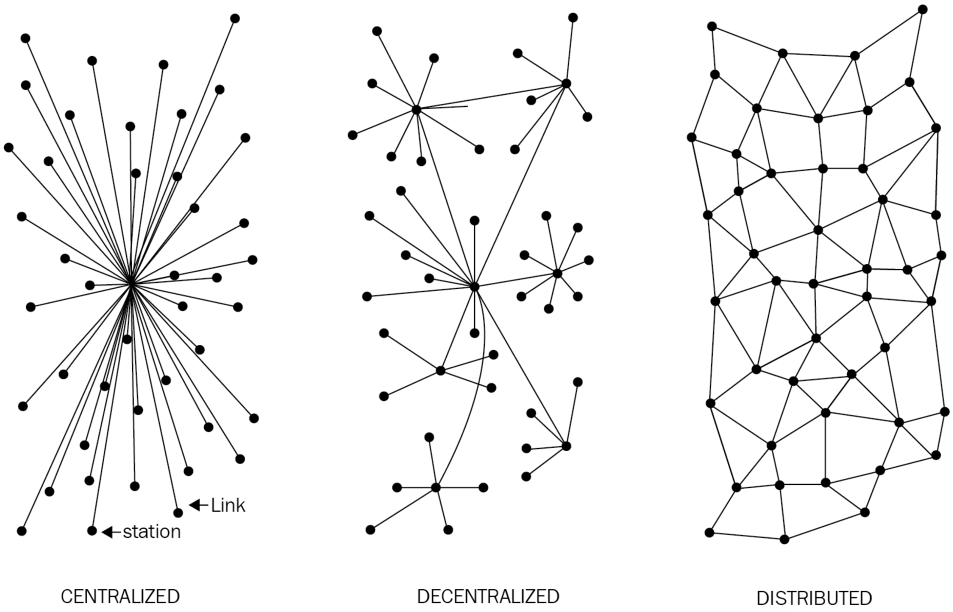



Figure 3.1: Different database network architectures (Source: Bashir 2018)

The availability of a database describes the probability of a system being reachable at a random point in time and functioning properly. While performance refers to the number of requests that can be processed during a specific time period.[61] In decentralized databases the data is stored on multiple storage devices, which are connected with each other. One of the main characteristics of decentralized databases is that they are basically a set of hierarchically organized centralized databases communicating with each other. And lastly, distributed databases are physically independent storage devices that are storing the data in a redundant fashion. Now, if one device fails, or is not available, another device can process the request. The key difference from decentralised databases is that distributed databases usually have no hierarchical structure and each device is therefore treated with equal rights. By implementing distributed databases, availability

[59] Sunyaev 2020, p. 266.
[60] Bashir 2018, p. 44.
[61] Sunyaev 2020, p. 266f.

can be increased and performance issues can be minimised.[62]

In order to maintain such a system, more effort is needed than in a centralized database, because each individual storage device (also called a node) needs to have the same information stored, which means the nodes need to be permanently synchronised. A node is able to send and receive messages and based on their intentions a node can be faulty, malicious or honest.[63] To be in a "consistent state", all the data on the nodes needs to be identical. For this to happen, the various nodes of the network need to find a common ground of what is true and what is not. This is achieved via consensus mechanisms which are coping with different Byzantine failures that can occur on such a network. Consensus mechanisms and Byzantine failures are explained in more detail in section 3.4.
But the main topic of this thesis is distributed ledger technologies and not distributed databases. So, a few smaller adaptations need to be made to define distributed ledgers. The key difference is also one of the main characteristics of DLTs, which is that ledgers only allow new data to be appended. The usual database operations "update" and "delete" are not available for distributed ledgers. Moreover, distributed ledgers are assuming that there are malicious actors present in the network. This means that distributed ledgers need more sophisticated consensus mechanisms to reach a common state of knowledge and ensure, that the network can't be compromised by malicious actors.[64] Therefore, DLT can be defined as follows:

> *"Distributed Ledger Technology (DLT) enables the realization and operation of distributed ledgers, which allow benign nodes, through a shared consensus mechanism, to agree on an (almost) immutable record of transactions despite Byzantine failures and eventually achieving consistency."*[65]

DLT, as it is defined above, is a broad term and encompasses several different concepts in which the updates to the ledger (transactions) are processed. Figure 3.2 shows an overview of the hierarchical structure of distributed ledger technology in detail.
The first level of differentiation between different DLTs can be called a DLT concept. This refers to the way how transactions are organised and stored. Blockchains, which are probably the most well-known example of DLTs, are basically a chain of blocks, where each block contains several transactions. Each block also has exactly one block as precursor which means that only one block can be added at a time. Blockchains are covered exhaustingly in chapter 3.5. In contrast, blockDAGs, block-structured directed acyclic graphs, allow a block to have multiple predecessors or successors. TDAG is the abbreviation for transaction-based directed acyclic graphs and in this concept, blocks are not used

[62] Sunyaev 2020, p. 267.
[63] Bashir 2018, p. 12.
[64] Sunyaev 2020, p. 268.
[65] Sunyaev 2020, p. 269.

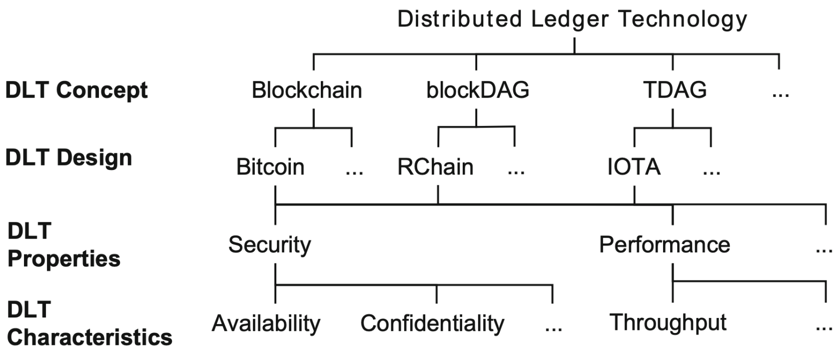



Figure 3.2: The different hierarchical levels of distributed ledger technology (Source: Kannengießer et al. 2019)

at all, the transactions are directly linked to each other. This concept is also covered in more detail in section 3.6.[66]

On the next level is the DLT design. The DLT design is a concrete implementation of a DLT concept. For example, Bitcoin and Ethereum are both associated with the DLT concept blockchain, but they are two different implementations and therefore two different DLT designs. All DLT designs have DLT properties like security and performance and DLT characteristics, but the configurations of these characteristics differ from design to design. Given the various possibilities to configure DLT characteristics, this changes the applicability of certain DLT designs to a specific DLT use case.[67]
Unfortunately, the DLT characteristics are heavily dependent on each other, which means the improvement of one characteristic may lead to the deterioration of another. Therefore, it is one of the key challenges to select the right DLT concept and design and configure it correctly to exactly meet the demands of the specific use case, where the DLT is applied.[68]

## 3.2 The Cryptography behind Distributed Ledger Technologies

DLT is built on the combination of several advanced computer science and cryptographic concepts, like hashing and asymmetric encryption using public and private keys. This section should give the reader a basic understanding of those concepts in order to better understand the operating principles of DLTs.

[66]Sunyaev 2020, p. 275.
[67]Kannengießer et al. 2019, p. 1.
[68]Kannengießer et al. 2019, p. 1.

### 3.2.1 Hashing

Hash functions play an important role in several computational systems, and also in DLTs hashing is a key concept. With the help of hash functions, it is possible to verify the integrity of specific data in an information system.[69] Hash functions are computing a string with a specified length from any arbitrary input data.[70] But what makes hash functions so special are some unique characteristics:[71]

- Hash functions are able to take input data of any length, but the output string always has the same length.
- Hashing has to be very fast. Therefore, common hashing algorithms need to be easy to compute.
- Only a minimal change in the input data should cause a severe change in the output data. This is called the avalanche effect.
- It should not be possible (without considering quantum computers) to calculate the input value from an output value (hash value). The hash function should only work in one direction. This is called preimage resistance.
- Hash functions should also be collision-resistant. This means that it is required, that two different input values do not produce the same output (strong collision resistance). And it should also be computationally infeasible, that if one input value is known, to find another input value that produces the same hash value.

There are several secure hash algorithms (SHA) already available, with SHA-256 and SHA-512 being commonly used. Whereas the number indicates the length of the hash value that is produced, 256 or respectively 512 bits.[72]
Most of the characteristics can be seen in a practical example:

- The SHA-256 hash of "17.09.2021" is:
  *DEFE4F0234A323E37B4775F8C4C89864E682A2EA8B8FE19E49EDDB0AB4F9F6D3*
- The SHA-256 hash of "18.09.2021" is:
  *03081004D3EFDC7929A571F2788744657E957354 41DD408D580F76BB5AFA58BE*

Despite the different input lengths, all hashes have the same amount of signs (64 signs) and due to the change of one sign in the input, the hash looks totally different.

[69] Sunyaev 2020, p. 277.
[70] Franco 2015, p.95 p.
[71] Bashir 2018, pp. 103-104.
[72] Sunyaev 2020, p. 278.

### 3.2.2 Asymmetric Encryption

Asymmetric encryption, or asymmetric-key cryptography, or public key cryptography has become a necessity in order to securely transfer data on an insecure network like the internet. Whenever two people need to share a secret message with each other, the message needs to be encrypted using a key. By utilising symmetric encryption, only one key is needed for encrypting and decrypting the message. In an offline setting, where the two persons can meet with each other privately and exchange keys this poses no problem. But as already mentioned: The internet is an insecure channel, which drives the need for more secure encryption possibilities. It is simply not trustworthy enough to share the key to a secret message via the internet with each other. In contrast to only having one key for both, with asymmetric encryption, there are two keys: One for encryption and another one for decryption of the message. This keypair is called public-private keypair, because one of the keys is the private key (which is supposed to not be shared with others) and the other one is the public key (as the name already says, this can be shared with others). This enables the users with two fundamental possibilities on the internet.[73]

- Messages can be encrypted in a way that only the recipients of the message can decrypt them. Assume Jakob wants to send a secret message to Philipp. Jakob needs to encrypt the message with Philipp's public key. The message can then be only decrypted with the help of Philipp's private key and only he is able to read the message.

- It can be assured that a message is coming from the right person. Assume Philipp wants to assure that the message he got, really came from Jakob and not some other person. Jakob needs to sign the message with his private key when he sends it. Philipp can then verify the signature with Jakob's public key. Only if the message was really signed with Jakob's private key initially, the verification is successful.

It should also be mentioned, that it is currently computationally infeasible to find the matching private key to a known public key by using brute force and other means. Brute force is a tactic that tests all possible combinations of private keys. In DLT asymmetric encryption is very essential, for example for the creation of transactions and for digitally signing them.[74]

## 3.3 Private and Public DLTs

Depending on who is allowed to participate in the maintenance of the distributed ledger, basically two different categories can be created: Private and Public DLTs. As the name

[73]Franco 2015, p.53 p.
[74]Sunyaev 2020, pp. 280-281.

already indicates, in public DLT designs random and unknown nodes are allowed to join and participate in the necessary actions to operate the DLT. There is no registration or verification of any kind needed, and nodes are free to join and leave at any point in time as they wish. Because there are no entry requirements, usually public DLTs are operated by a large number of nodes which contributes to a high level of availability. This also means, that public blockchains are not owned by any one single or handful of nodes, they are owned by each node.[75] The challenge in public networks is to find consensus among the large number of anonymous nodes, which results in the need for sophisticated consensus algorithms. Among the best-known representative DLT designs of this type are the Bitcoin and Ethereum networks.[76]

Private DLT networks, on the other hand, allow only a defined set of nodes with each node identifiable and known to the other nodes. This means that each node needs to be verified in order to join the distributed ledger. In these networks, it is mostly the case that they are not operated by a large number of nodes, which lowers the level of availability but also lowers the requirements regarding consensus mechanisms. Moreover, maintenance of the nodes is usually easier, which also results in better development flexibility.[77] If there is for example data transacted in the distributed ledger which the public should not be able to see, private ledgers are often the preferred solution.[78]
With private and public DLTs it is defined who is able to join the network at all. Another categorisation can be made on top of that regarding who is allowed to participate in the consensus-finding in the network. Consensus-finding can be delegated to a certain subset of nodes, in which case, the DLT design is called permissioned. In this case, simpler consensus algorithms can be applied as well, which generally results in faster consensus finding. One important point to note regarding permissioned DLTs is that they can reach finality. This means, that all nodes who participate in the consensus finding reach a final agreement on the ledger's current state.[79]

DLTs in which all nodes are allowed to participate in finding a consensus are called permissionless, because the identities of the nodes do not need to be known and all of them have the same permissions on the network. Usually, consensus finding among permissionless networks is probabilistic, which means practically, that the consistency between all nodes in a public, permissionless network can only be assumed with a certain probability at a certain point of time. This can be best understood using an example from the Bitcoin blockchain. Once a block $x$ is written on the blockchain it is not 100% sure that the

[75] Bashir 2018, p. 32.
[76] Sunyaev 2020, p. 276.
[77] Kannengießer et al. 2019, p. 7.
[78] Sunyaev 2020, p. 276.
[79] Sunyaev 2020.

data is already written permanently on the blockchain. But as soon as there are more blocks written on top of block $x$ the probability of block $x$ being final approaches 100% but never really reaches it. This is the case because in a DLT, where nodes are not known and are allowed to join and leave whenever they want, certain events can occur that can lead to a removal of block $x$. One such event could be for example if two blocks are mined at the exact same time which will temporarily split up the chain. When this is resolved at a later point of time because there can only be one valid blockchain, blocks could be temporarily removed from the chain until they are added again.[80][81]

Now it can be already seen that consensus algorithms are a core element in distributed ledger technologies. The next chapter will focus solely on explaining the need for consensus algorithms in a detailed way and presenting the most common consensus algorithms nowadays.

## 3.4 Consensus Mechanisms

Through the automated way of finding consensus in the network there is no need for a trusted third party for settlement between several unknown actors.[82] In order to reach a decision among a distributed network of nodes about what is true and what is not true, consensus algorithms are essential. Basically, three conditions need to be fulfilled to guarantee consensus in a distributed ledger:[83]

- All nodes who agreed on maintaining the ledger need to find a common agreement regarding the order of the transactions and write them to the ledger in this order.
- No **single** party should be able to manipulate this order of transactions.
- No one in the network should be able to stop the transactions from being processed.

In order to guarantee that these conditions are fulfilled, four general steps need to be taken, which can also be called the consensus process:

1. Every node which is allowed in the consensus finding records the transactions it wants to be written into the distributed ledger.
2. This data is shared with the other nodes involved in the network.
3. With the help of certain consensus algorithms, consensus among the nodes is established regarding the order of transactions.

[80] Sunyaev 2020, p. 277.
[81] Didovskiy 2021.
[82] Kannengießer et al. 2019, p. 1.
[83] Stevens 2018.

4. All nodes update their order of transactions in order to reflect the result of the consensus decision.

So much about the general way of establishing consensus in a distributed network. As already briefly discussed in section 3.3, different DLT implementations with different access rights need different consensus algorithms. Finality regarding the distributed ledgers state can only be achieved in a rather small network (in terms of node count) and if the resulting efforts for communication and synchronization stay small. That is the case because all permitted nodes need to agree on the state in order to reach consensus. In a large network with anonymous nodes joining and leaving arbitrarily, this is impossible, which results therein that only probabilistic consensus algorithms are suited for such kinds of networks.[84]
Following, the most common consensus algorithms are explained in order to gain a certain understanding of how consensus finding can work in detail.

### 3.4.1 Proof-of-Work

Proof-of-Work (PoW) was already invented in 1993 by Dwork and Naor in order to combat junk e-mail.[85] The idea was rather simple: Clients are requested to do a certain amount of work before they can request a service. It is the digital equivalent of depositing a certain amount of cash upfront before you buy something more expensive, just to ensure that you are serious about buying that thing. With the invention of Bitcoin in 2008 by Nakamoto, this concept was extended and the first time used as a consensus algorithm in the Bitcoin blockchain.[86]

Each node has to solve a computationally difficult challenge in order to be able to include new transactions in the ledger. The node that first solves this challenge can publish its transactions and is rewarded for the work it has put in, in the form of a network-specific incentive mechanism. In the case of Bitcoin, nodes who participate in the consensus finding are called miners and they are rewarded with Bitcoins (BTC). With respect to what has been stated in chapter 3.3, PoW can be used for consensus finding in public, permissionless DLT designs.[87] Inherently, this mechanism is also preventing the double-spending problem, which means basically that a user is not able to spend his coins more often than once. In order to accomplish that in a system with PoW, the user needs to have a significant amount of computing resources available in order to be able to manipulate the network this way.[88]

[84] Sunyaev 2020, p. 281.
[85] Dwork and Naor 1993.
[86] Nakamoto 2008.
[87] Sunyaev 2020.
[88] Bano et al. 2017, p. 6.

Since the aim of PoW is to computationally solve difficult challenges, there is a lot of computing power needed to participate in the consensus finding. Therefore, Bitcoin and PoW mining is a highly flexible load on the electricity grid, which can be easily turned on or off within a short matter of time, moreover it provides a payout in a liquid cryptocurrency. And with these characteristics, ultimately, Bitcoin could bring the world in a position where substantially more renewable energy is deployed, simply because it brings the needed flexibility regarding energy demand into an energy grid.[89] But still, energy usage is one of the most criticised aspects of the most prominent PoW blockchain. To put things into perspective, the annualized energy consumption of the Bitcoin blockchain is currently estimated to be 167.73 TWh. This can be compared to the annual energy consumption of Poland.[90] Certainly, this is a lot of energy, but still, this might not represent a threat to the climate. Moreover, the energy consumption resulted in a heavy focus in the industry to search for alternatives to Proof-of-Work.[91] One of the first developed alternatives is Proof-of-Stake.

### 3.4.2 Proof of Stake

Proof-of-Stake (PoS) is a less energy-consuming alternative to PoW, because there is no computational work to be done. The basic principle in consensus algorithms for public, permissionless DLTs is always, that node providers must have significant "skin-in-the-game" in order to participate. In PoW this is achieved by having to put in way more work and money in terms of computing power than what can be won by manipulating the network. In PoS the principle is similar, with the balance of tokens a node operator possesses being closely linked to the probability of mining the next block. Basically, this means a miner has to stake a certain amount of tokens in order to participate in the consensus finding. Staking in this case is describing nothing else than locking them up for a certain amount of time, which means, once the tokens are staked they cannot be sent anywhere. But, selecting a miner only based on the number of coins he has staked would of course lead to an unwanted centralization. Therefore, there are several different approaches being developed on how exactly this selection can work.[92] With randomised block selection[93], coin-age-based selection[94] and delegated Proof-of-Stake[95] being among the most prominent at the point of writing. Like PoW, PoS is also suited for public, permissionless DLTs. As a rough guideline, it can be expected that a PoS DLT needs

[89]BCEI 2021.
[90]Digiconomist 2021a.
[91]Sedlmeir et al. 2020.
[92]Sunyaev 2020.
[93]Vasin 2014.
[94]King and Nadal 2012.
[95]dantheman 2017.

about $10^3$ J per transaction compared to $10^9$ J per transaction in a PoW system.[96]

### 3.4.3 Proof of Authority

Proof-of-Authority (PoA) is a consensus algorithm that is suited for private, permissioned DLTs only. The operating principle of PoA is very basic: Instead of putting skin-in-the-game via computational power or tokens, in PoA systems nodes put their reputation on stake. In PoA algorithms a set of known and trusted entities are acting as node providers. Simply put, those node providers are proposing new blocks in a mining rotation scheme in order to fairly distribute the responsibility of creating new blocks. There are different implementations available on how this can be done in practice. The two most known are Aura (Authority Round) which is used in the private Ethereum implementation Parity. And Clique, which is implemented in Geth, which is another private Ethereum implementation.[97]

### 3.4.4 Apache Kafka

Apache Kafka is a consensus algorithm used in Hyperledger Fabric, which is one of the most prominent private DLT Designs. Kafka, in fact, is a widely used distributed event streaming platform which is essentially sending the transactions to a so-called "Orderer", which is ordering them and then broadcasting them to the other peers. This results herein, that it can reach finality in the network relatively quick. But, the more nodes are present on the network, the longer it takes to come to a decision. Moreover, Apache Kafka is not Byzantine fault tolerant, which prevents the system from reaching consensus in the case of malicious nodes. Basically, any behaviour which is not the expected behaviour of a node in the network can be classified as Byzantine fault. This term stems from the Byzantine generals problem, proposed by Lamport et al in 1982: A group of generals are planning to attack or retreat from a city, but they are split up around the city and the only way to communicate with each other is a messenger. The generals need to strike at the same time in order to be able to win. The issue is, that the generals need a viable mechanism to cope with messages not arriving and with traitors among them who could intentionally send a misleading message.[98] Therefore, consensus algorithms based on Apache Kafka are only applicable in private, permissioned settings.[99]

In this chapter an overview of consensus algorithms was given and a theoretical basis was built in order to understand why consensus in distributed ledger technology is even

[96] Sedlmeir et al. 2020.
[97] Angelis et al. n.d.
[98] Bashir 2018, p. 12.
[99] Siddharth 2019.

needed. In the next section the currently most common DLT concept, a blockchain, will be covered.

## 3.5 Blockchain

A blockchain is currently the most well-known DLT concept and it has basically started off all the developments in this direction with the advent of the Bitcoin blockchain in 2009. The blockchain concept is one possible data structure how the transactions can be organised and stored among a decentralized network of nodes.[100]

As the name already says, a blockchain is essentially a "chain of blocks". Whereas a block is a data structure that includes transactions and other data attributes, like the hash of the previous block. Whenever a block is finished, a hash of the content gets created in order to make sure that the transactions can't be changed afterward. If this were the case, the hash value would not be the same as the initially created value. Now, if this hash gets included in the next block before the content of the next block gets hashed, the two blocks are basically "chained together". This can be seen in figure 3.3, where the parent block hash is the hash of the preceding block in the blockchain.[101]

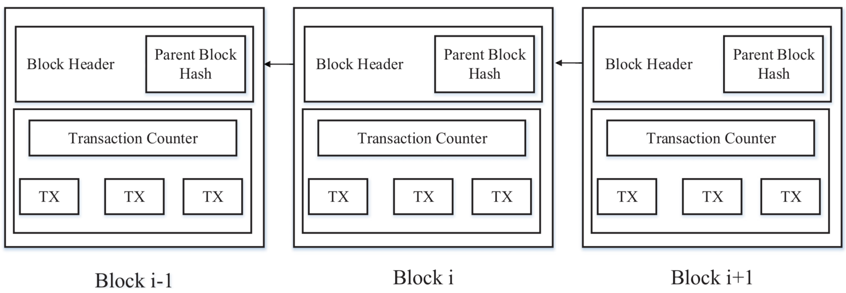



Figure 3.3: An example of blocks chained together by including the hash of the previous block (Source: Zheng et al. 2017)

## 3.6 Directed Acyclic Graph

Blockchains do have one big drawback. There can always only be one chain that is acknowledged by all the nodes and blocks can only be added one by one. This puts certain limitations in terms of throughput on a system like this. A directed acyclic graph (DAG) is another DLT concept, which can reduce these constraints. A DAG is a directed graph, where no paths are starting and ending at the same node (= acyclic), hence the growth can only go in one direction. This brings with it many advantages over traditional blockchains

[100] Sunyaev 2020.
[101] Zheng et al. 2017.

like the possibility of faster and fee-less transactions. Moreover, fewer resources are needed than for example in the Bitcoin blockchain because the process of mining is abandoned.[102]

At the moment, it can be differentiated between block-based directed acyclic graphs (blockDAG) and transaction-based directed acyclic graphs (TDAG), where no block structure at all is used. The transactions in the latter case are sent directly into the network and are linked to each other.[103] One mentionable implementation of a DAG is the IOTA Tangle.[104]

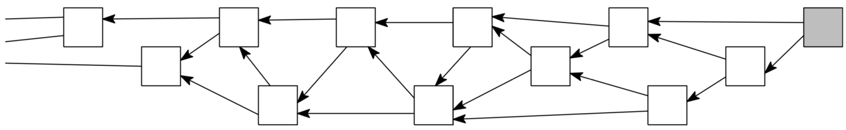


Figure 3.4: A directed acyclic graph. (Source: Popov 2018)

## 3.7 Smart Contracts

The concepts explained so far only allow the storage of raw data. However, there is another way of using DLTs that has not yet been explained but is of utmost interest for application in supply chains. Smart Contracts bring programmability to distributed ledger systems. A smart contract is essentially a computer program including business logic which is stored and executed in the DLT. This makes it possible to handle even more complex agreements than simple transactions on a DLT without the need for trusted third parties. This, in turn, results in fewer transaction costs than in traditional ways of making business.[105] Basically, smart contracts act according to the principle that code is the law. The conditions that are defined in the smart contracts are executed automatically when certain predefined conditions are met.[106]

In fact, the concept of smart contracts has been around way longer than Bitcoin, blockchains, and DLTs. It was Nick Szabo who first wrote about this concept in 1997 and defined a smart contract the following way:

> *"Smart contracts combine protocols, users interfaces, and promises expressed via those interfaces, to formalize and secure relationships over public networks. This gives us new ways to formalize the digital relationships which are far more functional than their inanimate paper-based ancestors. Smart contracts reduce*

[102] Kotilevets et al. 2018.
[103] Sunyaev 2020.
[104] Popov 2018.
[105] Sunyaev 2020, p. 289.
[106] Bashir 2018, p. 262.

> *mental and computational transaction costs, imposed by either principals, third parties, or their tools."*[107]

But before the era of cryptocurrencies these concepts were simply unfeasible. This changed with the advent of Bitcoin. The Bitcoin blockchain already supports simple smart contracts which enable features like multi-signature accounts or time locks. But the most prominent example of a DLT design implementing smart contracts is the Ethereum blockchain which launched initially in 2015. Ethereum has its own programming language, called Solidity, and the Ethereum virtual machine (EVM) that serves as an environment for running smart contracts.[108] Nowadays, there are even more smart-contract compatible DLTs that gain more and more popularity like Polkadot[109], Fantom[110], Avalanche[111], Solana[112], Terra[113] and more.
In this chapter, the most important terms and definitions regarding DLTs were covered as well as the cryptographic basics which are needed for DLTs to work. A differentiation between private and public DLTs was made and in this context also the need for consensus algorithms in DLTs was covered. After an explanation of consensus algorithms in general, some of the most known consensus algorithms are presented. As DLTs can be further differentiated into various DLT concepts, the two most known DLT concepts, a blockchain, and a DAG are also covered. Lastly, smart contracts are described which equip certain DLT designs with more advanced functions than just simply storing transaction data. The next chapter will focus on developing a quantitative evaluation model for DLT applications in the supply chain domain based on a systematic literature review, qualitative interviews, and a quantitative study.

[107] Szabo 1997.
[108] Sunyaev 2020.
[109] **https://polkadot.network**; **23.02.2022**.
[110] **https://fantom.foundation**; **23.02.2022**.
[111] **https://www.avax.network**; **23.02.2022**.
[112] **https://solana.com**; **23.02.2022**.
[113] **https://www.terra.money**; **23.02.2022**.

# 4 A quantitative model to evaluate DLTs with respect to Transparency and Traceability in Supply Chains

In this chapter, the results of the systematic literature review are presented. Based upon these findings a quantitative evaluation model for distributed ledger technologies with regards to increasing the transparency and traceability in a supply chain is developed. The aim of this quantitative evaluation model is to provide a simple framework to decide on a certain DLT design based on these requirements. The findings from the literature review are then validated with the opinions of domain experts. With an empirical study the performance of several DLT designs concerning these requirements is determined, which will be a core building block of the model.

The model should then be available for organisations who are considering an application including a DLT implementation in order to improve the transparency and traceability in their supply chain operations. There is already literature available that covers the aspects of how to define the requirements for supply chain use cases for a DLT implementation. But in all the reviewed articles the selection process of the DLT concept and design was not at all or only minimally covered. Due to several compromises that have to be made, the expectation of one general ideal DLT concept that solves all requirements is unrealistic. The trade-offs that result from the interdependencies between different DLT characteristics are currently most of the time not further investigated.[114] So, this model is aimed at building on what is already available, taking the requirements specifications of the supply chain use cases, and deciding upon a DLT design that is capable of fulfilling those requirements in the best way possible.

## 4.1 Methodology

In order to conduct this thesis properly, the underlying literature needs to be gathered in an organised way. The method for finding the main part of the literature is a systematic

[114] Kannengießer et al. 2019, p. 1.

literature review. The aim of a systematic review is to make the process of searching the literature as transparent and replicable as possible, meaning also to take a fair amount of subjectivity and bias away from the author. Following the process, the author should state clearly all his decisions, procedures, and conclusions. A systematic literature review consists of three phases: planning of the review, conducting the review,and lastly reporting and dissemination of the results.[115]

> *"A good systematic review is based on a well-formulated, answerable question. The question guides the review by defining which studies will be included, what the search strategy to identify the relevant primary studies should be, and which data need to be extracted from each study. Ask a poor question and you will get a poor review."*[116]

The first step for planning the systematic literature review is the identification of a need for a review. This has been already covered in section 1.1.

The second part is conducting the review. Therefore, a research question needs to be identified which can be found in section 1.2. Next, a selection of studies to be included in the systematic literature review needs to be done. And for the sake of total transparency about the process, figure 4.1 shows the used process.

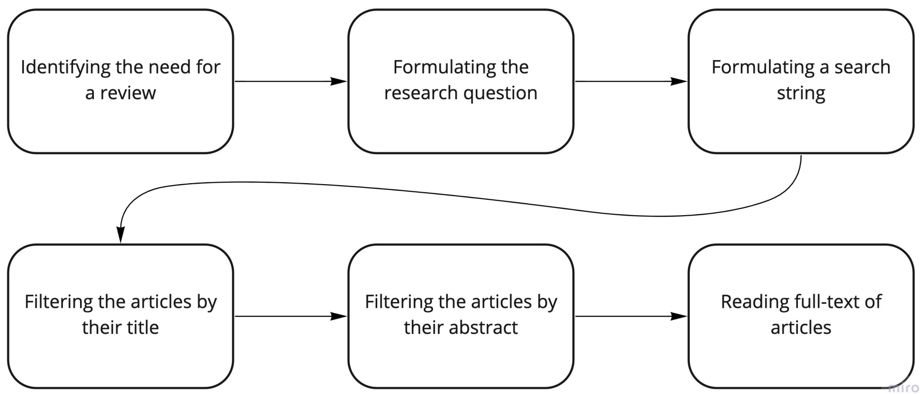



Figure 4.1: The process for the systematic literature review (Source: Tranfield et al. 2003)

In April 2021 a search on the Scopus database was conducted and after some iterations, the search term was limited to *TITLE-ABS-KEY ( ( ( transparency OR traceability ) AND ( supply AND chain ) ) AND ( ( distributed AND ledger AND technology ) OR dlt ) )* , because with this search term, both core topics of this thesis are covered. The publish date was restricted to 2018-2021, because especially the DLT space is evolving fast and

[115]Tranfield et al. 2003, p. 214.
[116]Counsell 1997, p. 380.

articles tracking back more than three years can easily be outdated. In order to be able to read these articles thoroughly, only English articles were included in the search. To make sure the sources for the systematic literature review are credible only articles, book chapters, and conference papers were selected.

This led to a search result of 106 articles, which were then reviewed by their title first. The title had to include any of the following keywords to be included: *blockchain, supply chain, traceability, tracing, transparency, logistics, distributed ledger*. On the other hand, titles that included any of the following words: *smart cities, supply chain sustainability* were excluded as well as titles that gave the impression that their focus lies solely on the underlying software development. Lastly, titles focusing on industry use cases of distributed ledger technologies in general without any mentioning of supply chain and/or related terms were excluded.

This narrowed down the number of articles to 67. In order to make sure that only articles that are relevant to the research question are considered, the number of articles was further narrowed down by reviewing the abstract. The following criteria were applied when reviewing the abstracts.

**Criteria for excluding articles:**

- Abstracts that were not focused on the application of DLT for supply chain management or logistical operations of any kind in an industry.
- Again, articles with the main focus solely on the software implementation.
- Articles, that seemed to have absolutely no takeaway for the topic, in general, were excluded.

**Criteria for including articles:**

- Abstracts that clearly stated the intention of applying DLT in a supply chain use case with a focus on transparency and/or traceability.
- Articles that are aiming to describe the methodologies and the process of how to define blockchain use cases in supply chain management.
- Articles that specifically stated in their abstract, that they cover the definition of necessary processes and transactions for transparency and trust in a supply chain.
- Reviews in the area of blockchain or DLT usage in supply chains with a focus on transparency and/or traceability were also included.

This resulted in a total number of 31 articles to be included in the systematic literature review where the full text was read.

The final part of the literature review, reporting and dissemination of results, will take place in the next chapter. In the following paragraphs, the results of the systematic literature review are presented, prior to the development of the quantitative evaluation model.

## 4.2 Results of the Systematic Literature Review

The process of conducting the systematic literature was already described in detail in section 4.1 in this thesis. Subsequently, the results of the review are presented, which are building the literature basis for the development of the evaluation model. As a first step, the reviewed articles are summarised hereafter.

Agrawal et al. proposed a blockchain-based traceability framework developed on their own which has specific characteristics for the application in the textile and clothing supply chain. The blockchain simulation which they developed is focused on providing data safety, the exchange of traceability information, and technology-based trust.[117] A decentralized NFC-enabled anti-counterfeiting System (dNAS) has been developed as a prototype by Yiu. dNAS is a decentralized system, which is aimed specifically at supply chain applications. It is based on a wide range of system requirements like data integrity, data privacy, and scalability.[118] In their literature review, Asante et al. are giving insights on the relevance of blockchain applications for supply chain security management. They conclude their article by stating that DLT systems are more reliable and less prone to data loss due to their decentralized architecture. But they also note that through the native transparency of a DLT network, sensitive information and other information can be seen and traced.[119] The capabilities of blockchain technology can be even further enhanced by combining it with Internet-of-Things (IoT). Shahzad and Zhang established a proof-of-concept in their article which is intended to cover the end-to-end process of food supply chain management. They integrate IoT sensors with GPS capabilities in order to get exact location data for shipments.[120] Centralized traceability solutions are lacking transparency. This results in the fact, that trust and data can be easily manipulated. This motivated Sunny et al. to consider decentralized applications utilising blockchain technology. Their findings are also presented in a proof-of-concept (PoC), where they implemented blockchain in the case of cold chain management in the pharmaceutical sector, where

[117] Agrawal et al. 2021.
[118] Yiu 2021.
[119] Asante et al. 2021.
[120] Shahzad and Zhang 2021.

the right temperature during storage and transport plays an important role.[121] There are many issues connected to an implementation of blockchain technology in a supply chain application with low scalability and high transaction fees leading to the discussions. By utilising other DLT approaches than blockchain technology, these issues could eventually be eliminated. Suhail et al. present a supply chain application that is based on the IOTA directed acyclic graph (DAG) in order to point out that there are far more possibilities than blockchain technology.[122] Ko et al. are proposing the implementation of a private blockchain network for tracking stainless steel throughout its production.[123] The article written by Schinle et al. is focusing on the aspects of how certain information can be disclosed in a DLT supply chain application. Certain requirements are specified and finally, a PoC which is based on a food supply chain application is presented.[124] Among other things, there is one core contradiction that has to be considered for the application of blockchain technology in supply chains. This is on one hand improving the transparency along the chain but on the other hand keeping sensitive information confidential. Ghode et al. are investigating this contradiction and are presenting a basic theoretical architecture for implementing blockchain technology in supply chains.[125] Together with a logistics company Maden and Alptekin assessed critical factors for a successful blockchain technology implementation in the supply chain sector.[126] Kumar et al. propose a framework to implement a private blockchain to secure the logistics and supply chain operations of an organisation. The framework is then also applied in a proof-of-concept in the pharmaceutical sector. Various different smart contracts were developed for operations like trading assets and exporting or importing assets.[127] When talking about blockchain applications for use in supply chains, smart contracts are an important building block. Terzi et al. are showing a large focus on smart contracts and are exploring two different supply chain use cases in their article. Furthermore, they are presenting pseudo-code for the respective smart contracts which should act as generic templates for further developments in this sector.[128] Wu et al. are discussing potential opportunities, requirements, and principles for designing blockchain implementations for supply chain management systems. They also identify technical challenges for the adoption of blockchain technology and present a case study in the food sector where the challenges and opportunities were addressed directly.[129] Reimers et al. developed a prototype of a blockchain application for the car supply chain. For the identification of the car, they used RFID labels. The prototype is

[121] Sunny et al. 2020.
[122] Suhail et al. 2020.
[123] Ko et al. 2020.
[124] Schinle et al. 2020.
[125] Ghode et al. 2020.
[126] Maden and Alptekin 2020.
[127] Kumar et al. 2020.
[128] Terzi et al. 2019.
[129] Wu et al. 2019.

depicted in reality with a toy car, with one production step, quality assurance, and transportation.[130] Blockchain technology is often also considered for supply chain applications because a heavy amount of information asymmetry exists among stakeholders. This inspired Kim et al. to create a prototype named "Harvest Network", which is a blockchain implementation on the Ethereum blockchain, specifically for food traceability from farm to fork.[131] A similar approach is taken by Caro et al. who are introducing "AgriBlockIoT". A blockchain solution for agricultural and food supply chain management. Interestingly, they implemented their prototype on two different blockchain networks and compared them with each other.[132] By conducting a case study with an Australian electrical manufacturing company, Maroun and Daniel propose the implementation of blockchain technology in order to enhance the authentication of products in different stages of the supply chain.[133] Shi et al. are building a blockchain and Internet-of-Things framework for the pharmaceutical sector which is based on the private Hyperledger Fabric protocol. The authors are heavily focusing on privacy issues of blockchain technology and are employing various encryption methods, to ensure that sensitive data is protected.[134] Another area of application for blockchain technology is the mining and metals industry. Mann et al. are investigating blockchain technology and its different possible use cases in this industry.[135] Furthermore, Liao and X. Wang are showing, that blockchain technology could also enhance logistics operations in integrated casinos and entertainment by introducing pseudo-code smart contracts which are developed in the scope of a PoC specifically for this industry.[136] Inconsistent data and lack of trust between various supply chain players are also often leading to friction regarding the document and workflow management. By proposing a basic framework built on the open-source Hyperledger Fabric network, Z. Wang et al. are showing how these paper-based processes could be digitalised in a secure manner.[137] With the help of Microsoft Azure Blockchain Workbench, Figorilli et al. developed a simulation in order to trace wood along its supply chain in a decentralized fashion. For the identification, RFID labels have been integrated into the solution.[138] Another present issue in supply chain management is the bullwhip effect, which is induced by a lack of information sharing between partners in a supply chain among other things. With this in mind, Engelenburg et al. are designing and evaluating a blockchain architecture with the aim of reducing the bullwhip effect.[139] Perboli et al. are introducing a standard and repeatable methodology to design blockchain projects regarding their digital strat-

[130] Reimers et al. 2019.
[131] Kim et al. 2018.
[132] Caro et al. 2018.
[133] Maroun and Daniel 2019.
[134] Shi et al. 2019.
[135] Mann et al. 2018.
[136] Liao and X. Wang 2018.
[137] Z. Wang et al. 2018.
[138] Figorilli et al. 2018.
[139] Engelenburg et al. 2018.

egy. To apply this methodology also in practice, they present a use case in the fresh food supply chain.[140] Kolb et al. are focusing on the specific part of vendor-managed inventory (VMI) in supply chain management and are seeing potential future improvements from blockchain technology in this area. They also developed a prototype application on the Ethereum Ropsten test network.[141]

As it can be seen, the articles in the literature review cover a wide range of blockchain applications for supply chain management throughout different sectors of industries. In order to answer the research question exhaustingly, the full-text articles found by conducting the literature review were analysed regarding the following two questions which are worth repeating at this point of the thesis:

- Which specifications and requirements are important to consider, when it comes to transparency and traceability applications in supply chains?
- How well do different DLT designs perform regarding the specifications and requirements of different supply chains?

With these questions in mind, the literature was reviewed in detail and a summary of the key components of each of the articles can be found in table 4.1. First of all, it is important to consider the methodology of the article, as the research included literature reviews and case studies. The literature was analysed on a high level to find out key components of each article and to get a good overview of the articles. Did it encompass only the concept on paper of an application or also an implementation? On which kind of DLT concept was the case study based on? Which DLT design was used/was referred to in the article? Was it a permissioned or public DLT implementation that was considered? On which industry sector was the case study based on?
Based on these factors the articles can be better understood and the scope of each case study can be brought into context.

[140] Perboli et al. 2018.
[141] Kolb et al. 2018.

Table 4.1: Summary of articles

| **Author(s)** | **Methodology** | **Goal** | **Implementation** | **Industry** | **DLT Concept** | **DLT Design** | **Private or Public** |
|---|---|---|---|---|---|---|---|
| Agrawal et al. 2021 | Case Study | Improve traceability | Simulation | Textile and Clothing | Blockchain | self developed | private |
| Yiu 2021 | Case Study | Anti-Counterfeiting | Prototype | Wine Industry | Blockchain | Ethereum Proof-of-Authority | private |
| Asante et al. 2021 | Literature Review | Supply Chain Security Management | - | - | - | - | - |
| Shahzad and Zhang 2021 | Case Study | End-to-End Supply Chain Management | Proof of Concept | Food Sector | Blockchain | Hyperledger Fabric | permissioned |
| Sunny et al. 2020 | Case Study | Improve supply chain transparency | Proof of Concept | Pharmaceutical Sector | Blockchain | Microsoft Azure Blockchain Workbench (Proof of Authority Ethereum) | Private |
| Suhail et al. 2020 | Case Study | Improve traceability | Proposed Framework | Electronics Industry | DAG | IOTA Tangle | Public |

Continued on next page

Table 4.1: Summary of articles continued

| **Author(s)** | **Methodology** | **Goal** | **Implementation** | **Industry** | **DLT Concept** | **DLT Design** | **Private or Public** |
|---|---|---|---|---|---|---|---|
| Ko et al. 2020 | Case Study | Anti-Counterfeiting | Proposed Framework | Steel Industry | Blockchain | Hyperledger Fabric | Private |
| Schinle et al. 2020 | Case Study | Protect trade secrets | Proof of Concept | No specific industry | Blockchain | Hyperledger Fabric | permissioned |
| Ghode et al. 2020 | Literature Review | Improve supply chain transparency | - | - | - | - | - |
| Maden and Alptekin 2020 | Literature Review | Assessing critical factors for a successful blockchain implementation | - | - | - | - | - |
| Kumar et al. 2020 | Case Study | Securing Supply Chain and logistics operations | Proof of Concept | Pharmaceutical Sector | Blockchain | Ethereum Ropsten Test Network | Private, permissioned |
| Terzi et al. 2019 | Case Study | Improve traceability | Proposed Framework | Food Sector | Blockchain | - | - |
| Wu et al. 2019 | Case Study | Technical challenges for applying blockchain for SCM in practice | Minimal-Viable-Product | Food Sector | Blockchain | Hyperledger Fabric | permissioned |

Continued on next page

Table 4.1: Summary of articles continued

| **Author(s)** | **Methodology** | **Goal** | **Implementation** | **Industry** | **DLT Concept** | **DLT Design** | **Private or Public** |
|---|---|---|---|---|---|---|---|
| Reimers et al. 2019 | Case Study | Ensure Transparency of production | Proof of Concept | Automotive Industry | Blockchain | Hyperledger Composer (Hyperledger Fabric) | permissioned |
| Kim et al. 2018 | Case Study | Improve supply chain transparency | Proposed Framework | Food Sector | Blockchain | Ethereum | Public |
| Maroun and Daniel 2019 | Case Study | Summary of opportunities for BC in supply chains | Proposed Framework | Electronics Industry | Blockchain | Not available | Private |
| Shi et al. 2019 | Case Study | Improve supply chain transparency | Proof of Concept | Pharmaceutical Sector | Blockchain | Hyperledger Fabric | permissioned |
| Mann et al. 2018 | Literature Review | Outline several key applications of blockchain for the mining industry | - | - | - | - | - |

Continued on next page

Table 4.1: Summary of articles continued

| **Author(s)** | **Methodology** | **Goal** | **Implementation** | **Industry** | **DLT Concept** | **DLT Design** | **Private or Public** |
|---|---|---|---|---|---|---|---|
| Liao and X. Wang 2018 | Case Study | Design and application of blockchain in ICE (Integrated Casinos and Entertainment) logistics | Proof of Concept | Integrated Casinos and Entertainment (ICE) | Blockchain | Ethereum | Not available |
| Z. Wang et al. 2018 | Case Study | Achieve a higher level of efficiency | Proposed Framework | Transport Industry | Blockchain | Hyperledger Fabric | Permissioned |
| Figorilli et al. 2018 | Case Study | Improve traceability | Simulation | Wood Industry | Blockchain | Microsoft Azure Blockchain Workbench (Proof of Authority Ethereum) | Private |
| Caro et al. 2018Caro et al. | Case Study | Improve supply chain transparency | Simulation | Food Sector | Blockchain | Ethereum and Hyperledger Sawtooth | Private |
| Engelenburg et al. 2018 | Literature | Reduce the Bullwhip effect | Proposed Framework | No specific industry | Blockchain | Not available | private |

Continued on next page

Table 4.1: Summary of articles continued

| **Author(s)** | **Methodology** | **Goal** | **Implementation** | **Industry** | **DLT Concept** | **DLT Design** | **Private or Public** |
|---|---|---|---|---|---|---|---|
| Perboli et al. 2018 | Case Study | Create a standard methodology to design blockchain technology use cases apart from the finance industry | Proof of Concept | Food Sector | Blockchain | Hyperledger Fabric | Private |
| Kolb et al. 2018 | Case Study | Improve VMI solutions | Prototype | No specific industry | Blockchain | Ethereum Ropsten Test Network | Private |

There are several key takeaways already from the listing in table 4.1. First of all, there are 20 case studies conducted spanning 13 different industries. That shows that the application of distributed ledger technology in supply chains is not restricted to certain industries. Although it can be seen, that most articles conducted a case study with the food sector as a focus (6 articles). This can be argued with the relevance of transparency across the supply chain, especially for the end consumers. On one hand, the awareness for food sustainability on the consumer side is rising, and on the other hand because traceability is important in the case of product recalls for food gone bad.[142]

Secondly, DLT and its application to logistics and supply chain management is still in its infancy. (Sunny et al. 2020; Asante et al. 2021) None of the case studies covered an implementation that was going to get used in a production environment. Most articles proposed a theoretical framework or showed a proof-of-concept, for example by producing pseudo-code for the smart contracts. Only in 6 cases the code was also deployed and tested. The most outstanding factor although is, that DLTs, in general, are basically not covered. All but one case study implemented a blockchain, for the use case without even considering any other DLT concept or design. Only in one article, the IOTA DLT which builds on a DAG is used.[143]

In most of the case studies private or permissioned DLT frameworks are used for the proof-of-concept or for the simulation implementation. The argumentation leading up to the selection of the DLT framework is most of the time missing or it is only minimally covered. It is also interesting to see, that some proof-of-concepts were implemented on a test network, which for pure testing of the functionality is a valid option, but does not consider at all if an application on the corresponding main network would be feasible.[144]This fact emphasizes the importance of this work to raise awareness for the selection of the appropriate DLT design for a supply chain use case, based on the characteristics of the various DLT designs.
In this section, the results of the systematic literature review are summarised. Starting with the next section the focus will be on answering the research questions of this thesis specifically.

### 4.2.1 State-of-the-Art of the DLT selection process

The selection of the appropriate DLT framework is only one part of the development of a supply chain application based on DLT. Beforehand, other decisions have to be made and the scope of the application has to be defined. These phases of the process are already

[142] Shahzad and Zhang 2021; Wu et al. 2019; Caro et al. 2018.
[143] Suhail et al. 2020.
[144] Kumar et al. 2020; Kolb et al. 2018.

covered in the literature. In order to provide full completeness regarding the development of a supply chain application based on DLT, also the phases leading up to the decision about the DLT framework are described briefly here:

As a first step considering a DLT application for supply chain use cases, a company should evaluate their needs and their expectations concerning the application. Maden and Alptekin provide a simplified evaluation framework, which should help decide about the implementation of a blockchain/DLT or a traditional database.[145] If DLT is the technology of choice, the next step is to define the roles and the operations of the system as it is done for example by Agrawal et al., Yiu and Kumar et al. The roles include all the participants in the supply chain system like for example the producer, manufacturer and the customer. The operations in the system are defining the actions or functions that the roles should be able to execute within the application, which could be for example the creation of a new asset, append data to an asset, transfer the ownership of an asset or read data from an asset.[146]

In order to find out more data about the DLT implementations and the underlying considerations, the following three questions were formulated:

1. What are the underlying issues? Specifically, what are currently missing properties of the supply chain or challenges for information systems in SCM?
2. What are the general expectations of the DLT application for the supply chain? How can a DLT solution help with those issues and challenges?
3. What are the main requirements and parameters that were considered in the supply chain application?

Based on these questions, the literature from the systematic literature review was analysed thoroughly and a great number of issues, expectations and parameters were identified. Due to the fact that some factors are just the same but only formulated in another way or that one or more factors have the same root, as a next step clustering was applied to the results. In this way, the main results were synthesised from the available literature.

### 4.2.2 Underlying issues

First of all, the articles were analysed regarding the underlying issues of the supply chain use cases. These issues are the reasons that were mentioned, **why** a DLT solution was even considered for this specific supply chain application. As the use cases are positioned

[145] Maden and Alptekin 2020.
[146] Agrawal et al. 2021; Yiu 2021; Kumar et al. 2020.

in various different industries, some issues are very specifically linked to one certain use case. But again, by clustering all different issues that were found, seven universal issues could be identified.

- **I1 - Visibility and Transparency:** Visibility and Transparency are the most often mentioned issues in the articles. Especially in the information flow of a supply chain a lack of transparency and low visibility up- and downstream are dominant issues. This leads to other issues mentioned, that fall into this category like information asymmetry when information is processed and used in a monopolistic way, and a certain opaqueness along the supply chain. This makes it also hard to monitor the supply chain risks properly. Moreover, nowadays often the end consumers are demanding a certain amount of transparency across the supply chain, because they want to assess their product in terms of sustainability, child-labour, and other factors. Another issue that is mentioned very often, which could be argued as a child issue and is therefore included here, is the lack of information sharing between partners in a supply chain. First and foremost, the participants do not want to share competitive and privacy-sensitive information with other players in the supply chain, because this data could be used against them in some situations. But even if they want to share the information with each other it is quite hard because of the heterogeneity of actors, stakeholders, and business models in a typical supply chain. Moreover, it is also complicated to share data across a supply chain, because there is often a lack of interoperability between the different information systems. Those are siloed legacy information systems where gathering data from multiple different sources and keeping it up to date is a challenge. Especially, for global supply chains, where it is impossible to have direct contact with all other organisations in the supply chain. Lastly, it is also mentioned, that supply chain benefits rely heavily on a network effect, which can be only properly achieved by information sharing.[147]

- **I2 - Data Tampering:** There are a lot of possibilities in legacy supply chain information systems where data can be tampered with. However, in most industries, it is critical that forgery and alteration of documents, data, or transactions is not possible. Because infiltrations of the product quality or even counterfeit products can not only harm the brand image, in some industries this could also harm human lives. Another issue that was mentioned in this regard is the threat of faulty data entries.[148]

[147] This issue was mentioned in: Agrawal et al. 2021; Asante et al. 2021; Ghode et al. 2020; Wu et al. 2019; Kim et al. 2018; Maroun and Daniel 2019; Liao and X. Wang 2018; Z. Wang et al. 2018; Caro et al. 2018; Schinle et al. 2020; Sunny et al. 2020; Shi et al. 2019; Engelenburg et al. 2018; Reimers et al. 2019; Suhail et al. 2020; Mann et al. 2018; Perboli et al. 2018.

[148] This issue was mentioned in: Schinle et al. 2020; Ghode et al. 2020; Wu et al. 2019; Ko et al. 2020; Shi et al. 2019; Ghode et al. 2020; Kumar et al. 2020; Maroun and Daniel 2019; Sunny et al. 2020; Shi et al. 2019; Asante et al. 2021; Caro et al. 2018.

- **I3 - Trust:** Obviously, trust is also a prevalent issue in supply chains. Certainly, it is hard for new participants, to establish trust within a short matter of time and it is especially challenging to trust data from various logistics providers, suppliers etc. It is also fairly hard to keep a balance between privacy and trust.[149]

- **I4 - Centralisation:** Nowadays, supply chain information systems rely on a heavily centralised infrastructure. Either provided by cloud providers or their own facilities. This implies the risk of a single-point-of-failure for the whole system. Moreover, from the infrastructure side, this also involves some sort of third-party dependency on trusted parties or intermediaries. In certain relationships, the power of centralisation can also be used to negatively influence transparency and trust in the system by deliberately making parts of the supply chain opaque.[150]

- **I5 - Traceability:** With inconsistent data flow and potential loss of documents, traceability also becomes an important issue. A complex tracking process makes it hard to trace events and investigate potential issues along the supply chain. Therefore it is hard for certain stakeholders to control the integrity of certain assets.[151]

- **I6 - Inefficiencies and Costs:** Due to data inconsistency, obstruction of operations, competitiveness, inequality, and the non-optimal use of resources, a lack of information inefficiencies can arise in supply chains. Furthermore, there are high initial investments necessary for the implementation of a supply chain information system. Also, the processing of documents and the administration is connected to the occurrence of certain costs in a supply chain, for which the goal always is to minimise them.[152]

- **I7 - Data Governance & Standardisation:** The issues mentioned the least, are connected to data governance and standardisation. Currently, there is an issue with misconceptions among different supply chain players relating to data definitions and standard data formats are lacking. Moreover, issues like a lack of regulations and a lack of data governance were mentioned.[153]

[149] This issue was mentioned in: Shahzad and Zhang 2021; Asante et al. 2021; Sunny et al. 2020; Schinle et al. 2020; Ghode et al. 2020; Shi et al. 2019; Liao and X. Wang 2018; Z. Wang et al. 2018; Kolb et al. 2018.

[150] This issue was mentioned in: Yiu 2021; Sunny et al. 2020; Perboli et al. 2018; Caro et al. 2018; Kumar et al. 2020; Suhail et al. 2020.

[151] This issue was mentioned in: Maroun and Daniel 2019; Wu et al. 2019; Shi et al. 2019; Caro et al. 2018; Liao and X. Wang 2018; Z. Wang et al. 2018; Kumar et al. 2020.

[152] This issue was mentioned in: Liao and X. Wang 2018; Asante et al. 2021; Shi et al. 2019; Figorilli et al. 2018; Shahzad and Zhang 2021; Wu et al. 2019; Z. Wang et al. 2018; Kolb et al. 2018.

[153] This issue was mentioned in: Caro et al. 2018; Kim et al. 2018; Ghode et al. 2020.

### 4.2.3 How a DLT solution is expected to help in those issues and challenges

Secondly, the expectations mentioned in the articles regarding a DLT application for the supply chain were gathered. Again, the mentioned expectations were clustered together, this time according to specific areas in which the expectations should bring improvements.

- **E1 - Overall Supply Chain:** Authors of case studies expect above all improved traceability and transparency for the whole supply chain with an implementation of DLT. Furthermore, the overall supply chain is expected to profit from improved efficiency and increased cyber resilience. All of these expectations are also closely related to the fact that effective and improved trust between supply chain participants is anticipated.[154]

- **E2 - Communication:** There are also big expectations regarding improvements in the communication flow in a supply chain. Currently, it is not really possible to share information and data in a trustable and secure manner between different companies. Especially in this regards the expectations for DLTs are immense. It is expected that data silos can be broken down, optimized and information sharing between numerous parties will be made possible. Furthermore, DLT could enable secure access to confidential information, by abstracting the data on the protocol level. Meaning, that for example data can be gathered in a DLT protocol and aggregated on-chain. Then only aggregated data can be accessed by certain parties, but not the granular data pieces.[155]

- **E3 - Economics:** Relating to economic benefits from the adoption of DLT some authors mention the possibility to gain a competitive advantage compared to other companies. Obviously, from an economic perspective, it is expected, that costs can be saved and profits can be increased. In some industries, it is also argued, that DLT could help with reducing the waste of goods.[156]

- **E4 - Process:** With the implementation of a DLT application in the supply chain, many authors also expect effects on the operational and organisational processes within the supply chain and the companies. Processes could be streamlined, by eradicating redundancies in the supply chain. Moreover, this could also enhance

[154] This expectation was mentioned in: Suhail et al. 2020; Kumar et al. 2020; Kim et al. 2018; Caro et al. 2018; Asante et al. 2021; Shahzad and Zhang 2021; Maroun and Daniel 2019; Shi et al. 2019; Perboli et al. 2018.

[155] This expectation was mentioned in: Kolb et al. 2018; Agrawal et al. 2021; Wu et al. 2019; Reimers et al. 2019; Shi et al. 2019; Liao and X. Wang 2018; Engelenburg et al. 2018; Maroun and Daniel 2019; Caro et al. 2018.

[156] This expectation was mentioned in: Asante et al. 2021; Ghode et al. 2020; Perboli et al. 2018; Wu et al. 2019; Kumar et al. 2020; Kim et al. 2018; Schinle et al. 2020.

cross-organisational or payment processes by automating them and e.g. saving time for data retrieval. Overall, a more efficient workflow management is envisioned.[157]

### 4.2.4 Main Requirements and Parameters considered in Supply Chain Applications

In total, 22 different factors and parameters, which were considered for the DLT implementation in a supply chain application, were mentioned in the surveyed articles. Most of them were at least mentioned in two separate articles. They were categorised into three different categories, which are the technical level, the user level and the data level.

Table 4.2: Parameters

| **Level** | **Name** | **Description** |
|---|---|---|
| User | Access Control | Based on their role in the supply chain the actors should have different access rights. Moreover, data should be only accessible to parties in the same supply chain. |
| User | Authentication and Authorization | The application should provide the possibility for users to be authenticated, e.g. with validateable and readable IDs. Moreover it should provide the possibility to authorize certain users for certain actions. |
| User | User Interface | The interface should be user friendly, understandable and easy to operate. |
| User | Flexibility regarding Users | Support for multiple participants with different business needs. |
| User | Identity Privacy | Complete privacy of the real identities behind certain actors or nodes. |
| Technical | Scalability | The ability to handle a growing amount of work within the system. |
| Technical | Flexibility regarding Integration | Being able to integrate applications, that are already in use and other technologies which are needed for a supply chain application like for example sensors and auto-id technologies. |
| Technical | High Reliability | The ability of a system to produce correct results over a certain amount of time. |

[157] This expectation was mentioned in: Ghode et al. 2020; Shi et al. 2019; Wu et al. 2019; Z. Wang et al. 2018.

| Level | Name | Description |
|---|---|---|
| Technical | Low Latency | The delay between a user's action and the applications response is the latency. A low latency (short delay) is required. |
| Technical | High Transactions per Second | The amount of updates that can be performed on the application in a certain timeframe should be as high as possible. |
| Technical | Availability | The more time a system is actually operational compared to the planned operation time, the larger is the availability. |
| Data | Security | Data should be protected from unauthorized access and corruption. |
| Data | Encryption | Data can be made unreadable using certain encryption methods. It can only be decrypted and read with the correct encryption key. |
| Data | Authentication | Data authentication is the confirmation of the origin and the integrity of the data. Data authenticity should be protected and the duplication of records should be made impossible. |
| Data | Provenance | Chronological record of the history of a specific object, e.g. including data about the ownership or the location of the asset at a specific time. |
| Data | Forecasting | Process of making predictions based on historical data. Since the quality of historical data should improve due to other specifications, also the forecast quality should improve. |
| Data | Confidentiality | Data should be protected against unintentional or unauthorized access, disclosure or theft. |
| Data | Immutability | Data in the supply chain application should not be able to be changed or tampered with. |
| Data | Data Privacy | Data privacy is concerning the governing of how data can be collected, shared and used. |
| Data | Integrity | Refers to the accuracy and consistency of the data over its entire lifecycle. |
| Data | Validity | Ensures that the data is correct and useful. |
| Data | Quality | Measures the condition of data in terms of various factors, like for example accuracy and completeness among others. |

## 4.3 Different DLT Designs from the Literature Review

The articles were also reviewed in terms of the DLT designs which were introduced or used in the scope of a case study or proof-of-concept. The different DLT concepts and designs in each article are already outlined in table 4.1. Consequently, the DLT designs depicted in figure 4.2 were implemented in at least one article in the systematic literature review.

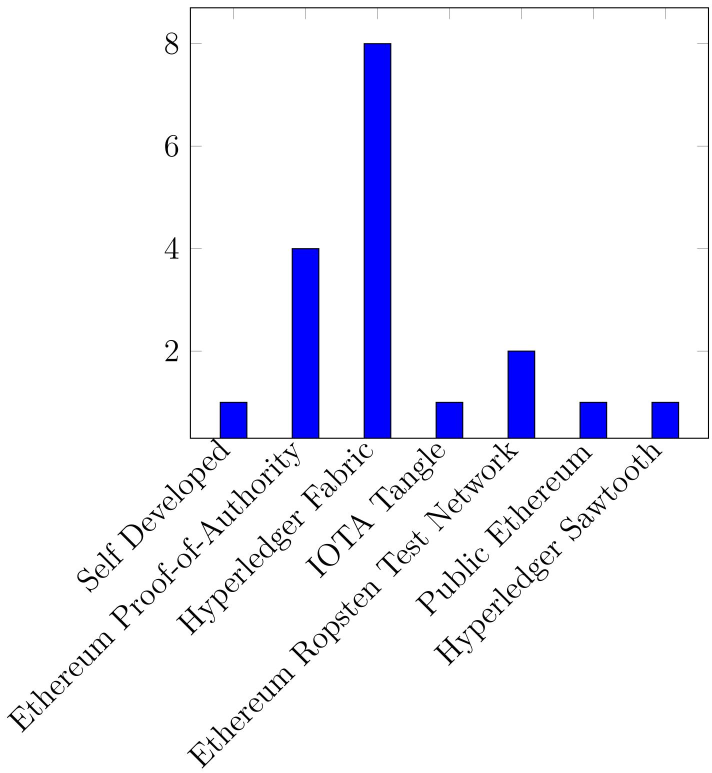



Figure 4.2: DLT designs from the systematic literature review

Since it is not possible to quantify the characteristics and configurations of a self developed DLT, this won't be considered in the ongoing efforts.

The literature research covers several recent implementations of DLT applications for supply chains, the DLT designs that were mentioned and used in the case studies serve as a good starting point for the ongoing efforts. In the scope of this thesis, also the available information from these DLT designs was studied and some characteristics were researched. In order to get an introduction to the DLT design that will play an important role in the next sections, each one of those is introduced shortly subsequently. The detailed research with the characteristics can be found in appendix 7.2.

### 4.3.1 Ethereum Public Network

Ethereum Mainnet is a public blockchain network built on a proof-of-work consensus mechanism. It is although planned to switch to the more energy-efficient Proof-of-Stake consensus in the near future (approximately in the timeframe of 2021-2022).[158] In order to use the network for transactions or for the deployment of smart contracts transaction fees (also called gas fees) need to be paid in Ether (ETH). Ether is the underlying cryptocurrency to the Ethereum network.[159]

### 4.3.2 Ethereum Ropsten Test Network

As Ethereum is a protocol, there are several networks that are implementing this protocol independently from each other. There are various test networks (Testnets) for Ethereum, where developers can test the functionalities of their smart contracts without having to pay real ETH for transaction fees. The Ropsten test network is the only Ethereum test network that is based on a proof-of-work consensus mechanism, therefore at the moment, this is the best representation of the Ethereum Mainnet. Apparently, some articles from the literature review also used the Ropsten test network to build proof-of-concepts or prototypes of their supply chain application.[160]

### 4.3.3 Ethereum Proof of Authority

The Ethereum protocol can be also deployed in a private network where all nodes are known to each other and trusted by each other. In this case, the nodes are not connected to any public Ethereum network (neither mainnet or testnet). Because of that, a simpler consensus algorithm known as proof-of-authority can be used in such networks.[161]

### 4.3.4 Hyperledger Fabric

Hyperledger is a global collaboration of leaders in finance, manufacturing, Internet of Things and supply chain. It is hosted under the Linux Foundation. Hyperledger itself does not promote a single blockchain project, it is rather an open-source community of developers who are developing several different pieces of infrastructure and code.

Hyperledger Fabric specifically is a platform that enables distributed ledger solutions to be built in a modular fashion. Through this flexibility, solutions built on Hyperledger Fabric

[158]Community 2021e.
[159]Community 2021b.
[160]Community 2021c.
[161]Community 2021c.

can be adapted for any industry. In contrast to most other DLT designs, Hyperledger Fabric does not rely on any native cryptocurrency.[162]

### 4.3.5 Hyperledger Sawtooth

Hyperledger Sawtooth is a platform that provides tools to build, deploy and run distributed ledgers in a modular way. The strength of Sawtooth is its modularity and flexibility, for example, is it possible to change the consensus algorithm while the blockchain is running. Furthermore, it is compatible with Ethereum smart contracts. It also provides the consensus algorithm Proof of elapsed time (PoET), which provides the scalability of Proof-of-Work without the drawback of high power consumption.[163]

### 4.3.6 IOTA Tangle

IOTA is an open and feeless data and value transfer protocol, specially designed for the Internet-of-Things (IoT) industry. The main differentiation to all other previously mentioned DLT designs is that IOTA builds upon a DAG called "The Tangle". More theoretical background on this subject was already provided in section 3.6. This concept brings with it advantages as well as disadvantages, as it can be seen in the following characteristics.[164][165]

## 4.4 Extending the findings of the Systematic Literature Review

In this part of the thesis the empirical part will be covered, starting by explaining the scientific method and process that was used to gather this knowledge. Afterward, the selection criteria for the experts are presented, before the details and the execution of the study are covered.

### 4.4.1 Scientific Method and Process

Generally, it can be differentiated between two different ways of conducting empirical studies.[166] On one hand, there are quantitative methods, which are typically executed with standardised methods and measurements while encompassing very large and representative samples. Often, such methods are also including surveying numerical values which can be statistically evaluated. On the other hand, there are qualitative methods

[162] H. W. P. W. Group 2018.
[163] H. W. P. W. Group 2018.
[164] Popov 2018.
[165] Services 2021.
[166] Gläser and Laudel 2010, p.24.

available. A qualitative study is deliberately very unstructured and conducted with a relatively small sample size. The feedback is generally collected verbally, visually, and/or audiovisually and is used to be interpretatively evaluated.[167]
After a thorough review of the outcomes of the systematic literature review, it became clear that for the objective of this thesis, the parameters are the key items to be considered in the ongoing efforts. In order to validate these findings and enhance them into a fully viable basis for a quantitative evaluation framework, additional input is needed. In order to gain new information on the research question, expert interviews with 5 experts were conducted. The interviews are split up into two studies: A preliminary study, consisting of qualitative interviews, with the main goal of evaluating which parameters are important to consider. And the main study, consisting of a quantitative survey, with the focus on rating the performance of certain DLT designs regarding those parameters. The detailed process that was followed during the empirical study can be seen in figure 4.3

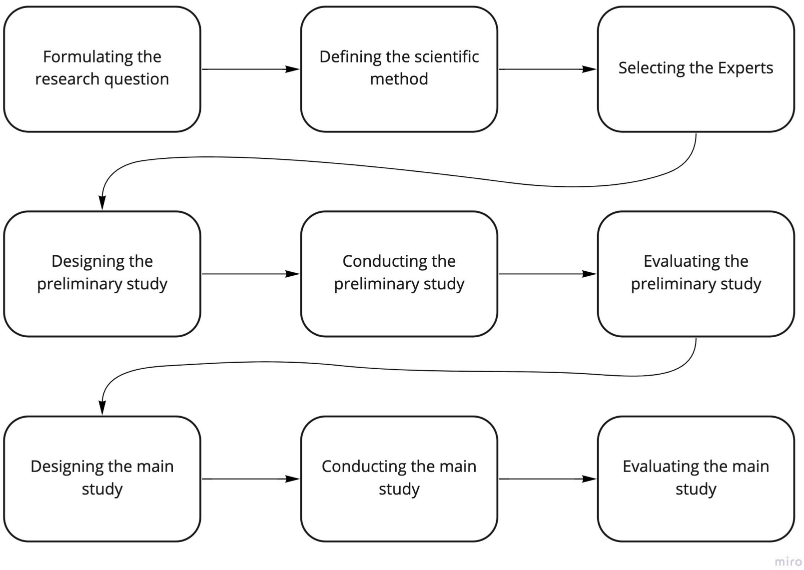



Figure 4.3: The scientific process for the empirical part

## 4.4.2 Selection of the Experts

The experts who were selected for participation in the study had to have at least one of the following prerequisites. The characteristics of the selected experts can be seen in 4.3.

- Deep understanding of DLTs and blockchain technology in general.
- Practical working experience with DLT applications.
- Deep knowledge of the involved DLT designs.

[167]Döring and Bortz 2016, pp. 25-26.

| Expert | Years of DLT Experience | Position | Business Sector |
|---|---|---|---|
| 1 | 4 | Tech Innovation Strategy Manager | Secondary & Tertiary Sector |
| 2 | 9 | CEO | Blockchain/DLT Platform Development |
| 3 | 6 | CEO | IT/DLT |
| 4 | 4 | Tech Lead | IT/DLT |
| 5 | 5 | Technical Project Lead | IT/DLT |

Table 4.3: Profiles of the experts

### 4.4.3 Empirical evaluation of DLT Parameters

The preliminary study was conducted via an online video meeting with the experts where the audio was recorded. It was started with a short introduction to the author, the title, and the vision of the thesis as well as the current status and the purpose of the interview. The interview was structured partly explorative and partly fully standardised, meaning there was a part with closed questions and closed answer alternatives, but also sections where the interviewees could freely tell what is on their mind.[168] The goal of the preliminary study was to validate and refine the number of parameters found in 4.2.4. In order to find out about potential parameters that were not found in the literature review at all, the interview was started with the following open question:

> *"Which parameters are important to consider for a DLT implementation in a supply chain context?"*

Afterward, the findings of the literature review were discussed with the participants, and aspects of importance of the specific parameters were discussed. The experts were shown a list of the parameters that were found and were asked to rank the parameters with the help of a 4-leveled Likert scale. Moreover, they had the possibility to ask questions about the parameters and get clarifications on their definition in the scope of the thesis, as well as the chance to add any parameters for each level and provide other input. The study design can be seen in figure 4.4.

Before concluding the interview, the experts were explained how the further proceedings will look like and what they have to expect from the main study. The whole video call for the preliminary study took about 25-40 minutes.

[168] Döring and Bortz 2016, p. 363.

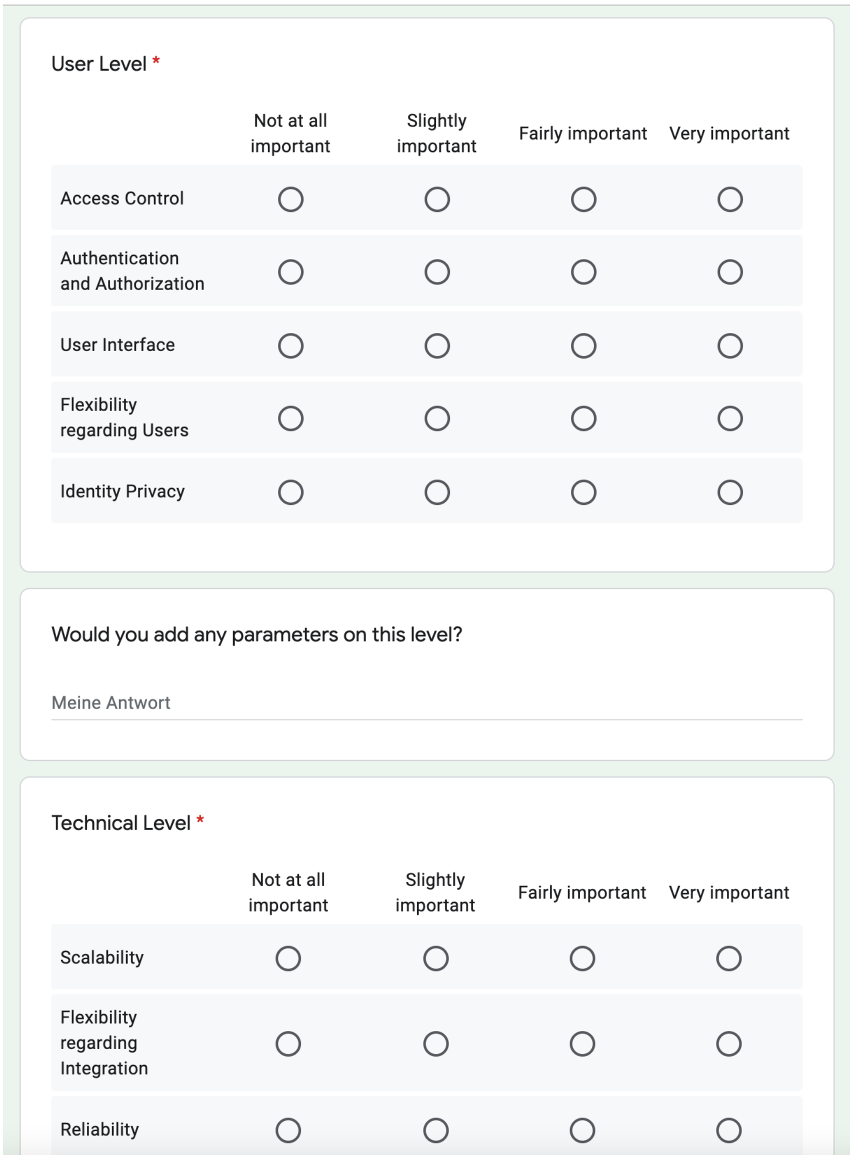



Figure 4.4: Design of the preliminary study

#### 4.4.3.1 Responses to the Preliminary Study

After the preliminary study was conducted with the experts, the evaluation took place. Following, the most important takeaways and results are included:

As feedback to the first question, which parameters are important to consider for a DLT implementation in a supply chain application, there are five arguments worth mentioning:

- Setup Costs: How complicated is it to set up the DLT implementation? Which resources are needed?
- Ongoing Costs: Costs for transactions and/or running and maintaining nodes.
- B2C or B2B: Is the DLT implementation targeted for a B2C (business-to-consumer) or a B2B (business-to-business) supply chain application?

- Collaboration: For the success of a supply chain application with DLT, collaboration among all involved parties in a supply chain is important.
- Customers: A DLT implementation is currently always considered as an "add-on" or a "nice to have" in supply chain applications, therefore it is also important to consider the customer's opinion about that.

Following, all of the three levels and the answers are represented separately.
**The User Level:** The responses to the parameters on the user level are depicted in figure 4.5.

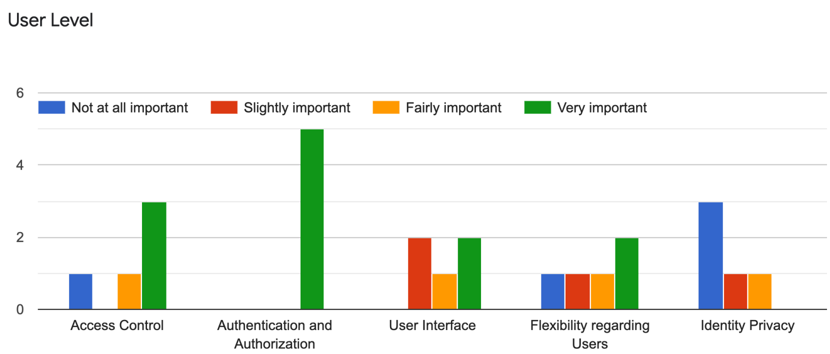



Figure 4.5: Responses: User Level

Furthermore, it was mentioned, that the two parameters "Authentication and Authorization" and "Access Control" can be merged because they are heavily connected. Regarding the importance of the parameter "User Interface", again, the point came up that it is important in this regard to know whether the application is focused on B2C or B2B. The factor of "Cost of Deployment" was also mentioned as a possible additional parameter.

**The Technical Level:** The responses to the parameters on the technical level are depicted in figure 4.6.

Additional comments regarding this category were that also "Interoperability" and "Incentive to use the network" may be important factors. There were also concerns regarding the importance of the parameters "Scalability", "Low Latency" and "High Transactions per Second" because they can be heavily dependent on certain specifications of different supply chain use cases and therefore may not be suited for consideration on such a high level. Moreover, it was mentioned that "Network Consistency" could also be important to consider as well as the decentralization of the DLT design, which influences the security and trust into the DLT design and later on also the supply chain application.

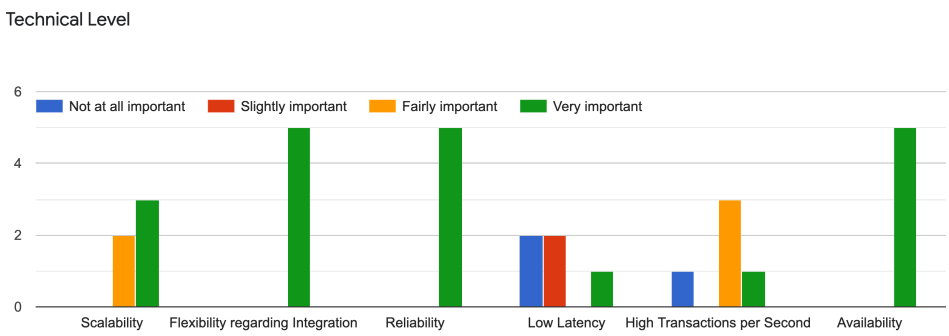



Figure 4.6: Responses: Technical Level

**The Data Level:** The responses to the parameters on the data level are depicted in figure 4.7.

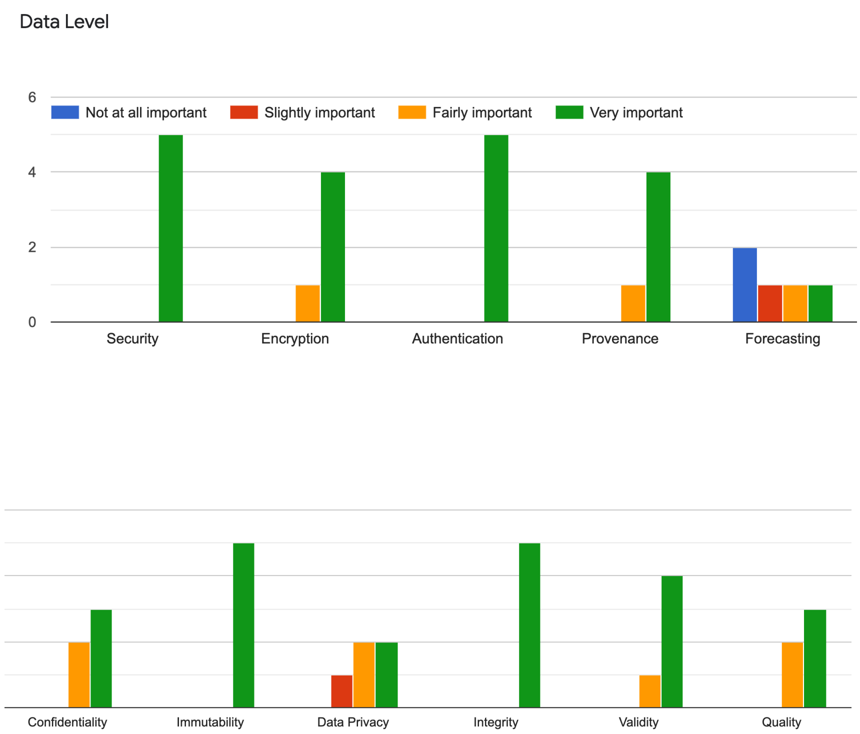



Figure 4.7: Responses: Data Level

On the data level, some parameters are tightly interconnected with each other, which resulted in many experts suggesting combining two or more parameters into one. This was the case for "Confidentiality", "Data Privacy" and "Encryption" which should be merged together into one parameter, as well as "Security", "Integrity" and "Immutability". Moreover, a new parameter was mentioned, namely "Data Persistence", regarding the

availability of the data. It was explained by the expert with how long the data needs to be stored on the DLT.
One interviewee also mentioned that he thinks that certain parameters from this list on the data level are fulfilled by every DLT design because they are inherent characteristics of DLTs. The exact answers of every single expert can be found in the appendix (7.1) of this thesis.

#### 4.4.3.2 Learnings from the Preliminary Study and preparation of the Main Study

Before the main study was conducted, the learnings from the preliminary study were applied. The parameters mentioned as an answer to the first question were all included in the main study except for "Collaboration" and "Customers" because those should be already clarified beforehand in one of the earlier decision phases (see section 4.2.1).

**The User Level:** Because of the similarities in their definition, the parameters "Authentication and Authorization", "Access Control" and "Flexibility regarding Users" were combined into one. The two parameters "User Interface" and "Identity Privacy" were discarded due to the outcome of the preliminary study. Therefore, the following parameter, as it can be seen in table 4.4 is used on the user level in the main study and the model:

| **Name** | **Description** |
|---|---|
| Flexibility regarding Users | Actors should have different access rights, based on their role in the supply chain and based on their business needs. This also implies the possibility to authenticate and authorize certain users for certain actions. |

Table 4.4: Selected Parameters: User Level

**The Technical Level:** On the technical level, "Interoperability" was mentioned as a parameter that could be added. As an action to that answer the description of the parameter "Flexibility regarding Integration" was slightly adapted to also include the factor of interoperability. The requirement of "Incentives to use the network" was discarded as the aim of the model is to support the selection of an appropriate DLT design and the incentives for partners to use this solution should already be cleared out at this stage of the decision. Furthermore, "Scalability", "Low Latency" and "High Transactions per Second" are moved into a new category called "Use Case specific Parameters". The description of "Reliability" was adapted to also include the term "Network Consistency", and the description of "Availability" was adapted to also include the mention of "Decentralization of the DLT design". An overview of the final parameters is given in table 4.5.

| Name | Description |
|---|---|
| Flexibility regarding Integration | Being able to integrate applications, that are already in use and other technologies which are needed for a supply chain application like for example sensors and auto-id technologies. Providing interoperability with other supply chain applications and/or other DLT implementation if needed. |
| Reliability | The ability of a system to produce correct results over a certain amount of time. Especially in distributed ledger technologies also the consistency of data among nodes is important to consider in order to achieve reliability. |
| Availability | The more time a system is actually operational compared to the planned operation time, the larger is the availability. The more nodes there are in a distributed network the more decentralized it is and the higher is the probability that the network is available. |

Table 4.5: Selected Parameters: Technical Level

**The Data Level:** Indeed, as nearly all experts mentioned certain interconnections between the parameters "Confidentiality", "Data Privacy" and "Encryption" all of those were combined together under the name of "Privacy". The same applied to the parameters "Security", "Integrity" and "Immutability", which were combined under the umbrella term "Security". "Data Persistence" as being mentioned only once in the interviews and not in the literature will not be further included. Moreover, the parameters "Authentication", "Integrity" and "Quality" were rated as very or fairly important for the most part, which results in them being included also in the main study. An overview of the final parameters is given in table 4.6.

Regarding the comment, that it may be the case that certain parameters on the data level could be fulfilled by all DLT designs, the action item is to keep this in mind for the evaluation of the main study and check for potential parameters that are fulfilled by every DLT design. Moreover, based on the feedback from the preliminary study, two more categories were created: "Economic Level" and "Use Case specific Parameters".

**The Economic Level:** Two important parameters to consider came up in the preliminary study, which didn't really fit in any of the other levels. Therefore, the economic level was created to be also considered in the main study. "Setup Costs" and "Ongoing Costs" are two parameters on this level that will be included. An overview of the final parameters is given in table 4.7.

**The Use Case specific Level:** For some parameters surprisingly often the comment was received, that these parameters are really dependent on the supply chain use case at

| Name | Description |
|---|---|
| Privacy | The protection of data against unintentional use. Governing how data can be collected, shared and used. Data encryption could be one method of achieving certain characteristics. |
| Security | Data should be protected from unauthorized access and corruption and it should not be able to be changed or tampered with. Furthermore it should stay accurate and consistent over it lifecylce. |
| Authentication | Data authentication is the confirmation of the origin and the integrity of the data. This information should be protected and the duplication of records should be made impossible. |
| Provenance | Chronological record of the history of a specific object, e.g. including data about the ownership or the location of the asset at a specific time. |
| Validity | Ensures that the data is correct and useful. |
| Quality | Measures the condition of data in terms of various factors, like for example accuracy and completeness among others. |

Table 4.6: Selected Parameters: Data Level

| Name | Description |
|---|---|
| Setup Costs | How complicated is it to setup the DLT implementation? Which resources are needed in terms of know-how, human resources and capital? |
| Ongoing Costs | Costs for transactions and/or running and maintaining nodes. And all other DLT design specific costs which need to be considered during running the implementation. |

Table 4.7: Selected Parameters: Economic Level

hand. Mostly, those parameters were very specific regarding the technical performance of the DLT design. Additionally, this category fits also the question whether the DLT implementation is targeted for a B2C application or a B2B application, which was mentioned as an additional parameter. An overview of the final parameters is given in table **??**.

### 4.4.4 Empirical evaluation of DLT Designs

The goal of this part was for the experts to rate how the different DLT designs perform, regarding each of the parameters that were the outcome of the preliminary study. Different to the preliminary study, the main study was conducted via a survey that was sent out via E-Mail to the experts. This survey was designed and hosted on the popular web service of LimeSurvey[169] The structure of the main study, therefore, needed to be carefully designed,

[169] **https://www.limesurvey.org**.

| Name | Description |
|---|---|
| Scalability | The ability to handle a growing amount of work within the system. |
| Low Latency | The delay between a user's action and the applications response is the latency. A low latency (short delay) is required. |
| High Transactions per Second | The amount of updates that can be performed on the application in a certain timeframe should be as high as possible. |
| B2C or B2B | Is the DLT implementation targeted for a B2C (business-to-consumer) or a B2B (business-to-business) supply chain application? |

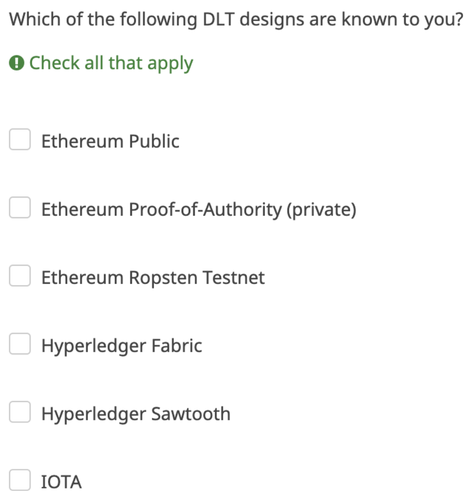
Table 4.8: Selected Parameters: Use Case specific Level

in order to lead the experts through the survey on their own. Therefore, the main study was split up in three parts.
Due to the fact, that no supply chain-specific domain knowledge was to be needed for the main study the expert group was expanded by one additional expert, as shown in table 4.9.

| Expert | Years of DLT Experience | Position | Business Sector |
|---|---|---|---|
| 6 | 1 | Web3 Frontend Developer | IT/DLT |

Table 4.9: Profile of the additional expert

The study was started by asking the experts which of the following DLT designs they are familiar with. This was done in order to prevent the experts from having to answer questions about a DLT design that they do not even know. It was implemented with the help of a multiple selection question, as shown in figure 4.8.
After the experts have answered this question the main part of the study started. The participants were presented one question for every DLT design that they have selected in the previous part. They were given 4 different options to select from: "Very Good", "Good", "Poor" and "Very Poor" as can be seen in figure 4.9. As additional guidance the list of parameters with their definitions how it is used in this thesis was provided as a pdf file to the participants.
As a conclusion of these parameter ratings, the experts were also asked about their opinion, whether they would recommend using a specific DLT design rather for a B2B or a B2C application.


Which of the following DLT designs are known to you?

Check all that apply

- Ethereum Public
- Ethereum Proof-of-Authority (private)
- Ethereum Ropsten Testnet
- Hyperledger Fabric
- Hyperledger Sawtooth
- IOTA

Figure 4.8: First part of the main study

#### 4.4.4.1 Responses to the Main Study

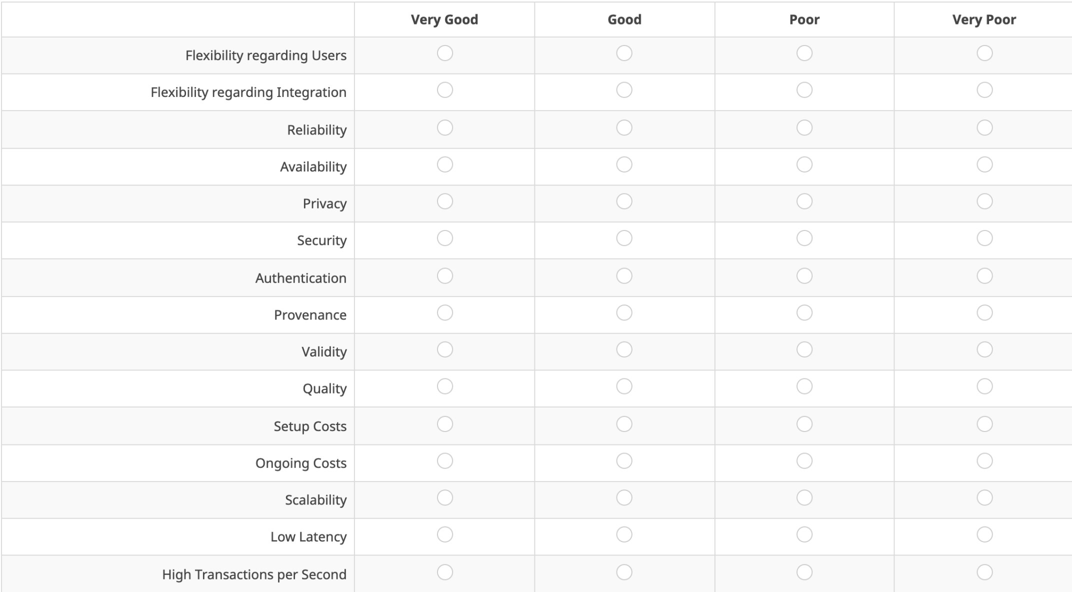
The responses to the main study will be presented in the same order as the main study was structured. In total, all six experts have provided answers to the main study, and their rating of their knowledge of the different DLT designs can be seen in table 4.10.

Table 4.10: Known DLT designs

| DLT Design | Ethereum Public | Ethereum PoA | Ethereum Ropsten Testnet | Hyperledger Fabric | Hyperledger Sawtooth | IOTA |
|---|---|---|---|---|---|---|
| Expert 1 | Yes | Yes | Yes | Yes | No | Yes |
| Expert 2 | Yes | Yes | Yes | Yes | Yes | Yes |
| Expert 3 | Yes | Yes | Yes | Yes | No | Yes |
| Expert 4 | Yes | Yes | Yes | Yes | Yes | Yes |
| Expert 5 | Yes | No | No | No | No | No |
| Expert 6 | Yes | No | Yes | No | No | Yes |

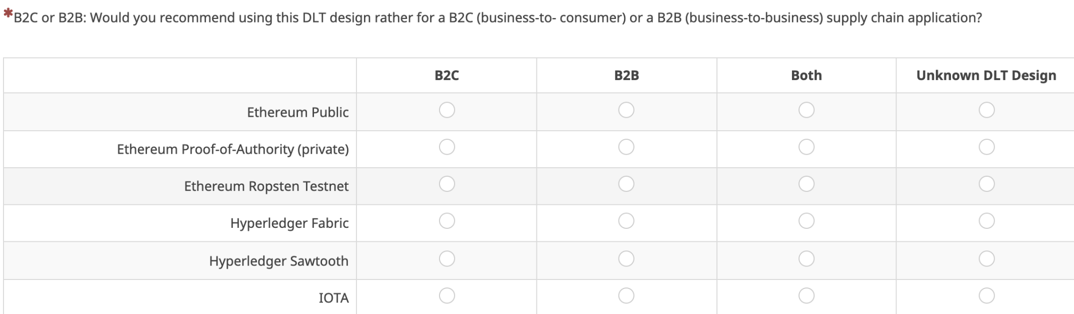
Regarding the main part of the study, the experts were asked how the different DLT designs perform regarding each parameter. In order to prevent the experts from rating also DLT designs which they are not aware of, only the DLT designs which the know of were asked to them. To be able to use the answers of the experts they were coded into numbers from one (very poor) to four (very good) and the average value of all answers was calculated. The average values for each combination of DLT design and parameter can be seen in table 4.11.

Lastly, the experts were also asked about their opinion, whether they would use a specific



| | Very Good | Good | Poor | Very Poor |
|---|---|---|---|---|
| Flexibility regarding Users | | | | |
| Flexibility regarding Integration | | | | |
| Reliability | | | | |
| Availability | | | | |
| Privacy | | | | |
| Security | | | | |
| Authentication | | | | |
| Provenance | | | | |
| Validity | | | | |
| Quality | | | | |
| Setup Costs | | | | |
| Ongoing Costs | | | | |
| Scalability | | | | |
| Low Latency | | | | |
| High Transactions per Second | | | | |

Figure 4.9: Second part of the main study



*B2C or B2B: Would you recommend using this DLT design rather for a B2C (business-to- consumer) or a B2B (business-to-business) supply chain application?

| | B2C | B2B | Both | Unknown DLT Design |
|---|---|---|---|---|
| Ethereum Public | | | | |
| Ethereum Proof-of-Authority (private) | | | | |
| Ethereum Ropsten Testnet | | | | |
| Hyperledger Fabric | | | | |
| Hyperledger Sawtooth | | | | |
| IOTA | | | | |

Figure 4.10: Third part of the main study

DLT design rather than a B2C application or a B2B application. The results of this question, can be seen in table 4.12.

## 4.5 Evaluation and Interpretation

Now, it is time that all those findings are brought together into one model. To reiterate what has been accomplished so far: The results of the systematic literature review have been analysed in terms of issues in current supply chains, expectations towards an implementation of DLT, and parameters that are important for such a specific DLT application. Further on, the different DLT designs that were utilised in the case studies in the literature review were gathered.

The parameters found in the systematic literature review were taken as a starting point

Table 4.11: The results of the survey

| | Ethereum Public | Ethereum PoA | Ethereum Ropsten Testnet | Hyperledger Fabric | Hyperledger Sawtooth | IOTA |
|---|---|---|---|---|---|---|
| Parameter | Average | Average | Average | Average | Average | Average |
| Flexibility regarding Users | 3,17 | 3,25 | 3 | 2,75 | 3,5 | 4 |
| Flexibility regarding Integration | 3,00 | 3,25 | 2,8 | 2,5 | 3 | 3,2 |
| Reliability | 3,50 | 3,5 | 2,2 | 3,25 | 3,5 | 2,8 |
| Availability | 3,67 | 3,5 | 2,6 | 3,5 | 3,5 | 3,2 |
| Privacy | 2,83 | 3,5 | 2,6 | 4 | 3,5 | 3,4 |
| Security | 3,00 | 3 | 2 | 3,25 | 3,5 | 3,2 |
| Authentication | 3,17 | 3,5 | 3 | 3,75 | 3,5 | 3,4 |
| Provenance | 3,50 | 3,5 | 3,2 | 3,75 | 3 | 3,6 |
| Validity | 3,67 | 3,5 | 2,8 | 3,75 | 3 | 3,8 |
| Quality | 3,67 | 3,75 | 3 | 3,75 | 3 | 4 |
| Setup Costs | 2,50 | 2,5 | 2,8 | 1,75 | 4 | 3 |
| Ongoing Costs | 1,17 | 2,75 | 3 | 2,25 | 3,5 | 3,2 |
| Scalability | 1,50 | 3 | 1,8 | 2,75 | 3,5 | 3,4 |
| Low Latency | 1,83 | 3,25 | 2,2 | 3,75 | 3 | 3,8 |
| High Transactions per Second | 1,67 | 3 | 2 | 3,5 | 3,5 | 3,8 |

Table 4.12: B2C or B2B

| DLT Design | Ethereum Public | Ethereum PoA | Ethereum Ropsten Testnet | Hyperledger Fabric | Hyperledger Sawtooth | IOTA |
|---|---|---|---|---|---|---|
| Expert 1 | Both | B2B | B2C | B2B | Unknown | Both |
| Expert 2 | B2C | Both | B2C | B2B | B2B | Both |
| Expert 3 | B2C | B2B | Unknown | B2B | Unknown | Both |
| Expert 4 | B2C | B2B | B2B | B2B | Both | Both |
| Expert 5 | Both | Unknown | Unknown | Unknown | Unknown | Unknown |
| Expert 6 | Both | B2B | Both | Unknown | Unknown | Both |

for an empirical study. The aim of the empirical study was on one hand to refine the parameters from the literature with input from domain experts. On the other hand, the knowledge and experience from these experts are also used to rate the performance of the DLT designs regarding the various parameters. The aim of this section is to link all this information together and develop a model, which can easily be applied in any supply

chain to select the most appropriate DLT design for the focal use case.
For the final evaluation framework, a scoring model is the basis. With the help of a scoring model, various criteria can be rated and different alternatives can be compared. In such a model, each parameter needs a weight and a rating. The rating is usually gathered through comparison of different alternatives by experts.[170] As it is in this case, the average points from the result of the empirical study are taken for each combination of DLT design and parameter.

The weight of each parameter can be also considered as the importance of this specific parameter to the user. Therefore, this is the part of the model where the user can influence the outcome depending on how important certain parameters of the application are. Usually, a scoring model is constructed in a way that the total sum of all weights is equal to 100.[171]

In order to get the score of one criteria, the weight and the rating for each alternative are multiplied with each other. The sum of the scores of all criteria for one alternative is then the total score of this alternative. Calculating all total scores of the different alternatives, those can be compared to each other, presenting the best alternative with the highest total score.[172] The model has been constructed in Microsoft Excel and is exemplarily visualized in figure 4.11. The following elements can be seen in this figure:

- On the left side, all parameters are listed, which are the different criteria in this specific scoring model.
- The weight of each parameter needs to be filled out by the user when he applies the evaluation framework. With the weight, they are able to rate the importance of specific parameters to his DLT application.
- For each alternative DLT design two columns are given:

  Rating: This is the average rating from the empirical study.

  Score: The score is calculated by multiplying the weight with the rating for each combination of parameter and DLT design. If the weight $w_i$ is given for parameter $i$ and the rating $r_{i,j}$ is given for a parameter $i$ and a DLT design $j$. The score $S_{i,j}$ is calculated in the following way: $S_{i,j} = w_i * r_{i,j}$.
- The total score is calculated by summing up all individual scores of one alternative. Total Score $TS_j$ for alternative $j$ is $\sum_{i=0}^{I} S_{i,j}$.

[170] Büssow 2004, p. 58.
[171] Büssow 2004, p. 58.
[172] Büssow 2004, p. 58.

- Moreover, the preference of the experts is shown for each alternative, regarding whether they would use this DLT design for a B2C or a B2B application.

| | Weight | Ethereum Public | | Ethereum PoA | | Ethereum Ropsten Testnet | | Hyperledger Fabric | | Hyperledger Sawtooth | | IOTA | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Parameter** | | **Rating** | **Score** | **Rating** | **Score** | **Rating** | **Score** | **Rating** | **Score** | **Rating** | **Score** | **Rating** | **Score** |
| **Flexibility regarding Users** | | 3,17 | 0 | 3,25 | 0 | 3 | 0 | 2,75 | 0 | 3,5 | 0 | 4 | 0 |
| **Flexibility regarding Integration** | | 3,00 | 0 | 3,25 | 0 | 2,8 | 0 | 2,5 | 0 | 3 | 0 | 3,2 | 0 |
| **Reliability** | | 3,50 | 0 | 3,5 | 0 | 2,2 | 0 | 3,25 | 0 | 3,5 | 0 | 2,8 | 0 |
| **Availability** | | 3,67 | 0 | 3,5 | 0 | 2,6 | 0 | 3,5 | 0 | 3,5 | 0 | 3,2 | 0 |
| **Privacy** | | 2,83 | 0 | 3,5 | 0 | 2,6 | 0 | 4 | 0 | 3,5 | 0 | 3,4 | 0 |
| **Security** | | 3,00 | 0 | 3 | 0 | 2 | 0 | 3,25 | 0 | 3,5 | 0 | 3,2 | 0 |
| **Authentication** | | 3,17 | 0 | 3,5 | 0 | 3 | 0 | 3,75 | 0 | 3,5 | 0 | 3,4 | 0 |
| **Provenance** | | 3,50 | 0 | 3,5 | 0 | 3,2 | 0 | 3,75 | 0 | 3 | 0 | 3,6 | 0 |
| **Validity** | | 3,67 | 0 | 3,5 | 0 | 2,8 | 0 | 3,75 | 0 | 3 | 0 | 3,8 | 0 |
| **Quality** | | 3,67 | 0 | 3,75 | 0 | 3 | 0 | 3,75 | 0 | 3 | 0 | 4 | 0 |
| **Setup Costs** | | 2,50 | 0 | 2,5 | 0 | 2,8 | 0 | 1,75 | 0 | 4 | 0 | 3 | 0 |
| **Ongoing Costs** | | 1,17 | 0 | 2,75 | 0 | 3 | 0 | 2,25 | 0 | 3,5 | 0 | 3,2 | 0 |
| **Scalability** | | 1,50 | 0 | 3 | 0 | 1,8 | 0 | 2,75 | 0 | 3,5 | 0 | 3,4 | 0 |
| **Low Latency** | | 1,83 | 0 | 3,25 | 0 | 2,2 | 0 | 3,75 | 0 | 3 | 0 | 3,8 | 0 |
| **High Transactions per Second** | | 1,67 | 0 | 3 | 0 | 2 | 0 | 3,5 | 0 | 3,5 | 0 | 3,8 | 0 |
| **Total Score:** | 0% | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 |
| | | | | | | | | | | | | | |
| **B2C or B2B** | | B2C or Both | | B2B | | B2C | | B2B | | B2C or Both | | Both | |

... Needs to be filled out by the user

... Best Alternative

Figure 4.11: The Model

# 5 Exemplary usage of the model in MUL 4.0

Now that the model has been developed, it is ready to be applied in practice. Currently, a research project MUL 4.0 is conducted at Montanuniversität Leoben and it is planned to include a DLT application into the supply chain use case in the scope of this project. In this chapter, the potential use case within the scope of the research project is described and afterward the process of applying the model in order to find an appropriate DLT design is covered.

## 5.1 The potential Use Case

The metal processing industry is a supplier for nearly every other manufacturing industry, not at least for the automotive and aircraft construction companies. Due to the critical function of the manufactured products in those industries, several laws exist which oblige the manufacturing company to keep track of their supply chain in a detailed manner. With the discussions about an EU-wide supply chain law in mind, OEMs are thinking about how to monitor the production of purchased parts from their suppliers, especially their lower-tier suppliers, in the future. One approach to this is the roll-out of a decentralised, unforgeable data storage, in which the lower-tier suppliers directly feed in product-related data from their production facilities – which is an application based on a distributed ledger.

To ensure a broad acceptance and applicability of this solution, especially in the typically not very digitalized SMEs at the upstream end of the supply chain, easy integration of the solution in existing software has to be guaranteed. In order to guarantee members that their data can only be injected and modified by themselves, there must be a strict authentication mechanism. The background application shall enable plausibility checks of the inserted data to prevent incorrect entries. Due to the financial position of the OEMs, the setups costs, on the one side, do not play a big role, but on the other side, the ongoing costs have to be as low as possible to prevent competitiveness from being impaired. This is due to the high number of participants in the system, which arises another requirement: scalability and the possibility to insert a lot of data in a short amount of time. On the opposite, the system does not need to have the ability to react in real-time, because it should connect to the participants' ERP systems and not their machinery, and is used primarily for reporting and analysis, not for production control or other things that raise the need for near-real-time data transmission. A depiction of the stakeholders and their goals can be seen in figure 5.1.

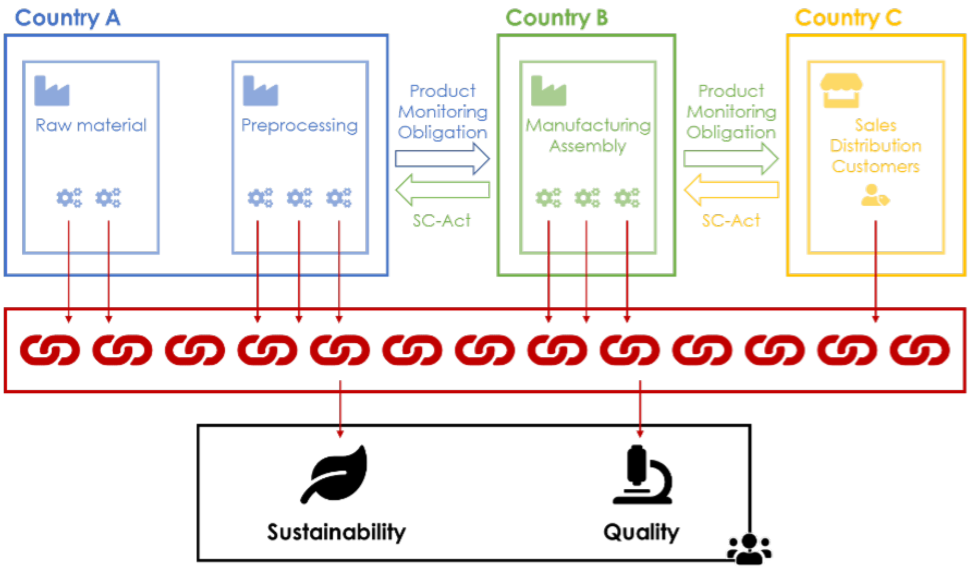



Figure 5.1: Depiction of the use case

## 5.2 Application of the Model to select a DLT Design

The model (as it is depicted in figure 4.11) was given to a researcher working on the project accompanied by one sheet summarising all the parameters and their descriptions as they are written in section 4.4.3.2. The weighting of the different parameters was filled out and the total score was calculated automatically for each DLT design. The result can be seen in figure 5.2.
Based on the total score as a result of the model, **IOTA** would be the preferable DLT design to be implemented for this use case.

## 5.3 User Feedback on Model Application

This first application of the model was also used for a round of feedback regarding its usability and applicability in practice. The main point of feedback was, that it was quite difficult to distribute exactly 100% to the parameters. Because of their high number and the "competition between the parameters" that arises from this.

| | Weight | Ethereum Public | | Ethereum PoA | | Ethereum Ropsten Testnet | | Hyperledger Fabric | | Hyperledger Sawtooth | | IOTA | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Parameter** | | Rating | Score | Rating | Score | Rating | Score | Rating | Score | Rating | Score | Rating | Score |
| **Flexibility regarding Users** | 5,0% | 3,17 | 0,158333 | 3,25 | 0,1625 | 3 | 0,15 | 2,75 | 0,1375 | 3,5 | 0,175 | 4 | 0,2 |
| **Flexibility regarding Integration** | 10,0% | 3,00 | 0,3 | 3,25 | 0,325 | 2,8 | 0,28 | 2,5 | 0,25 | 3 | 0,3 | 3,2 | 0,32 |
| **Reliability** | 5,0% | 3,50 | 0,175 | 3,5 | 0,175 | 2,2 | 0,11 | 3,25 | 0,1625 | 3,5 | 0,175 | 2,8 | 0,14 |
| **Availability** | 5,0% | 3,67 | 0,183333 | 3,5 | 0,175 | 2,6 | 0,13 | 3,5 | 0,175 | 3,5 | 0,175 | 3,2 | 0,16 |
| **Privacy** | 10,0% | 2,83 | 0,283333 | 3,5 | 0,35 | 2,6 | 0,26 | 4 | 0,4 | 3,5 | 0,35 | 3,4 | 0,34 |
| **Security** | 10,0% | 3,00 | 0,3 | 3 | 0,3 | 2 | 0,2 | 3,25 | 0,325 | 3,5 | 0,35 | 3,2 | 0,32 |
| **Authentication** | 10,0% | 3,17 | 0,316667 | 3,5 | 0,35 | 3 | 0,3 | 3,75 | 0,375 | 3,5 | 0,35 | 3,4 | 0,34 |
| **Provenance** | 10,0% | 3,50 | 0,35 | 3,5 | 0,35 | 3,2 | 0,32 | 3,75 | 0,375 | 3 | 0,3 | 3,6 | 0,36 |
| **Validity** | 2,5% | 3,67 | 0,091667 | 3,5 | 0,0875 | 2,8 | 0,07 | 3,75 | 0,09375 | 3 | 0,075 | 3,8 | 0,095 |
| **Quality** | 2,5% | 3,67 | 0,091667 | 3,75 | 0,09375 | 3 | 0,075 | 3,75 | 0,09375 | 3 | 0,075 | 4 | 0,1 |
| **Setup Costs** | 0,0% | 2,50 | 0 | 2,5 | 0 | 2,8 | 0 | 1,75 | 0 | 4 | 0 | 3 | 0 |
| **Ongoing Costs** | 10,0% | 1,17 | 0,116667 | 2,75 | 0,275 | 3 | 0,3 | 2,25 | 0,225 | 3,5 | 0,35 | 3,2 | 0,32 |
| **Scalability** | 10,0% | 1,50 | 0,15 | 3 | 0,3 | 1,8 | 0,18 | 2,75 | 0,275 | 3,5 | 0,35 | 3,4 | 0,34 |
| **Low Latency** | 0,0% | 1,83 | 0 | 3,25 | 0 | 2,2 | 0 | 3,75 | 0 | 3 | 0 | 3,8 | 0 |
| **High Transactions per Second** | 10,0% | 1,67 | 0,166667 | 3 | 0,3 | 2 | 0,2 | 3,5 | 0,35 | 3,5 | 0,35 | 3,8 | 0,38 |
| **Total Score:** | 100% | | 2,683333 | | 3,24375 | | 2,575 | | 3,2375 | | 3,375 | | 3,415 |
| | | | | | | | | | | | | | |
| **B2C or B2B** | | B2C or Both | | B2B | | B2C | | B2B | | B2C or Both | | Both | |
| | | | | | | | | | | | | | |
| | | ... Needs to be filled out by the user | | | | | | | | | | | |
| | | ... Best Alternative | | | | | | | | | | | |

Figure 5.2: The result of the model

Currently, the user is basically getting asked two questions with the model: "How important is this parameter to me?" and at the same time "How important is it in relation to the other parameters?", which is (maybe too) challenging. If there is one parameter that is considered very important, the user will probably have to give this one only a weighting of 15% anyway – because all the other parameters need also consideration.

Comment from the user on the process:

> *"I did the weight assignment as follows: I went through the list of parameters and their descriptions and highlighted the ones that were most important to me. At the end, 8 out of 15 were highlighted. Then I assigned a 10% weight to those 8 and tried to split the remaining "amount of weight" to the other ones. In my opinion, this is a quite primitive (and potentially misleading) approach."*

Moreover, feedback regarding the parameters themselves was given. The parameters "Validity" and "Quality" are hard to distinguish for the user. For the user, these two were somehow complementary: When data is of high quality (high accuracy and completeness), it already implies Validity (correctness and usefulness) of the data. Based on this feedback these two parameters were combined into one parameter "Quality".

| **Name** | **Description** |
|---|---|
| Quality | Measures the condition of data in terms of various factors, like for example accuracy and completeness among others. (This implies that the data is also correct and useful) |

Table 5.1: Adapted Parameter

# 6 Conclusion

The aim of this thesis was to develop a quantitative evaluation model for DLT designs regarding several parameters which are important to consider for a DLT application in a supply chain context. In order to develop this model, in the first chapter, the topic of this thesis was introduced, goals were set and a research question was formulated. Afterward, the theory behind supply chain terminology and transparency in supply chains was covered. The second chapter was closed with having a look at all the current challenges present in supply chain management. The third chapter was fully dedicated to distributed ledger technology. The most important terms and definitions were covered as well as the concepts and operating principles of the most well-known DLT concepts. The fourth chapter is presenting the main part of this thesis and in this chapter, the evaluation model itself is developed by utilising a systematic literature review, qualitative expert interviews, and quantitative expert surveys. The model is then applied to a case study in the fifth chapter. This chapter is aimed at concluding this thesis by summarising and discussing the findings.

## 6.1 Summary and discussion of results

Within the course of this thesis the research questions which were formulated at the start of this thesis could be answered. The first question was, *which specifications and requirements are important to consider when it comes to transparency and traceability applications in supply chains?* In chapter four, a systematic literature review was conducted which resulted in a list of parameters that were considered throughout all the articles. This list was then the basis for qualitative expert interviews and based on their input a finalised list of specifications and requirements was put together.

Afterward also the second question could be worked on, which was, *how well do different DLT designs perform regarding the specifications and requirements of different supply chains?* By designing and conducting a quantitative survey for domain experts, the most used DLT designs in the supply chain domain got rated regarding their performance in the various specifications and requirements found from the first research question. Based on this rating the final evaluation model was developed.

Several findings were made within this thesis with the most outstanding one probably being DLTs in general not really recognised beyond blockchain technology in the supply chain sector. Meaning, that the terms and definitions and classification like it is picked up in this thesis is still a relatively new perspective. This is supported by the results of the systematic literture review. All but one case study implemented a blockchain, for the use case without even considering any other DLT concept or design. Only in one article the IOTA DLT which builds on a DAG is used.[173]

Furthermore, the need for a thesis like this has presented itself during the systematic literature review, with most of the articles surveyed having not put any effort at all into selecting an appropriate DLT design for their application. But certainly one of the key challenges of developing a DLT application is to select the right DLT concept and design and configure it correctly to exactly meet the demands of the specific use case.
DLTs properly deployed can provide a possible solution to balance the privacy for each company and the sharing of information in a supply chain in order to provide transparency and traceability to the end consumer as well as to any other parties in the supply chain.

## 6.2 Recommended action items

**For Research:** Based on these findings it is recommended to still put more research focus on DLTs in general, going beyond blockchain technology. As there are many case studies and proof-of-concepts already present, generally the applicability of such technologies for the supply chain sector is definitely proven. Now, the next steps need to be taken, where one potential focus could definitely be the further dissemination of characteristics and their possible configurations of various DLT concepts and designs and their consequences for supply chain applications. The model presented in this thesis can be seen as one building block towards this focus.

Further research can work upon this model and specialise on one hand on the economic effects of applying DLTs to supply chain use cases. On the other hand there is also the computer science perspective to this topic, where further research can be done with detailing the specifications and requirements and implementing applications.

**For practice:** For practical applications of DLT in the supply chain sector it is recommended to thoroughly study the topic of DLT, understand it's strengths and weaknesses and to define the goals for this application. Further on the model, which was developed in the course of this thesis should be used to support decisions regarding the right DLT design to choose. What's most important although is to not stop experimenting with such new technologies and to be open for change in many aspects.

[173] Suhail et al. 2020.

**For improving the model:** For the model itself, there is also room for improvement. The DLT sector is in a fast evolving state and the model can always be adapted with adding more DLT designs. On another dimension, also the parameters can be adapted based on feedback from usage of the model. As the expert group for the quantitative survey rating the performance of the various DLT designs was rather small, the scoring model could also be enhanced by conducting a large scale study and refine the rating.

By applying the model to more case studies, it can also be improved regarding user experience. As it can be seen in section 5.3, already the first user brought up some potential improvements. Especially, distributing exactly 100% across that many parameters is a challenge. In the future, a mechanism should be found to allow the user of the model to assign weights more easily. One idea would be to use a Likert-scale or a range from 1-100 for each parameter individually and then calculating the relative score of the parameters within this voting.

# Bibliography

## Books and Articles

Agrawal, Tarun Kumar et al. (04/2021). "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry". en. In: *Computers & Industrial Engineering* 154, p. 107130. ISSN: 03608352. DOI: 10.1016/j.cie.2021.107130.
https://linkinghub.elsevier.com/retrieve/pii/S0360835221000346
(visited on 04/16/2021)

Angelis, Stefano De et al. (n.d.). "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain". en. In: (), p. 11

Arnold, Dieter (2008). *Handbuch Logistik*. de. 3., neu bearb. Aufl. VDI-[Buch]. OCLC: 244039737. Berlin: Springer. ISBN: 978-3-540-72928-0 978-3-540-72929-7

Asante, Mary et al. (2021). "Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey". en. In: *IEEE Transactions on Engineering Management*, pp. 1–27. ISSN: 0018-9391, 1558-0040. DOI: 10.1109/TEM.2021.3053655.
https://ieeexplore.ieee.org/document/9366288/
(visited on 04/28/2021)

Aung, Myo Min and Yoon Seok Chang (05/2014). "Traceability in a food supply chain: Safety and quality perspectives". en. In: *Food Control* 39, pp. 172–184. ISSN: 09567135. DOI: 10.1016/j.foodcont.2013.11.007.
https://linkinghub.elsevier.com/retrieve/pii/S0956713513005811
(visited on 01/03/2022)

Bano, Shehar et al. (11/2017). "Consensus in the Age of Blockchains". In: *arXiv:1711.03936 [cs]*. arXiv: 1711.03936.
http://arxiv.org/abs/1711.03936
(visited on 01/30/2019)

Bashir, Imran (2018). *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained*. eng. Second edition, fully revised and updated. Expert insight. Birmingham Mumbai: Packt. ISBN: 978-1-78883-904-4

Büssow, Christian (2004). *Prozessbewertung in der Logistik*. de. Wiesbaden: Deutscher Universitätsverlag. ISBN: 978-3-8244-8026-5 978-3-322-81685-6. DOI: 10.1007/978-3-322-81685-6.
http://link.springer.com/10.1007/978-3-322-81685-6
(visited on 12/28/2021)

Butt, Atif Saleem (09/2021). "Supply chains and COVID-19: impacts, countermeasures and post-COVID-19 era". en. In: *The International Journal of Logistics Management* ahead-of-print.ahead-of-print. ISSN: 0957-4093. DOI: 10.1108/IJLM-02-2021-0114.
https://www.emerald.com/insight/content/doi/10.1108/IJLM-02-2021-0114/full/html
(visited on 01/13/2022)

Camps, Th et al., eds. (2004). *The Emerging World of Chains and Networks, Bridging Theory and Practice*. English. Reed Business Information. ISBN: 978-90-5901-928-7

Caro, Miguel Pincheira et al. (05/2018). "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation". en. In: *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany)*. Tuscany: IEEE, pp. 1–4. ISBN: 978-1-5386-6930-3. DOI: 10.1109/IOT-TUSCANY.2018.8373021.
https://ieeexplore.ieee.org/document/8373021/
(visited on 05/22/2021)

Chowdhury, Mohammad Jabed Morshed et al. (2019). "A Comparative Analysis of Distributed Ledger Technology Platforms". en. In: *IEEE Access* 7, pp. 167930–167943. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2953729.
https://ieeexplore.ieee.org/document/8902067/
(visited on 06/02/2021)

Counsell, Carl (09/1997). "Formulating Questions and Locating Primary Studies for Inclusion in Systematic Reviews". en. In: *Annals of Internal Medicine* 127.5, p. 380. ISSN: 0003-4819. DOI: 10.7326/0003-4819-127-5-199709010-00008.
http://annals.org/article.aspx?doi=10.7326/0003-4819-127-5-199709010-00008
(visited on 04/12/2021)

Denyer, David and David Tranfield (2009). “Producing a systematic review.” In: *The Sage handbook of organizational research methods*. Thousand Oaks, CA: Sage Publications Ltd, pp. 671–689. ISBN: 978-1-4129-3118-2 (Hardcover)

Döring, Nicola and Jürgen Bortz (2016). *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*. de. Springer-Lehrbuch. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-642-41088-8 978-3-642-41089-5. DOI: 10.1007/978-3-642-41089-5.
http://link.springer.com/10.1007/978-3-642-41089-5
(visited on 12/03/2021)

Dwork, Cynthia and Moni Naor (1993). “Pricing via Processing or Combatting Junk Mail”. en. In: *Advances in Cryptology — CRYPTO’ 92*. Ed. by Ernest F. Brickell. Vol. 740. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 139–147. ISBN: 978-3-540-57340-1. DOI: 10.1007/3-540-48071-4_10.
http://link.springer.com/10.1007/3-540-48071-4_10
(visited on 09/24/2021)

Egels-Zandén, Niklas, Kajsa Hulthén, and Gabriella Wulff (11/2015). “Trade-offs in supply chain transparency: the case of Nudie Jeans Co”. en. In: *Journal of Cleaner Production* 107, pp. 95–104. ISSN: 09596526. DOI: 10.1016/j.jclepro.2014.04.074.
https://linkinghub.elsevier.com/retrieve/pii/S0959652614004375
(visited on 01/03/2022)

Engelenburg, Sélinde van, Marijn Janssen, and Bram Klievink (2018). “A Blockchain Architecture for Reducing the Bullwhip Effect”. en. In: *Business Modeling and Software Design*. Ed. by Boris Shishkov. Vol. 319. Series Title: Lecture Notes in Business Information Processing. Cham: Springer International Publishing, pp. 69–82. ISBN: 978-3-319-94213-1 978-3-319-94214-8. DOI: 10.1007/978-3-319-94214-8_5.
http://link.springer.com/10.1007/978-3-319-94214-8_5
(visited on 05/22/2021)

Engelhardt-Nowitzki, Corinna and Elisabeth Lackner, eds. (2006). *Chargenverfolgung: Möglichkeiten, Grenzen, Anwendungsgebiete*. de. 1. Aufl. Leobener Logistik Cases. Wiesbaden: Dt. Univ.-Verl. ISBN: 978-3-8350-0639-3

Feng Tian (06/2017). “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things”. en. In: *2017 International Conference on*

*Service Systems and Service Management*. Dalian, China: IEEE, pp. 1–6. ISBN: 978-1-5090-6370-3. DOI: 10.1109/ICSSSM.2017.7996119.
http://ieeexplore.ieee.org/document/7996119/
(visited on 07/16/2021)

Figorilli, Simone et al. (09/2018). "A Blockchain Implementation Prototype for the Electronic Open Source Traceability of Wood along the Whole Supply Chain". en. In: *Sensors* 18.9. Number: 9, p. 3133. ISSN: 1424-8220. DOI: 10.3390/s18093133.
http://www.mdpi.com/1424-8220/18/9/3133
(visited on 05/22/2021)

Franco, Pedro (2015). *Understanding bitcoin: cryptography, engineering, and economics*. eng. Wiley finance series. Chichester: Wiley. ISBN: 978-1-119-01914-5 978-1-119-01916-9

Ghode, Dnyaneshwar J. et al. (2020). "Architecture to Enhance Transparency in Supply Chain Management using Blockchain Technology". en. In: *Procedia Manufacturing* 51, pp. 1614–1620. ISSN: 23519789. DOI: 10.1016/j.promfg.2020.10.225.
https://linkinghub.elsevier.com/retrieve/pii/S2351978920320965
(visited on 05/22/2021)

Gläser, Jochen and Grit Laudel (2010). *Experteninterviews und qualitative Inhaltsanalyse*. de. Wiesbaden: VS Verlag für Sozialwissenschaften. ISBN: 978-3-531-17238-5 978-3-531-91538-8. DOI: 10.1007/978-3-531-91538-8.
http://link.springer.com/10.1007/978-3-531-91538-8
(visited on 12/03/2021)

Göpfert, Ingrid and Wanja Wellbrock (2012). "Die Entwicklung innovativer Supply-Chain-Management-Konzepte — Bedarf und Prozessmodell". de. In: *Supply Management Research*. Ed. by Ronald Bogaschewsky et al. Wiesbaden: Gabler Verlag, pp. 105–132. ISBN: 978-3-8349-3927-2 978-3-8349-3928-9. DOI: 10.1007/978-3-8349-3928-9_5.
http://www.springerlink.com/index/10.1007/978-3-8349-3928-9_5
(visited on 09/24/2019)

Kannengießer, Niclas et al. (2019). "What Does Not Fit Can be Made to Fit! Trade-Offs in Distributed Ledger Technology Designs". en. In: DOI: 10.24251/HICSS.2019.848.
http://hdl.handle.net/10125/60143

Kim, Mark et al. (11/2018). "Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution". en. In: *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*. Vancouver, BC: IEEE, pp. 335–340. ISBN: 978-1-5386-7266-2. DOI: 10.1109/IEMCON.2018.8615007.
https://ieeexplore.ieee.org/document/8615007/
(visited on 05/22/2021)

King, Sunny and Scott Nadal (2012). "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake". en. In: p. 6

Ko, Kyungchan et al. (09/2020). "Towards Blockchain-based Stainless Steel Tracking". en. In: *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*. Daegu, Korea (South): IEEE, pp. 318–321. ISBN: 978-89-950043-8-8. DOI: 10.23919/APNOMS50412.2020.9237041.
https://ieeexplore.ieee.org/document/9237041/
(visited on 05/22/2021)

Kolb, Julian, David Julian Hornung, and Axel Winkelmann (2018). "INDUSTRIAL APPLICATION OF BLOCKCHAIN TECHNOLOGY – ERASING THE WEAKNESSES OF VEN- DOR MANAGED INVENTORY". en. In: p. 17

Kotilevets, I.D. et al. (2018). "Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions". en. In: *IFAC-PapersOnLine* 51.30, pp. 693–696. ISSN: 24058963. DOI: 10.1016/j.ifacol.2018.11.213.
https://linkinghub.elsevier.com/retrieve/pii/S2405896318328799
(visited on 11/19/2021)

Kumar, Ajay et al. (11/2020). "Securing logistics system and supply chain using Blockchain". en. In: *Applied Stochastic Models in Business and Industry*, asmb.2592. ISSN: 1524-1904, 1526-4025. DOI: 10.1002/asmb.2592.
https://onlinelibrary.wiley.com/doi/10.1002/asmb.2592
(visited on 05/22/2021)

Liao, Da-Yin and Xuehong Wang (11/2018). "Applications of Blockchain Technology to Logistics Management in Integrated Casinos and Entertainment". en. In: *Informatics* 5.4. Number: 4, p. 44. ISSN: 2227-9709. DOI: 10.3390/informatics5040044.
http://www.mdpi.com/2227-9709/5/4/44
(visited on 05/22/2021)

Maden, Ayça and Emre Alptekin (11/2020). “Evaluation of factors affecting the decision to adopt blockchain technology: A logistics company case study using Fuzzy DEMATEL”. en. In: *Journal of Intelligent & Fuzzy Systems* 39.5. Ed. by Cengiz Kahraman, pp. 6279–6291. ISSN: 10641246, 18758967. DOI: 10.3233/JIFS-189096.
https://www.medra.org/servlet/aliasResolver?alias=iospress&doi=10.3233/JIFS-189096
(visited on 05/22/2021)

Mann, Suruchi et al. (2018). “Blockchain Technology for Supply Chain Traceability, Transparency and Data Provenance”. en. In: *Proceedings of the 2018 International Conference on Blockchain Technology and Application - ICBTA 2018*. Xi’an, China: ACM Press, pp. 22–26. ISBN: 978-1-4503-6646-5. DOI: 10.1145/3301403.3301408.
http://dl.acm.org/citation.cfm?doid=3301403.3301408
(visited on 05/22/2021)

Maroun, Elias Abou and Jay Daniel (2019). “Opportunities for Use of Blockchain Technology in Supply Chains: Australian Manufacturer Case Study”. en. In: p. 12

Mol, Arthur P.J. (11/2015). “Transparency and value chain sustainability”. en. In: *Journal of Cleaner Production* 107, pp. 154–161. ISSN: 09596526. DOI: 10.1016/j.jclepro.2013.11.012.
https://linkinghub.elsevier.com/retrieve/pii/S0959652613007762
(visited on 12/17/2021)

Nakamoto, Satoshi (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. en. In: p. 9

Patterson, Kirk A., Curtis M. Grimm, and Thomas M. Corsi (03/2003). “Adopting new technologies for supply chain management”. en. In: *Transportation Research Part E: Logistics and Transportation Review* 39.2, pp. 95–121. ISSN: 13665545. DOI: 10.1016/S1366-5545(02)00041-8.
https://linkinghub.elsevier.com/retrieve/pii/S1366554502000418
(visited on 01/12/2022)

Perboli, Guido, Stefano Musso, and Mariangela Rosano (2018). “Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases”. en. In: *IEEE Access* 6, pp. 62018–62028. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2018.2875782.
https://ieeexplore.ieee.org/document/8493157/
(visited on 05/22/2021)

Reimers, Tim, Felix Leber, and Ulrike Lechner (04/2019). "Integration of Blockchain and Internet of Things in a Car Supply Chain". en. In: *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*. Newark, CA, USA: IEEE, pp. 146–151. ISBN: 978-1-72811-264-0. DOI: 10.1109/DAPPCON.2019.00028. https://ieeexplore.ieee.org/document/8783146/ (visited on 05/22/2021)

Schinle, Markus et al. (08/2020). "How to Disclose Selective Information from Permissioned DLT-Based Traceability Systems?" en. In: *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*. Oxford, United Kingdom: IEEE, pp. 153–158. ISBN: 978-1-72816-978-1. DOI: 10.1109/DAPPS49028.2020.00020. https://ieeexplore.ieee.org/document/9126006/ (visited on 05/03/2021)

Sedlmeir, Johannes et al. (12/2020). "The Energy Consumption of Blockchain Technology: Beyond Myth". en. In: *Business & Information Systems Engineering* 62.6, pp. 599–608. ISSN: 2363-7005, 1867-0202. DOI: 10.1007/s12599-020-00656-x. https://link.springer.com/10.1007/s12599-020-00656-x (visited on 01/29/2022)

Shahzad, Aamir and Kaiwen Zhang (2021). "An Integrated IoT-Blockchain Implementation for End-to-End Supply Chain". en. In: *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 2*. Ed. by Kohei Arai, Supriya Kapoor, and Rahul Bhatia. Vol. 1289. Series Title: Advances in Intelligent Systems and Computing. Cham: Springer International Publishing, pp. 987–997. ISBN: 978-3-030-63088-1 978-3-030-63089-8. DOI: 10.1007/978-3-030-63089-8_65. http://link.springer.com/10.1007/978-3-030-63089-8_65 (visited on 05/22/2021)

Shi, Jianfeng, Dian Yi, and Jian Kuang (2019). "Pharmaceutical Supply Chain Management System with Integration of IoT and Blockchain Technology". en. In: *Smart Blockchain*. Ed. by Meikang Qiu. Vol. 11911. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 97–108. ISBN: 978-3-030-34082-7 978-3-030-34083-4. DOI: 10.1007/978-3-030-34083-4_10. http://link.springer.com/10.1007/978-3-030-34083-4_10 (visited on 05/22/2021)

Suhail, Sabah et al. (12/2020). "Orchestrating product provenance story: When IOTA ecosystem meets electronics supply chain space". en. In: *Computers in Industry* 123,

p. 103334. ISSN: 01663615. DOI: 10.1016/j.compind.2020.103334.
https://linkinghub.elsevier.com/retrieve/pii/S0166361520305686
(visited on 05/22/2021)

Sunny, Justin, Naveen Undralla, and V. Madhusudanan Pillai (12/2020). "Supply chain transparency through blockchain-based traceability: An overview with demonstration". en. In: *Computers & Industrial Engineering* 150, p. 106895. ISSN: 03608352. DOI: 10.1016/j.cie.2020.106895.
https://linkinghub.elsevier.com/retrieve/pii/S0360835220305829
(visited on 05/22/2021)

Sunyaev, Ali (2020). "Distributed Ledger Technology". en. In: *Internet Computing*. Cham: Springer International Publishing, pp. 265–299. ISBN: 978-3-030-34956-1 978-3-030-34957-8. DOI: 10.1007/978-3-030-34957-8_9.
http://link.springer.com/10.1007/978-3-030-34957-8_9
(visited on 07/23/2021)

Szabo, Nick (09/1997). "Formalizing and Securing Relationships on Public Networks". In: *First Monday* 2.9. ISSN: 13960466. DOI: 10.5210/fm.v2i9.548.
http://journals.uic.edu/ojs/index.php/fm/article/view/548
(visited on 11/20/2021)

Terzi, Sofia et al. (11/2019). "Transforming the supply-chain management and industry logistics with blockchain smart contracts". en. In: *Proceedings of the 23rd Pan-Hellenic Conference on Informatics*. Nicosia Cyprus: ACM, pp. 9–14. ISBN: 978-1-4503-7292-3. DOI: 10.1145/3368640.3368655.
https://dl.acm.org/doi/10.1145/3368640.3368655
(visited on 05/22/2021)

Tranfield, David, David Denyer, and Palminder Smart (09/2003). "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review". en. In: *British Journal of Management* 14.3, pp. 207–222. ISSN: 1045-3172, 1467-8551. DOI: 10.1111/1467-8551.00375.
http://doi.wiley.com/10.1111/1467-8551.00375
(visited on 04/11/2021)

Vasin, Pavel (2014). "BlackCoin's Proof-of-Stake Protocol v2". en. In: p. 2

Wang, Ziyuan et al. (10/2018). "Distributed Ledger Technology for Document and Workflow Management in Trade and Logistics". en. In: *Proceedings of the 27th ACM International Conference on Information and Knowledge Management*. Torino Italy: ACM, pp. 1895–1898. ISBN: 978-1-4503-6014-2. DOI: 10.1145/3269206.3269222.
https://dl.acm.org/doi/10.1145/3269206.3269222
(visited on 05/22/2021)

Werner, Hartmut (2008). *Supply Chain Management: Grundlagen, Strategien, Instrumente und Controlling*. de. 3., vollst. überarb. und erw. Aufl. Gabler Lehrbuch. OCLC: 228137527. Wiesbaden: Gabler. ISBN: 978-3-8349-0504-8

Wu, Hanqing et al. (07/2019). "Data Management in Supply Chain Using Blockchain: Challenges and a Case Study". en. In: *2019 28th International Conference on Computer Communication and Networks (ICCCN)*. Valencia, Spain: IEEE, pp. 1–8. ISBN: 978-1-72811-856-7. DOI: 10.1109/ICCCN.2019.8846964.
https://ieeexplore.ieee.org/document/8846964/
(visited on 05/22/2021)

Xu, Zhitao et al. (09/2020). "Impacts of COVID-19 on Global Supply Chains: Facts and Perspectives". en. In: *IEEE Engineering Management Review* 48.3, pp. 153–166. ISSN: 0360-8581, 1937-4178. DOI: 10.1109/EMR.2020.3018420.
https://ieeexplore.ieee.org/document/9174793/
(visited on 02/23/2022)

Yiu, Neo C. K. (03/2021). "Decentralizing Supply Chain Anti-Counterfeiting and Traceability Systems Using Blockchain Technology". en. In: *Future Internet* 13.4, p. 84. ISSN: 1999-5903. DOI: 10.3390/fi13040084.
https://www.mdpi.com/1999-5903/13/4/84
(visited on 04/28/2021)

Zheng, Zibin et al. (06/2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". en. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. Honolulu, HI, USA: IEEE, pp. 557–564. ISBN: 978-1-5386-1996-4. DOI: 10.1109/BigDataCongress.2017.85.
http://ieeexplore.ieee.org/document/8029379/
(visited on 11/19/2021)

Zsifkovits, Helmut E (2012). *Logistik*. Vol. 3673. UTB

## Internet Sources

amfori (02/2020). *Dutch Child Labour Due Diligence Law.*
https://www.amfori.org/sites/default/files/amfori-2020-26-02-Dutch-Child-Labour-Due-Diligence-Law.pdf
(visited on 01/06/2022)

Authors, The go-ethereum (2021). *Private Networks.*
https://geth.ethereum.org/docs/interface/private-network
(visited on 08/13/2021)

Bateman, Alexis and Leonardo Bonanni (08/2019). *What Supply Chain Transparency Really Means.*
https://hbr.org/2019/08/what-supply-chain-transparency-really-means
(visited on 01/07/2022)

BCEI (04/2021). *Bitcoin Clean Energy Initiative Memorandum.*
https://assets.ctfassets.net/2d5q1td6cyxq/5mRjc9X5LTXFFihIlTt7QK/e7bcba47217b60423a01a357e036105e/BCEI_White_Paper.pdf
(visited on 12/09/2021)

*Beyond Supply Chain Transparency Laws* (09/2016).
https://www.cfr.org/blog/beyond-supply-chain-transparency-laws
(visited on 01/04/2022)

Bowman, Bob and Alexis Bateman (10/2019). *Is Supply-Chain Transparency Achievable?*
https://www.supplychainbrain.com/articles/30386-qa-is-supply-chain-transparency-achievable
(visited on 01/04/2022)

Community, Ethereum (2021a). *GAS AND FEES.*
https://ethereum.org/en/developers/docs/gas/
(visited on 08/06/2021)

– (2021b). *INTRO TO ETHEREUM.*
https://ethereum.org/en/developers/docs/intro-to-ethereum/#what-is-ethereum
(visited on 08/06/2021)

Community, Ethereum (2021c). *NETWORKS.*
https://ethereum.org/en/developers/docs/networks/
(visited on 08/06/2021)

– (2021d). *Privacy.*
https://docs.ethhub.io/ethereum-roadmap/privacy/
(visited on 08/13/2021)

– (2021e). *PROOF-OF-STAKE (POS).*
https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
(visited on 08/06/2021)

dantheman (2017). *DPOS Consensus Algorithm - The Missing White Paper.*
https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper
(visited on 10/01/2021)

Didovskiy, Andrey (02/2021). *Finality in Bitcoin.*
https://medium.com/coinmonks/finality-in-bitcoin-f82890bf39b7
(visited on 09/17/2021)

Digiconomist (10/2021a). *Bitcoin Energy Consumption Index.*
https://digiconomist.net/bitcoin-energy-consumption/
(visited on 10/01/2021)

– (2021b). *Ethereum Energy Consumption Index.*
https://digiconomist.net/ethereum-energy-consumption
(visited on 08/06/2021)

*Ethereum testnet (Ropsten) explorer* (08/2021).
https://teth.bitaps.com/
(visited on 08/13/2021)

Etherscan (08/2021a). *Ethereum Average Block Size.*
https://etherscan.io/chart/blocksize
(visited on 08/13/2021)

Etherscan (2021b). *Ethereum Blocktime.*
https://etherscan.io/chart/blocktime
(visited on 08/06/2021)

Foundation, IOTA (11/2017). *Introducing Masked Authenticated Messaging.*
https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e/
(visited on 09/16/2021)

– (05/2020). *An Introduction to IOTA Smart Contracts.*
https://blog.iota.org/an-introduction-to-iota-smart-contracts-16ea6f247936/
(visited on 09/16/2021)

– (03/2021). *IOTA Smart Contracts Protocol Alpha Release.*
https://blog.iota.org/iota-smart-contracts-protocol-alpha-release/
(visited on 09/16/2021)

*France's Duty of Vigilance Law* (n.d.).
https://www.business-humanrights.org/en/latest-news/frances-duty-of-vigilance-law/

Group, Hyperledger White Paper Working (08/2018). *An Introduction to Hyperledger.* (Visited on 08/26/2021)

Harris, Kamala D. (2015). *The California Transparency in Supply Chains Act - A Resource Guide*

Hyperledger Architecture Working and Group (2017). *Hyperledger Architecture, Volume 1 - Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus.* (Visited on 08/26/2021)

Hyperledger Sawtooth, Contributors to (2018). *Sawtooth FAQ - Consensus Algorithms.*
https://sawtooth.hyperledger.org/faq/consensus/#what-consensus-algorithms-does-sawtooth-support
(visited on 08/26/2021)

*ISO9000:2015(en)* (01/2022).
https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en
(visited on 01/03/2022)

Office, Home (12/2021). *Transparency in supply chains: a practical guide.*
https://www.gov.uk/government/publications/transparency-in-supply-chains-a-practical-guide/transparency-in-supply-chains-a-practical-guide
(visited on 01/06/2022)

Popov, Serguei (04/2018). *The Tangle.* (Visited on 09/15/2021)

Ramachandran, Navin (05/2021). *Energy Benchmarks for the IOTA Network.*
https://blog.iota.org/internal-energy-benchmarks-for-iota/
(visited on 09/15/2021)

Rosenberger, Bettina (02/2022). *EU-Lieferkettengesetz: Zivilgesellschaft präsentiert Entwurf.*
https://www.ots.at/presseaussendung/OTS_20220201_OTS0024/eu-lieferkettengesetz-zivilgesellschaft-praesentiert-entwurf
(visited on 02/08/2022)

Services, IOTA (2021). *What is IOTA?*
https://www.iota-services.com/what-is-iota/
(visited on 09/15/2021)

Siddharth, Jain (04/2019). *Hyperledger Fabric Consensus Explained.*
https://sidshome.wordpress.com/2019/04/01/hyperledger-fabric-consensus-explained/
(visited on 11/19/2021)

Stevens, Anthony (04/2018). *Distributed ledger consensus explained.*
https://hackernoon.com/distributed-ledger-consensus-explained-b0968d1ba087
(visited on 09/24/2021)

*The world's most valuable resource is no longer oil, but data | The Economist* (2021).
https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-

resource-is-no-longer-oil-but-data
(visited on 07/30/2021)

Thomson, Olivia (08/2021). *Supply chain legislation update: Australia, Germany and Norway.*
https://www.sedex.com/supply-chain-legislation-update-australia-germany-and-norway/
(visited on 01/04/2022)

ycharts.com (12/2021). *Ethereum Average Transaction Fee.*
https://ycharts.com/indicators/ethereum_average_transaction_fee
(visited on 12/10/2021)

# 7 Appendix

## 7.1 Interview Forms

# DLT for Supply Chain Applications - Preliminary Study

Which parameters are important to consider for a DLT implementation in a supply chain context? *

First thing is, what is the company doing. Top Lane & Bottom Lane.
Customers are willing to pay more for a sustainable sourced product. Depends on what the customers want. Most of the applications are specific. Reconciliation, any organization tells you much about it on its own. Interaction between financial flow and physical flow, very context specific.

## Rate the parameters

Following you see a list of parameters and requirements which can be considered in developing DLT solutions in the supply chain management domain. The parameters are clustered into three different sectors: User level, technical level and data level.
Please rate them according to how important you see them for architecting the DLT solution.

Thank you for your participation!

User Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Access Control | ○ | ○ | ○ | ◉ |
| Authentication and Authorization | ○ | ○ | ○ | ◉ |
| User Interface | ○ | ○ | ○ | ◉ |
| Flexibility regarding Users | ◉ | ○ | ○ | ○ |
| Identity Privacy | ◉ | ○ | ○ | ○ |

Would you add any parameters on this level?

Cost of implementation and deployment

Technical Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Scalability | ○ | ○ | ○ | ◉ |
| Flexibility regarding Integration | ○ | ○ | ○ | ◉ |
| Reliability | ○ | ○ | ○ | ◉ |
| Low Latency | ◉ | ○ | ○ | ○ |
| High Transactions per Second | ◉ | ○ | ○ | ○ |
| Availability | ○ | ○ | ○ | ◉ |

Would you add any parameters on this level?

Interoperability

Data Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Security | ○ | ○ | ○ | ◉ |
| Encryption | ○ | ○ | ○ | ◉ |
| Authentication | ○ | ○ | ○ | ◉ |
| Provenance | ○ | ○ | ○ | ◉ |
| Forecasting | ◉ | ○ | ○ | ○ |
| Confidentiality | ○ | ○ | ○ | ◉ |
| Immutability | ○ | ○ | ○ | ◉ |
| Data Privacy | ○ | ○ | ○ | ◉ |
| Integrity | ○ | ○ | ○ | ◉ |
| Validity | ○ | ○ | ○ | ◉ |
| Quality | ○ | ○ | ○ | ◉ |

Would you add any parameters on this level?

verifiable Claim, Verifiability

Anything else you want to mention?

At the end of the day it is use case specific, Blockchain is an add-on to the solution, slowly industry is also looking at how to provide value, up and coming platforms that bring scalability, and interoperability

# DLT for Supply Chain Applications - Preliminary Study

Which parameters are important to consider for a DLT implementation in a supply chain context? *

making sure that everyone wants to collaborate (or a majority of them), pull other people along when they see the benefits coming in
people who seat at the head of the chain and fund the process, willing to be able to make the investment
good understanding within the collection of businesses in the SC

## Rate the parameters

Following you see a list of parameters and requirements which can be considered in developing DLT solutions in the supply chain management domain. The parameters are clustered into three different sectors: User level, technical level and data level.
Please rate them according to how important you see them for architecting the DLT solution.

Thank you for your participation!

User Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Access Control | ◉ | ○ | ○ | ○ |
| Authentication and Authorization | ○ | ○ | ○ | ◉ |
| User Interface | ○ | ◉ | ○ | ○ |
| Flexibility regarding Users | ○ | ○ | ◉ | ○ |
| Identity Privacy | ◉ | ○ | ○ | ○ |

Would you add any parameters on this level?

identify the role in the organization rather than identify the user itself

Technical Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Scalability | ○ | ○ | ○ | ◉ |
| Flexibility regarding Integration | ○ | ○ | ○ | ◉ |
| Reliability | ○ | ○ | ○ | ◉ |
| Low Latency | ○ | ○ | ○ | ◉ |
| High Transactions per Second | ○ | ○ | ○ | ◉ |
| Availability | ○ | ○ | ○ | ◉ |

Would you add any parameters on this level?

Transactions per second also a second view on that - financial, finality delivery vs payment and completion, territoriality (where a tx occurs, law requires that the tx must physically complete in that country it origins)
reliability and availability is a very general thing
dlt that aren't hampered by the consensus mechanisms can handle the amount of txs way better
hybrid consensus @ activeledger (better for financial txs) -> consensus is an important part to understand

Data Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Security | ○ | ○ | ○ | ◉ |
| Encryption | ○ | ○ | ○ | ◉ |
| Authentication | ○ | ○ | ○ | ◉ |
| Provenance | ○ | ○ | ○ | ◉ |
| Forecasting | ○ | ○ | ○ | ◉ |
| Confidentiality | ○ | ○ | ○ | ◉ |
| Immutability | ○ | ○ | ○ | ◉ |
| Data Privacy | ○ | ○ | ○ | ◉ |
| Integrity | ○ | ○ | ○ | ◉ |
| Validity | ○ | ○ | ○ | ◉ |
| Quality | ○ | ○ | ○ | ◉ |

Would you add any parameters on this level?

utilizing neutral people talking about quality
data privacy is connected to encryption of data
quality assessment is also important
everyone has to understand the value of how data is validated, trade secrets can't be shared

Anything else you want to mention?

wrote a chapter for "industrial revolution 4" written by cranfield university

problem when implementing sc solutions: who is gonna fund it and what are the incentives to use it?
BMW is very much in control of their network, other buyers don't have the same power as BMW... it is very hard to find an incentive for all the other parties, natural behavior to distrust people; difficult to gather a bunch of companies towards one common objective
one thing that will make the people work together: money - sell SC finance systems that provide pre-shipment finance
previously letter of credit system - all was post-shipment loans;
use pre-shipment financing: APO (advanced payment obligations) that can be traded down the sc tiers; based on information how the APOs are used (no trade secrets), all past performances from a supplier are recorded on the DLT (important for a funder), independent quality assesser assess the quality of the goods & materials -> information becomes available anonymously for players in the finance SC
when smth goes wrong, treasurer for BMW can see where smth goes wrong, can do whatever it takes
Volkswagen scenario as a example

Incentive to use a SC platform has to be financial, preferrably driven by a big player. SCs compete not companies anymore.

# DLT for Supply Chain Applications - Preliminary Study

Which parameters are important to consider for a DLT implementation in a supply chain context? *

Scalability
Privacy, share data on one hand but not all of it
access control
how complicated it is to set up such a dlt network (setup costs)
transaction fees (ongoing costs, running and maintaining)

## Rate the parameters

Following you see a list of parameters and requirements which can be considered in developing DLT solutions in the supply chain management domain. The parameters are clustered into three different sectors: User level, technical level and data level.
Please rate them according to how important you see them for architecting the DLT solution.

Thank you for your participation!

User Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Access Control | ○ | ○ | ○ | ◉ |
| Authentication and Authorization | ○ | ○ | ○ | ◉ |
| User Interface | ○ | ◉ | ○ | ○ |
| Flexibility regarding Users | ○ | ◉ | ○ | ○ |
| Identity Privacy | ◉ | ○ | ○ | ○ |

Would you add any parameters on this level?

application addressed also for end users or only for companies, this influences identity privacy, in this case no end users

Technical Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Scalability | ○ | ○ | ○ | ◉ (selected) |
| Flexibility regarding Integration | ○ | ○ | ○ | ◉ (selected) |
| Reliability | ○ | ○ | ○ | ◉ (selected) |
| Low Latency | ○ | ◉ (selected) | ○ | ○ |
| High Transactions per Second | ○ | ○ | ◉ (selected) | ○ |
| Availability | ○ | ○ | ○ | ◉ (selected) |

Would you add any parameters on this level?

Data Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Security | ○ | ○ | ○ | (X) |
| Encryption | ○ | ○ | ○ | (X) |
| Authentication | ○ | ○ | ○ | (X) |
| Provenance | ○ | ○ | (X) | ○ |
| Forecasting | ○ | ○ | (X) | ○ |
| Confidentiality | ○ | ○ | ○ | (X) |
| Immutability | ○ | ○ | ○ | (X) |
| Data Privacy | ○ | ○ | (X) | ○ |
| Integrity | ○ | ○ | ○ | (X) |
| Validity | ○ | ○ | (X) | ○ |
| Quality | ○ | ○ | (X) | ○ |

Would you add any parameters on this level?

depends from which perspective you look on it, some parameters are tightly connected to each other importance of certain parameters will be different, depending on the definition of those, depends on the aspects/context it is handled

Anything else you want to mention?

# DLT for Supply Chain Applications - Preliminary Study

Which parameters are important to consider for a DLT implementation in a supply chain context? *

Scalability
Security
Speed
Depends on the context of the Supply Chain (transaction costs)
to whom do you prove it? (less decentralization in B2B context vs. more decentralization eg for the public)
how easy is it to onboard an existing supply process onto the blockchain (eg plug and play and integration)

## Rate the parameters

Following you see a list of parameters and requirements which can be considered in developing DLT solutions in the supply chain management domain. The parameters are clustered into three different sectors: User level, technical level and data level.
Please rate them according to how important you see them for architecting the DLT solution.

Thank you for your participation!

User Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Access Control | ○ | ○ | ○ | ◉ |
| Authentication and Authorization | ○ | ○ | ○ | ◉ |
| User Interface | ○ | ○ | ◉ | ○ |
| Flexibility regarding Users | ○ | ○ | ○ | ◉ |
| Identity Privacy | ○ | ○ | ◉ | ○ |

Would you add any parameters on this level?

..............................................................................................................................

Technical Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Scalability | ○ | ○ | ◉ | ○ |
| Flexibility regarding Integration | ○ | ○ | ○ | ◉ |
| Reliability | ○ | ○ | ○ | ◉ |
| Low Latency | ◉ | ○ | ○ | ○ |
| High Transactions per Second | ○ | ○ | ◉ | ○ |
| Availability | ○ | ○ | ○ | ◉ |

Would you add any parameters on this level?

scalability depends on how many entries there will be in connection with scalability
how decentralized is the network (means how much you can trust the network)
how secure is the network
incentives to use the network? or do they just HAVE to use it

Data Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Security | ○ | ○ | ○ | ● |
| Encryption | ○ | ○ | ● | ○ |
| Authentication | ○ | ○ | ○ | ● |
| Provenance | ○ | ○ | ○ | ● |
| Forecasting | ● | ○ | ○ | ○ |
| Confidentiality | ○ | ○ | ● | ○ |
| Immutability | ○ | ○ | ○ | ● |
| Data Privacy | ○ | ○ | ● | ○ |
| Integrity | ○ | ○ | ○ | ● |
| Validity | ○ | ○ | ○ | ● |
| Quality | ○ | ○ | ● | ○ |

Would you add any parameters on this level?

combine integrity, immutability and security into one
it could be the case that all dlt design already have certain parameters so that would result in rating them not at all important because they are included in every one
merge confidentiality and encryption, privacy

what kind of data can be added (storing data on dlts is expensive) eg storing pictures could be an issue

Anything else you want to mention?

many of the points depend highly on the use case

# DLT for Supply Chain Applications - Preliminary Study

Which parameters are important to consider for a DLT implementation in a supply chain context? *

throughput, could be a restriction if a lot of objects are tracked
economic predictability in regards to tx fees, clear estimation what it costs
time to finality, absolute finality vs. probabilistic finality , important that it is fixed more or less fast
if multiple parties access the same data very closely afterwards -> network sync time, the whole network should be at the same state within a short matter of time
programmability: flexibility, what can you do with the network, allowing you to have multisig txs
high availability: network should not be congested, fast way to uncongest itself, favor liveness over safety
privacy: data privacy, but transactions can be public, no privacy measures at all

## Rate the parameters

Following you see a list of parameters and requirements which can be considered in developing DLT solutions in the supply chain management domain. The parameters are clustered into three different sectors: User level, technical level and data level.
Please rate them according to how important you see them for architecting the DLT solution.

Thank you for your participation!

User Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Access Control | ○ | ○ | ◉ | ○ |
| Authentication and Authorization | ○ | ○ | ○ | ◉ |
| User Interface | ○ | ○ | ○ | ◉ |
| Flexibility regarding Users | ○ | ○ | ○ | ◉ |
| Identity Privacy | ○ | ◉ | ○ | ○ |

Would you add any parameters on this level?

access control and flexibility regarding users tightly connected
identity privacy: depending on the scope of privacy
authentication and access control could be merged

Technical Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Scalability | ○ | ○ | ● | ○ |
| Flexibility regarding Integration | ○ | ○ | ○ | ● |
| Reliability | ○ | ○ | ○ | ● |
| Low Latency | ○ | ● | ○ | ○ |
| High Transactions per Second | ○ | ○ | ● | ○ |
| Availability | ○ | ○ | ○ | ● |

Would you add any parameters on this level?

scalability strongly depends on use case and setting; active scaling (grwoing demand) and passive scaling (supply shrinking)
low latency depending on use case
high tps depending on the use case, how granular is the data; is in interplay with economic predictability
consistency, thinking of sharding, no matter how many tps you have; shards are drawing down the tps

Data Level *

| | Not at all important | Slightly important | Fairly important | Very important |
|---|---|---|---|---|
| Security | ○ | ○ | ○ | ◉ |
| Encryption | ○ | ○ | ○ | ◉ |
| Authentication | ○ | ○ | ○ | ◉ |
| Provenance | ○ | ○ | ○ | ◉ |
| Forecasting | ○ | ◉ | ○ | ○ |
| Confidentiality | ○ | ○ | ◉ | ○ |
| Immutability | ○ | ○ | ○ | ◉ |
| Data Privacy | ○ | ◉ | ○ | ○ |
| Integrity | ○ | ○ | ○ | ◉ |
| Validity | ○ | ○ | ○ | ◉ |
| Quality | ○ | ○ | ○ | ◉ |

Would you add any parameters on this level?

encryption depending on the use case, can also correlate back to access control
provenance is always given for a single data point, but not on application level, actual benefit of the SC implementation
forecasting emerges from the properties of DLT if you need it you can do it
confidentiality heavily correlating with encryption
data privacy is fighting against data privacy - trade off
encryption and data privacy very closely connected, interpreted it as data anonymity
integrity is always given
needs quite some resources upfront to find out how to describe data, how to refer, how to get the input
Security = privacy, immutability, integrity = that those things cannot be changed

persistence: do I need the data all the time or is it enough if data is deleted after ~2 days

Anything else you want to mention?

data part was quite hard to evaluate, not sure if it's about the data point or about the application (higher level); might be easier to implement the different properties

what was missing overall: use case, domain specific information, boundaries, how should the application grow? this alone brings huge changes to al the properties

## 7.2 Different DLT Designs, Characteristics and their Configurations

In order to retrieve the characteristics and the configuration possibilities of each of the covered DLT designs, first, the interesting characteristics and the networks to be included need to be identified. The literature research covers several recent implementations of DLT applications for supply chains, the DLT designs that were mentioned and used in the case studies serve as a good starting point for considerations. As the goal of this thesis is to establish a quantitative evaluation framework for different DLT frameworks, also quantifiable characteristics are obtained for further investigations. Chowdhury et al. provide a comprehensive list of quantitative attributes to consider, when evaluating different DLT networks and platforms.[174]

- **Type:** Public or Private.
- **Scalability:**

  **Block Size:** Maximum allowed block size in a DLT system.

  **Block Creation Time:** Average block creation time of a system.
- **Transaction Costs:** Costs for processing or storing data in the ledger.
- **Consensus Algorithm:** Specifies how consensus in the distributed ledger is achieved.
- **Energy Consumption:** How much energy is used for the creation of a new block a new transaction?
- **Privacy:** Has the system built in privacy mechanisms?
- **Identity and Auditability:** The identification method used in the network.
- **Suitability:** Indicates the systems ability to be suitable to different data types, sizes or volumes.
- **Robustness and Resilience:** How does the system react to certain types of attacks and errors?

Although, these characteristics are basically valid for a lot of DLT concepts and designs, some characteristics are not applicable to some DLT designs. For example the IOTA network, which is a TDAG doesn't use blocks at all, therefore it has no block size and creation time per se.[175]

[174] Chowdhury et al. 2019.
[175] Sunyaev 2020.

So, after this initial considerations, the characteristics and their configuration possibilities for each DLT design that should be included in the model should be found out. For this reason the documentation and crucial blog articles regarding these networks are studied. The characteristics can have different configurations and to make it possible to clearly differentiate them from each other, clear configurations are defined before analysing the different DLT designs.

- **Type:** Public or Private.
- **Scalability:**

  **Block Size:** NA, Customisable, Small, Large

  **Block Creation Time:** NA, Customisable, Low, High
- **Transaction Costs:** Free, Low (<1$), High (>1$)
- **Consensus Algorithm:** Proof-of-Stake, Proof-of-Work, Proof-of-Authority, PBFT, ...
- **Energy Consumption:** Low, High
- **Privacy:** No possibility, In Development, Possible, Built In
- **Identity and Auditability:** Known Entities, Pseudonymus, Anonymus
- **Suitability:** Very Limited, Limited, High
- **Robustness and Resilience:** Not Resilient, OK, High Resilience

### 7.2.1 Ethereum Public Network

Ethereum Mainnet is a public blockchain network built on a proof-of-work consensus mechanism. It is although planned to switch to the more energy efficient Proof-of-Stake consenus in the near future (approximately in the timeframe of 2021-2022).[176] In order to use the network for transactions or for the deployment of smart contracts transaction fees (also called gas fees) need to be paid in Ether (ETH). Ether is the underlying cryptocurrency to the Ethereum network.[177]

- **Type: Public**
- **Scalability:**

[176] Community 2021e.
[177] Community 2021b.

**Block Size: Large.** Dependent on network demand, target size of 15 million gas but block size can increase up to 30 million gas.[178] On average this corresponds to 72.470 bytes as of 12.08.2021.[179]

**Block Creation Time: High.** 13,48 seconds, as of 06.08.2021[180]

- **Transaction Costs: High.** The cost for an Ethereum transaction is dependent on computational work that is needed to perform this transaction. Meaning, that a simple transaction needs less transaction costs than the execution of a smart contract. Moreover, it is also important to consider, that the dollar price for a transaction is dependent on the current price of the Ethereum cryptocurrency (ETH). But generally it can be said, that transactions on Ethereum are expensive, with simple transactions costing around $4 and smart contract calls costing quickly $100 and upwards, as of 10.12.2021.[181]
- **Consensus Algorithm: Proof-of-Work**[182]
- **Energy Consumption: High.** 134.54 kWh per transaction or the average of 4,55 US households[183]
- **Privacy: In Development.** There are no privacy mechanisms built in the public Ethereum network. However, several teams are working on developing different privacy mechanisms which can be used on top of Ethereum.[184]
- **Identity and Auditability: Pseudonymus.** The whole blockchain is publicly transparent and users interact with the help of addresses derived from public-private keypairs with each other, meaning the network is pseudonymous.
- **Suitability: High.** Ethereum is a DLT design which also allows for the deployment of smart contracts. Moreover, several standards for different data formats are already developed, which make Ethereum very suitable to different needs.[185]
- **Robustness and Resilience: High Resilience**

### 7.2.2 Ethereum Ropsten Test Network

As Ethereum is a protocol, there are several networks that are implementing this protocol independently from each other. There are various test networks (Testnets) for Ethereum,

[178] Community 2021a.
[179] Etherscan 2021a.
[180] Etherscan 2021b.
[181] ycharts.com 2021.
[182] Community 2021e.
[183] Digiconomist 2021b.
[184] Community 2021d.
[185] Community 2021b.

where developers can test the functionalities of their smart contracts without having to pay real ETH for transaction fees. The Ropsten test network is the only Ethereum test network that is based on a proof-of-work consensus mechanism, therefore at the moment, this is the best representation of the Ethereum Mainnet. Apparently some articles from the literature review also used the Ropsten test network to build proof-of-concepts or prototypes of their supply chain application.[186]

- **Type: Public**
- **Scalability:**

  **Block Size: Small.** Average block size as of 13.08.2021 is 15.475 bytes[187]

  **Block Creation Time: High.** 14 seconds, as of 13.08.2021[188]
- **Transaction Costs: Free.** Although there are also transaction fees on Ropsten Testnet, these are paid with Testnet ETH, which have no value and can be claimed for free in certain amounts.
- **Consensus Algorithm: Proof-of-Work**[189]
- **Energy Consumption: High**
- **Privacy: In Development.** Privacy mechanisms which are developed for Ethereum Mainnet are also compatible with Ropsten Testnet.
- **Identity and Auditability: Pseudonymus**
- **Suitability: High**
- **Robustness and Resilience: Not Resilient.** Due to the fact, that Ropsten Testnet uses the Proof-of-Work consensus mechanisms, but has no valuable incentive for miners (Testnet ETH do not possess any monetary value unlike to Mainnet ETH), the network is very vulnerable.[190]

### 7.2.3 Ethereum Proof of Authority

The Ethereum protocol can be also deployed in a private network where all nodes are known to each other and trusted by each other. In this case the nodes are not connected to any public Ethereum network (neither mainnet or testnet). Because of that, a simpler consensus algorithm known as proof-of-authority can be used in such networks.[191]

[186] Community 2021c.
[187] Community 2021a.
[188] *Ethereum testnet (Ropsten) explorer* 2021.
[189] Community 2021c.
[190] Community 2021c.
[191] Community 2021c.

- **Type: Private**
- **Scalability:**

  **Block Size: Customisable**

  **Block Creation Time: Customisable**
- **Transaction Costs: Free**
- **Consensus Algorithm: Proof-of-Authority**[192]
- **Energy Consumption: Low**
- **Privacy: In Development** Privacy mechanisms which are developed for Ethereum Mainnet are also compatible with private Ethereum implementations.
- **Identity and Auditability: Known Entities**
- **Suitability: High**
- **Robustness and Resilience: OK.** Due to the fact, that all network actors are known entities, certain attack vectors can be neglected. However, usually the number of nodes in such networks is restricted to a certain size, which contributes to the fact, that the network is more centralised and not as resilient as a fully decentralised network.[193]

### 7.2.4 Hyperledger Fabric

Hyperledger is a global collaboration of leaders in finance, manufacturing, Internet of Things and supply chain. It is hosted under the Linux Foundation. Hyperledger itself does not promote a single blockchain project, it is rather an open-source community of developers who are developing several different pieces of infrastructure and code.

Hyperledger Fabric specifically is a platform which enables distributed ledger solutions to be built in a modular fashion. Through this flexibility, solutions built on Hyperledger Fabric can be adapted for any industry. In contrast to most other DLT designs, Hyperledger Fabric does not rely on any native cryptocurrency.[194]

- **Type: Private**

[192] Authors 2021.
[193] Angelis et al. n.d.
[194] H. W. P. W. Group 2018.

- **Scalability:**

  **Block Size: Customisable**

  **Block Creation Time: Customisable**

- **Transaction Costs: Free**

- **Consensus Algorithm: Kafka.** Consensus in Hyperledger Fabric networks is achieved in three steps:

  1. Endorsement of transactions
  2. Ordering of transactions
  3. Validating of transactions

  Theoretically for each of these 3 phases different consensus mechanisms can be plugged in, but Kafka is the out of the box solution. Other implementations are still mostly under development.[195]

- **Energy Consumption: Low**

- **Privacy: Built In**

- **Identity and Auditability: Known Entities**

- **Suitability: High**

- **Robustness and Resilience: Not Resilient.** While Hyperledger Fabric with Kafka consensus is crash fault tolerant it is not Byzantine fault tolerant.

### 7.2.5 Hyperledger Sawtooth

Hyperledger Sawtooth is a platform which provides tools to build, deploy and run distributed ledgers in a modular way. The strength of Sawtooth is its modularity and flexibility, for example is it possible to change the consensus algorithm while the blockchain is running. Furthermore, it is compatible with Ethereum smart contracts. It also provides the consensus algorithm Proof of elapsed time (PoET), which provides the scalability of Proof-of-Work without the drawback of high power consumption.[196]

- **Type: Private**

- **Scalability:**

  **Block Size: Customisable**

  **Block Creation Time: Customisable**

[195] Hyperledger Architecture Working and Group 2017.
[196] H. W. P. W. Group 2018.

- **Transaction Costs: Free**
- **Consensus Algorithm: Supports several algorithms: Devmode, PBFT, PoET CFT, PoET SGX, Raft.**[197]
- **Energy Consumption: Low**
- **Privacy: In Development**
- **Identity and Auditability: Known Entities**
- **Suitability: High**
- **Robustness and Resilience: OK**

### 7.2.6 IOTA Tangle

IOTA is an open and feeless data and value transfer protocol, especially designed for the Internet-of-Things (IoT) industry. The main differentiation to all other previously mentioned DLT designs is that IOTA builds upon a DAG called "The Tangle". More theoretical background on this subject was already provided in section 3.6. This concept brings with it advantages as well as disadvantages, as it can be seen in the following characteristics.[198][199]

- **Type: Public**
- **Scalability:**

  **Block Size: NA**

  **Block Creation Time: NA.** Due to the fact, that the underlying concept of IOTA is based on transactions written directly in the tangle, there are no blocks in IOTA.
- **Transaction Costs: Free**
- **Consensus Algorithm: NA**
- **Energy Consumption: Low**[200]
- **Privacy: Possible**[201]
- **Identity and Auditability: Pseudonymous**

[197] Hyperledger Sawtooth 2018.
[198] Popov 2018.
[199] Services 2021.
[200] Ramachandran 2021.
[201] Foundation 2017.

- **Suitability: Limited.** There are certain more advanced possibilities than just transferring assets possible on IOTA. But currently IOTA does not support smart contracts, which would provide a greater suitability for various use cases.[202] At the moment, an alpha release of smart contracts on IOTA can be tested.[203]

- **Robustness and Resilience: OK**

[202]Foundation 2020.
[203]Foundation 2021.