ENHANCING TRUST IN SUPPLY CHAIN PROCESSES USING BLOCKCHAIN TECHNOLOGY

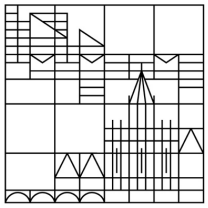
Bachelor's thesis

submitted by

DANIEL MUFFLER

at the

Universität Konstanz



to obtain the academic degree
Bachelor of Science (B. Sc.)

Information Science Group

Department of Computer and Information Science

Enrolment number: 01/951524

1. Reviewer: PROF. DR. BELA GIPP

2. Reviewer: PROF. DR. KARSTEN DONNAY

Supervisor: THOMAS HEPP

Konstanz, March 2019

REVIEWERS:
Prof. Dr. Bela Gipp
Prof. Dr. Karsten Donnay

SUPERVISOR:
Thomas Hepp

LOCATION:
Konstanz

AUTHOR:
Daniel Muffler

Daniel Muffler: *Enhancing Trust in Supply Chain Processes using Blockchain Technology,* Bachelor's thesis, © March 2019

ABSTRACT

The blockchain technology gains more and more importance in the industrial sector. Consequently, Supply Chain Management as one of the most critical topics in the present globalized world for companies and consumers will also be affected by blockchains. Supply Chain Management is a pivotal factor of success for enterprises but also for consumer protection reasons. The aims of this work are to successfully integrate the blockchain technology into supply chain processes and enhance trust for all participating parties. In addition to this, upcoming issues like latency and scalability are investigated and analyzed.

The main contribution of this thesis is the development and implementation of a blockchain-based supply chain approach which enhances trust and maintains scalability. Through an extensive evaluation and comparison between existing work and the prototype, trust indication parameters in blockchain-based supply chains can be specified and a newly blockchain design for usage in supply chains is proposed. Furthermore, the introduction of new features and the use of technologies, which support decentralization, leads to a completely novel approach for blockchain-based supply chains including payments, orders, and tracking. With this new design, trust and transparency for participating parties in the supply chain are supported while data timestamps ensure a highly scalable system.

Finally, the comparison to existing approaches together with additional expert interviews illustrate the necessity of future research that has to be done in order to improve processes in supply chains and provide support for the integration of blockchain technology (BT). Nevertheless, the evaluation of the system approaches shows the potential of the BT integration in supply chain processes and emphasizes upcoming issues and obstacles that need to be overcome.

ZUSAMMENFASSUNG

Die Blockchain-Technologie gewinnt im industriellen Bereich immer mehr an Bedeutung. Demzufolge wird auch das Supply Chain Management als eines der kritischsten Themen in der heutigen globalisierten Welt für Unternehmen und Verbraucher von Blockchains beeinflusst werden. Lieferkettenmanagement ist zudem ein zentraler Erfolgsfaktor für Unternehmen, aber auch von entscheidender Bedeutung für den Verbraucherschutz. Ziel dieser Arbeit ist es, die Blockchain-Technologie in Lieferketten-Prozesse zu integrieren und das Vertrauen aller Beteiligten zu stärken. Darüber hinaus werden anstehende Probleme wie Latenz und Skalierbarkeit untersucht und analysiert.

Der wichtigste Beitrag dieser Arbeit ist die Entwicklung und Umsetzung eines neuen Ansatzes einer blockchain-basierten Lieferkette, der das Vertrauen zwischen Beteiligten in der Lieferkette stärkt und dabei gleichzeitig Skalierbarkeit erhält. Durch eine umfassende Bewertung und Gegenüberstellung von bestehenden Arbeiten und dem Prototyp können Parameter für Vertrauensindikatoren in blockchainbasierten Lieferketten spezifiziert und ein neues Blockchain-Design für den Einsatz in Lieferketten vorgeschlagen werden. Darüber hinaus führt die Einführung neuer Features und der Einsatz von Technologien zur Unterstützung der Dezentralisierung zu einem völlig neuen Ansatz für blockchain-basierte Lieferketten einschließlich von Zahlung, Bestellung und Tracking. Vertrauen und Transparenz für die Beteiligten in der Lieferkette werden unterstützt, während Datenzeitstempel ein hochskalierbares System gewährleisten.

Schließlich zeigen der Vergleich mit bestehenden Ansätzen und zusätzliche Experten-Interviews die Notwendigkeit zukünftiger Forschungsarbeiten, um Prozesse in Lieferketten zu verbessern und die Integration der Blockchaintechnologie (BT) zu unterstützen. Dennoch zeigt die Bewertung der Systemansätze das Potenzial der BT-Integration in Lieferketten-Prozesse und verdeutlicht noch ungelöste Probleme und Hindernisse, die es zu überwinden gilt.

Science is knowledge which we understand so well
that we can teach it to a computer;
and if we don't fully understand something,
it is an art to deal with it.

— Donald E. Knuth [54]

ACKNOWLEDGEMENTS

This bachelor thesis would not have been possible without the collaboration and generous support of numerous individuals. I am thankful to my doctoral advisor, Thomas Hepp, for his support in my research. I also thank Professor Bela Gipp and Professor Karsten Donnay for their examination of the thesis. Without the help and willingness of the experts for the interviews, the evaluation would not have been as good and comprehensive as it would have been without. Therefore, I wish to thank them for their collaboration. Finally, I would like to thank my family and friends for their general support and feedback on the thesis.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

API Application Programming Interface: Software-to-software interface managing the seamless interaction between multiple applications.

BT Blockchain Technology

B2B Business-to-business

B2C Business-to-consumer

HTLC Hashed TimeLock Contract

P2P Peer-to-peer

REST REpresentational State Transfer: Architectural style for developing web services.

SCM Supply Chain Management

1 INTRODUCTION

This bachelor thesis deals with the novel topic of blockchain-based supply chains. It addresses the problem of insufficient trust in supply chains between participating parties and upcoming scalability issues. As an example, food fraud caused by tracking and transparency lacks in supply chain is still a present issue [1]. Without consistent and transparent traceability, especially consumers cannot trust sold products and thus cannot trust the sellers. Another example that demonstrates major problems in supply chains is wine scandals [2]. If there is no traceability and no transparency in supply chain processes, wine scandals and other scandals will continue to occur. There are numerous other examples illustrating the deficits in supply chain processes.

1.1 PROBLEM SETTING

The P2P electronic cash system called Bitcoin was the starting point of a new technology called blockchain. Originally invented by Satoshi Nakamoto, the usage of blockchains and their fields of application increase massively [14]. "The blockchain data structure is an ordered back-linked list of blocks of transactions. The blockchain can be stored as a flat file, or in a simple database. Blocks are linked “back”, each referring to the previous block in the chain. Each block within the blockchain is identified by a hash, generated using the SHA256 cryptographic hash algorithm on the header of the block. Each block also references a previous block, known as the parent block, through the “previous block hash” field in the block header." [3] Using blockchains for the cryptocurrency, Bitcoin is the first currency that is no longer dependent on third-party institutions like banks. Therefore, Bitcoin is a fully decentralized currency [3].

Since the publication of the Bitcoin whitepaper by Nakamoto in 2009 the blockchain technology (BT) and its popularity is rising inexorably[3]. Several large corporations have developed or plan to develop their own blockchain systems or integrate BT into existing systems[4].

1 http://www.haz.de/Nachrichten/Wissen/Uebersicht/Wir-brauchen-eine-gesetzliche-Kontrollpflicht-der-Handelsketten

2 https://www.washingtonpost.com/lifestyle/food/two-of-the-years-wine-scandals-could-have-far-reaching-consequences/2018/12/20/3c3fa676-04a0-11e9-b5df-5d3874f1ac36_story.html

3 https://smartereum.com/40345/

4 https://www.forbes.com/sites/andrewrossow/2018/07/10/top-10-new-blockchain-companies-to-watch-for-in-2018/

Even in supply chain processes, research is spreading enormously [14]. The necessity for improvements in supply chains was clearly evident when the horse meat scandal in Europe took place in 2013[5]. This food scandal was followed by many others[6]. In 2013, it was not possible to clarify for how long horse meat was sold incorrectly as beef. This was due to the fact that the source of the wrong meat could not be found quickly enough and governments stated that no irregularities had been found [7]. This shows that current Supply Chain Management (SCM) systems no longer meet the requirements of an increasingly globalized world. In addition, customer confidence is weakened, especially in the food supply chain. That is the reason why an SCM system has to meet certain criteria and requirements to be reliable for customers. In this work, the main focus is set on trust optimization in supply chain processes.

1.2 MOTIVATION

My motivation for doing research in the novel topic of supply chains with blockchain integration is based on the dynamic in the research field of blockchains. The connection of blockchains to supply chains increases timeliness and thus is gaining huge importance. Besides, there are still large areas that have not been researched yet which makes it exciting to explore new scientific achievements work in this field.

1.3 RESEARCH OBJECTIVES

As blockchain systems offer the possibility for decentralization, data immutability and consensus finding (e.g. in cryptocurrencies), the integration of the BT in supply chain processes has the potential to improve supply chains in order to prevent security lacks and breaches of trust between the participating parties in supply chains. Consequently, the following research questions arise:

1. *How can BT be integrated into supply chain processes while maintaining supply chain scalability?*
2. *How can trust be enhanced in supply chains using blockchain integration?*

5 https://www.bbc.com/news/uk-21335872
6 http://www.thatsmags.com/shanghai/post/21647/10-of-china-s-worst-food-scandals-2017
7 https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide

Answering these two questions results in the following scientific contributions: Currently known approaches of blockchain-integrating supply chain systems are presented and evaluated. In addition, based on the evaluations, an own prototype of a blockchain-based approach is introduced. The prototype itself is analyzed so that the strengths and weaknesses can be shown and indication parameters for trust enhancement in supply chains can be proposed. Finally, with the introduction of a new blockchain design for supply chain systems which maintains scalability, the last contribution is made.

Thus, the following research tasks can be derived:

> **Task 1:** *Perform an extensive literature survey in order to analyze the strengths and weaknesses of state-of-the-art blockchain-based supply chain approaches.*
>
> **Task 2:** *Develop an integrity-ensuring storing of the data which is stored in the supply chain and integrate the OriginStamp service.*
>
> **Task 3:** *Design a mapping of products and consumers that ensures and guarantees security with respect to unique mappings using Hashed Timelock Contracts.*
>
> **Task 4:** *Implement a prototype of this supply chain system where it is possible to add data to the supply chain.*
>
> **Task 5:** *Prepare and conduct expert interviews in order to enrich and extend the prototype evaluation.*
>
> **Task 6:** *Evaluate the proposed concept by comparing it to other blockchain-based supply chain systems and evaluate the expert interviews.*

1.4 THESIS OUTLINE

Chapter 1 describes the problem setting, the research motivation, and the research objective. Chapter 2 gives a brief overview of existing surveys and evaluations on blockchain-based systems and blockchain-based supply chain system. Chapter 3 then explains the concepts for the examined papers and presents the setup for the expert interviews. Within Chapter 4, the prototype and the related design choices are presented. Different approaches of blockchain-based supply chain systems and their comparisons to the prototype are introduced in Chapter 5 as well as the results of the expert interviews. This is followed by a comprehensive discussion in Chapter 6. Finally, Chapter 7 illustrates possible future work concludes.

2

BACKGROUND AND RELATED WORK

This chapter provides an overview of core concepts and related work. The number of publications in the blockchain area has increased enormously over the past years [14]. Therefore, central and relevant work is presented here together with important background information.

2.1 CRYPTOCURRENCIES AND BLOCKCHAINS

As stated in Chapter 1, Bitcoin as the first cryptocurrency marks the beginning of the underlying BT. Nowadays, blockchains have more general usages. Blockchains can be described as distributed databases or private ledgers, where transactions need to be verified before they can be collected in blocks. Blocks are connected through the previous block hash. Additionally, blockchains by design meet the following four key characteristics: decentralization, data immutability, security, and smart execution [83].

2.1.1 *Consensus protocols*

Assuring data immutability, integrity, authentication, and verifiability, the blockchain has to provide a mechanism on how to decide which block of transactions will be included in the blockchain. The category of algorithms which solve the arising problem is named *Byzantine Fault Tolerance (BFT)*. Therefore, a consensus protocol is defined. For the purpose of this thesis, the scope is limited to two consensus protocols: Proof-of-Work (PoW), which is also used by Bitcoin, and Proof-of-Stake (PoS), which will be used by the cryptocurrency Ethereum. These two are the most widely used consensus protocols [4].
The concept of PoW implies that mining is based on solving calculations. As shown in Figure 1, each block contains a nonce. A nonce can be a number that has to be calculated by the mining nodes. Further, each block has a so-called difficulty. The difficulty declares the number of zero bits of the hash value of the transaction block. The task for the miners is to find a nonce such that the entire block hash value meets the difficulty of the block. If the nonce is found, the block is added to the chain [4, 67, 70].

In comparison to the concept of PoW, PoS is based on the accumulation of stakes. During the initial mining phase, PoW is used. After that, each coin in the blockchain has an individual *age*. The impact of a node results from the number of coins and their age. The older the coins, the more stake has a node. For adding a new block, a certain

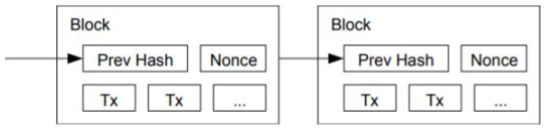


Figure 1: Blocks within a PoW-based blockchain, taken from [4]

amount of stake is necessary. If a participant has the specified amount of stake and is chosen by the network to mine the block, the block can be added to the blockchain [4, 7, 67, 70].
Compared to PoS, PoW requires much more computing power, since the reward for mining is distributed to the node that first solved the mathematical puzzle. This leads to a competition of miners and an increased energy demand [57].

2.1.2 *Scalability*

A central problem of blockchains is the scalability. This means that in the case of cryptocurrencies, for example, the number of transactions per second is sometimes severely limited. With Bitcoin, a block confirmation with a 10-minute interval takes approximately 1 hour. This limitation results from the choice of the consensus protocol. Ethereum, however, uses a 14-second block interval. This results in a block confirmation time of about 3 minutes [104]. Using PoS instead of PoW can decrease the block confirmation time enormously because PoS gets rid of the latency caused by solving complex calculations first.

Croman et al. provide an extensive analysis of scalability in blockchains [20]. They take different layers of the blockchain and discuss them in terms of scalability issues. As stated above, one bottleneck is the consensus protocol in the consensus layer. For highly scalable blockchains, the consensus protocol has to fit the use case. Croman et al. propose different optimizations, like sharding, to improve concurrent tasks. The network layer can also become problematic if e.g. the bandwidth is not fully used. The third layer is the storage plane as a global memory of the consensus layer's output, where write and read operations in the blockchain has to be carefully set. Otherwise, the performance will be bad. Finally, the last plane introduced by the authors is the side layer. Discussing this layer, the authors refer to off-chain storage and off-chain consensus (see Section 2.2). In summary, the authors name scalability issues and discuss them briefly.
Hepp et al. take a look at the usage of Directed Acyclic Graphs (DAGs) and their scalability performance [42]. Their analysis emphasizes that DAGs instead of chains can increase the throughput of transactions per second. Compared to Bitcoin, DAGs outperform it by factor 5 to 850. However, the authors state the necessity of a gener-

alized testing scheme to standardize parameter settings and further circumstances.

2.1.3 *Smart Contracts*

An extension for blockchains was realized by Smart Contracts. Smart Contracts are pieces of code that are executed on the blockchain. Among other things, conditions can be defined. Once the code for a Smart Contract has been stored in the blockchain, it is usually unchangeable. This concept makes it possible to build up trust between parties through contracts. Thus, Smart Contracts can automate complex multi-step processes [16].
As real-world contracts can be mapped to contracts running on a blockchain, Smart Contracts extend the use cases of blockchains massively [16].

2.2 STORAGE

Hepp et al. examines on-chain versus off-chain storage for supply chains [39]. They state in their work that on-chain storage should not be used for supply chains. This can be justified by various reasons including the huge amount of data. It exceeds the means of on-chain storage and off-chain storage and thus decreases scalability. Therefore off-chain storage is chosen for this work.
For the tracking data, the InterPlanetary File System (IPFS) is used. IPFS can be described as a peer-to-peer distributed file system. It offers the possibility of decentralized storage without storing the data in a blockchain. IPFS is based on the Bitcoin protocol and consists of nodes which participate in the network. Files are stored locally by nodes or can be pinned by other nodes. The file distribution is based on the BitSwap protocol and files can be accessed via an IPFS hash. IPFS builds a directed acyclic graph to link between objects in the network. Thus, the file distribution in IPFS is designed for high throughput. Additionally, IPFS is decentralized and has no single point of failure [5].

2.3 TIMESTAMPS

OriginStamp is a trusted timestamping service, arisen from a research project. Timestamps are submitted as hash values by aggregating them in a Merkle Tree. Only the root hash is embedded in a transaction of a cryptocurrency. At present, only Bitcoin as cryptocurrency is supported. Verification of the timestamp can be done through cer-

tificates without OriginStamp, where the essential parts of the Merkle Tree for the verification of the root hash are included [31, 40].[1]

2.4 TRUST IN EXCHANGES

Petersen states in his work that the term trust should be defined first in order to avoid ambiguity and confusion. Blockchain integration could solve and overcome trust issues in supply chain processes. Therefore, *Contract Trust, Predictability* and *Dependability* are introduced as measurement variables for trust in blockchain-based supply chains [76]. "Contractual trust is if the other party will carry out its contractual agreements, and rests on a shared moral norm of honesty and promise keeping" [76]. The author also provides descriptions of the other parameters: "predictability is when a partner in an inter-organizational relationship will behave in a predictable manner and will act and negotiate fairly when the possibility for opportunism is present even though the possibility of betrayal is present" [76] and "dependability refers to expectations that the partner will act in the alliance's best interest" [76]. For this thesis, the term trust is always used and examined in the context of these three aspects.

2.5 RELATED WORK

Next follows an overview of related work about blockchain-based supply chains and their possibilities.
Sternberg et al. confirm the actuality of blockchains in supply chains [86]. They also state that the research area is sparsely researched and name industry initiatives as well as current researches.
Saberi et al. generally deal with the connection of the BT and supply chains and how blockchains can be used in supply chains [83]. Figure 2 shows the possible integration points of blockchains into supply chain processes. The usage of Smart Contracts can optimize and decentralize the processes in supply chains. The role of Smart Contracts in the context of supply chains is also discussed. The authors state, that Smart Contracts offer improvements for business supply chain use cases. Furthermore, sustainability and barriers of blockchain-based supply chains are covered.

1 https://originstamp.org

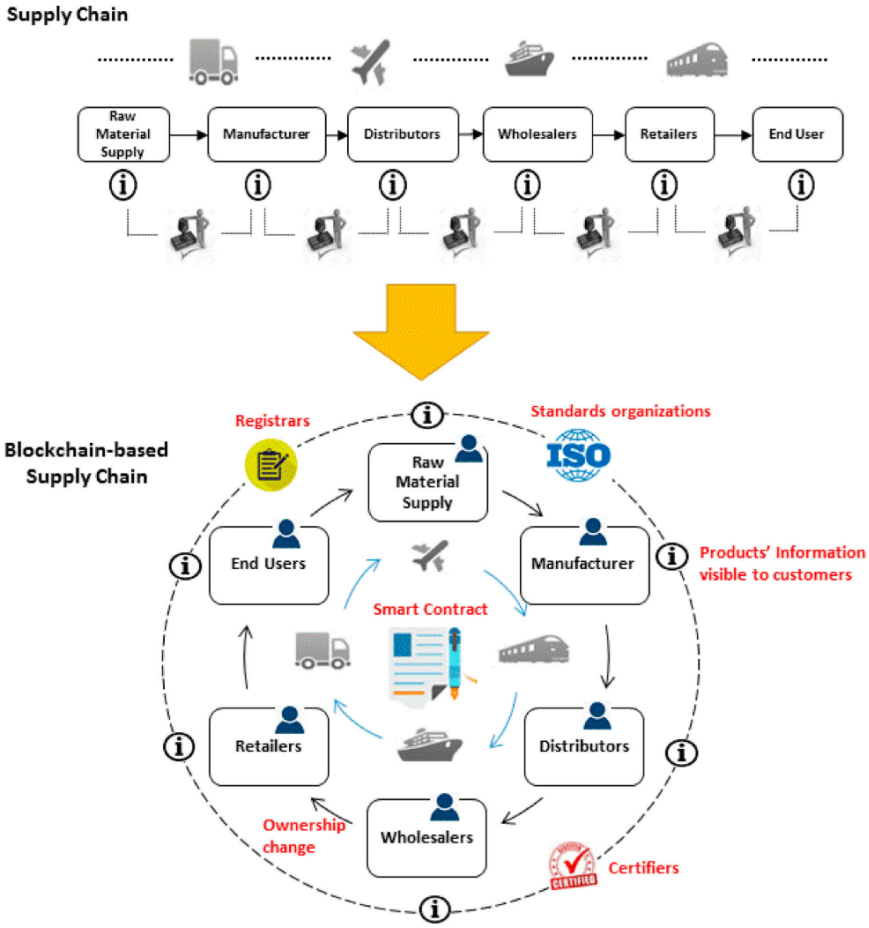


Figure 2: Integrating blockchains in supply chains, taken from [83]

Casino et al. present an extensive literature review of blockchain-based applications [14]. Starting with an analysis of the state-of-the-art, they end up pointing out different research gaps and significant research directions.
Dujak et al. give an overview of possible blockchain applications in supply chains and provide extensive background information [24]. The authors also take a critical look at the integration of blockchain technology and examine possible problems that may arise.
Providing a mathematically proved design for blockchains in supply chains, the authors have shown that the blockchain technology "can help firms reduce order quantities, lower selling prices and reduce the target-inventory levels." [15] They model supply chains and participating parties with mathematical models to analyze the impact of blockchains in supply chain processes.
Petersen et al. divide the range of blockchain applications in supply chain systems into three parts: product tracking, product tracing, and supply chain finance [77]. Their extensive literature review intends to find research gaps and structure the possible application of the blockchain technology in supply chains.

Among other things, research areas for further investigations are analyzed by Kouhizadeh et al. and potentials for blockchain integration in supply chains are shown [56].
A taxonomy for blockchain applications, including a literature review, is done by Labazova et al. [60]. The authors have the aim to guide blockchain application development by linking technical knowledge on blockchains and its application.
Developing a conceptual model for blockchain-based supply chains, Francisco et al. focus on transparency for such systems. They formulate various propositions and indicating variables to characterize trust and transparency in supply chains with blockchain integration [28].
Tribis et al. have done a systematic literature review on papers dealing with blockchain-based supply chains [95]. Figure 3 covers an overview of the number of papers in each category, including main topics.

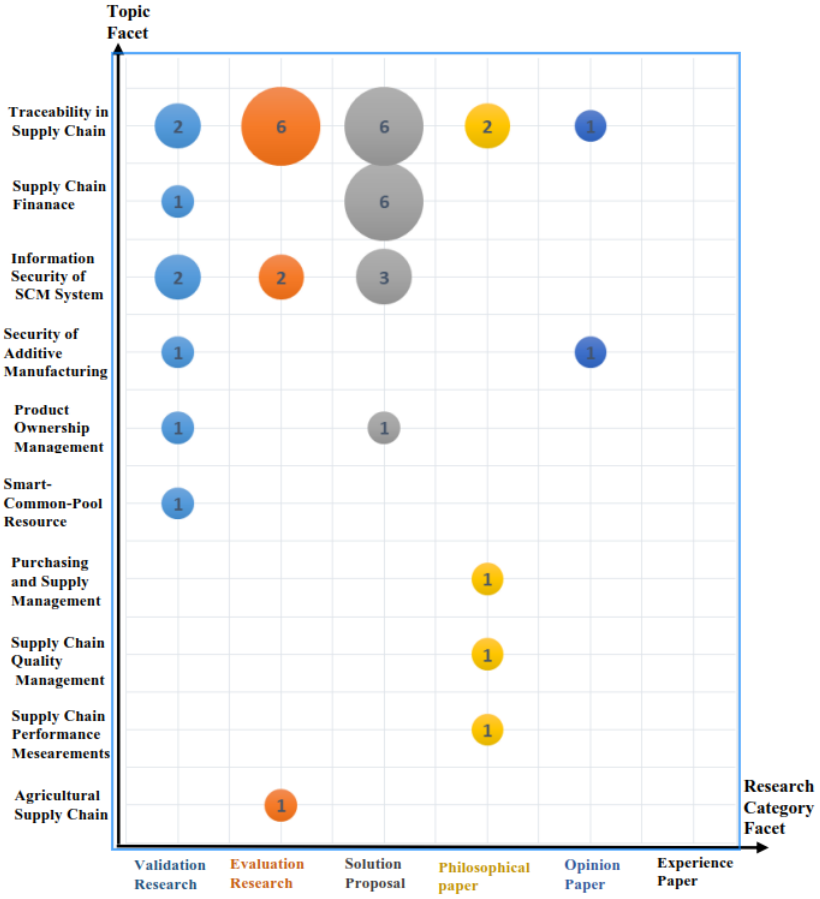


Figure 3: Systematic literature map, taken from [95]

More general and less in-depth papers are published by Kshetri [58] and Jabbari et al. [49]. They both deal with the integration of blockchains in supply chains and the resulting potential for the systems and participating parties. Further, for completeness's sake mentioned, work around blockchains in supply chains is done in [38, 51].

3

METHODOLOGY

Analyzing and comparing the prototype presented in Chapter 4 to other approaches requires a selection of existing or proposed approaches for blockchain-based supply chains. Within this chapter, the selection of these approaches and evaluation criteria for the prototype are presented. Furthermore, guidelines and methods for an expert interview are introduced.
The methodological approach includes the following steps:

1. Identify relevant blockchain-based supply chain approaches and assess their quality.
2. Introduce criteria for the prototype evaluation.
3. Compare and evaluate the relevant approaches with the proposed prototype in Chapter 4.
4. Report the results of the comparison and evaluation.

For the expert interviews, the following steps are considered:

1. Development of a guideline for the interviews.
2. Conducting the interviews.
3. Evaluating the interviews, summarize the results and compare it to the criteria evaluation.

3.1 LOCATING APPROACHES

As the blockchain research area is fairly new, many useless, outdated and non-scientific papers exist. On the contrary, there are systems which integrate the BT and are already in the testing phase. Thus, the preselection is characterized by primitive criteria.
For this work, approaches are examined that have a practical or scientific reference and have, at best, already been implemented.

Casino et al. provide the results of their literature review of blockchain applications in Figure 4. According to the figure, this work is assigned to the *Business and Industry - Supply Chain* cluster. Additional approaches are also extracted from the same cluster.

Figure 4: Mindmap abstraction of the different types of blockchain applications, taken from [14]

Figure 5 shows the distribution of the analyzed blockchain-based supply chain approaches over the past years. The graph clearly shows that there has been a significant increase in research.

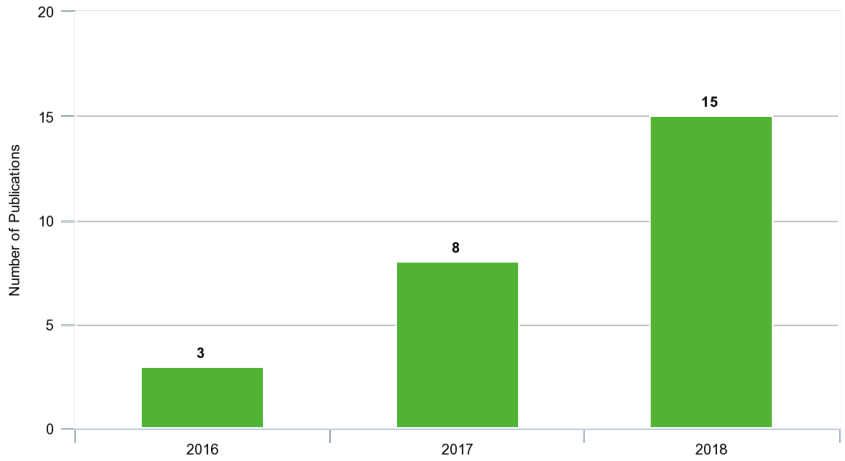


Figure 5: Distribution of publications over the past years

Scientific work and approaches are located by searching on ResearchGate, Google Scholar, and further search engines for scientific literature. If the abstract or the heading contains the keywords "blockchain", "decentralized ledger" or "decentralized", and "supply chain", the papers are continue to be used. Superficial work is no longer considered. Furthermore, the papers have to have a clear scientific contribution and propose an own concept of blockchain integration into supply chains.
Based on the selected approaches, the evaluation will be performed by grouping the system proposals in units of concepts. The comparison will also be based on the division into concepts.
Concepts are defined by the type of tracking items in supply chains, like physical assets or finance. Next, each approach is classified into the defined concepts. The results can be extracted from Table 1, Table 2 and Table 3, where 26 papers are analyzed and grouped together in concepts.

Table 1: Categorization and classification of blockchain-based supply chain approaches (Physical Assets)

	Physical Assets																								
Ref.	*Pharmacy*					*Agri-Food*					*Garments*					*Wood*					*General/Consensus*				
	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E
[2]																						✗	✗	✗	✗
[6]									✗																
[9]	✗	✗	✗																						
[12]						✗	✗	✗		✗															
[27]																✗	✗	✗		✗					
[37]														✗											
[41]																						(✗)		✗	
[53]																					✗	✗			
[59]			✗																						
[71]																					✗	(✗)		(✗)	
[74]																								✗	
[78]																								✗	
[87]																								✗	(✗)
[90]						✗																			

Table 1: Categorization and classification of blockchain-based supply chain approaches (Physical Assets)

	Physical Assets																								
Ref.	*Pharmacy*					*Agri-Food*					*Garments*					*Wood*					*General/Consensus*				
	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E
[91]						✗	(✗)		✗																
[92]																					✗	✗	✗		✗
[103]																								✗	(✗)

Legend: TA (technical/practical approach), I (implemented approach), T (tested approach), THA (theoretical approach), E (evaluated approach)

Table 2: Categorization and classification of blockchain-based supply chain approaches

	Financial					**Governance**					**Business**									
Ref.	*Finance*					*Drugs*					*Price Tracking*					*Agriculture*				
	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E
[45]				✗																
[61]																✗	(✗)			
[64]	✗	✗	✗		✗															
[97]									✗											
[106]											✗	✗	✗							

Legend: TA (technical/practical approach), I (implemented approach), T (tested approach), THA (theoretical approach), E (evaluated approach)

Table 3: Categorization and classification of blockchain-based supply chain approaches (continuation of Table 2)

	Business																			
Ref.	*Postage Stamps*					*Energy Management*					*Textile*					*Wine*				
	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E	TA	I	T	THA	E
[23]									✗											
[25]														✗	✗					
[69]																✗	✗	✗	(✗)	
[105]	✗	✗	✗																	

Legend: TA (technical/practical approach), I (implemented approach), T (tested approach), THA (theoretical approach), E (evaluated approach)

Table 1, Table 2, and Table 3 illustrate that the existing proposals are largely incomplete in terms of implementation, testing, and evaluation. There is a great need here to close these research gaps.
For the analysis and evaluation parts of this thesis, mostly implemented, tested and at least partly evaluated approaches are relevant because the comparisons with the prototype should be as representative as possible. Furthermore, the type of tracking items are decisive for whether the systems are suitable for later analysis and comparison.

3.2 EXPERT INTERVIEWS

At the beginning and in preparation of the actual expert interviews, the development of the interview questions arises [1]. As the interviews are intended to support and extend the evaluation, structured interviews will be conducted. The interview partners should have experience and in-depth knowledge of logistics and/or SCM so that the questions in Appendix B can be answered comprehensively. Furthermore, the interview questions are slightly adapted for the different interview partners because the have different backgrounds. The focus of the subsequent evaluation is mainly set on the topic of trust in supply chains and its role in the prototype. Furthermore, fields for future work can be extracted from the interviews. The interviews were mostly conducted over the phone, as the distances are not acceptable for personal interviews. Guidelines and help for difficulties in phone interviews are summarized in [17].
The eight experts have a university or industrial background. Therefore, the prototype evaluation will be completed and enriched by the interviews.

3.3 COMPARISON AND EVALUATION

The criteria introduced in Chapter 5 can be used directly for the evaluation of the prototype. Furthermore, this enables a common basis for the analysis and evaluation of the prototype and comparable approaches. Taking all criteria into account, a performance measurement system was created that allows us to perform comparisons between existing approaches and the proposed prototype. A comparison between the approaches is necessary for a comprehensive evaluation. The expert interviews complete the evaluation of the prototype. Besides, future research aspects and future work can be detected. Afterwards, the results are summarized in indication parameters for trust enhancement in supply chains and a design for blockchain-based supply chain scalability.

1 https://www.bachelorprint.de/experteninterview/

4

PROTOTYPE

In this chapter, the requirements and the developed prototype are presented. Technical details on structure and design are explained as well as the implemented workflows and processes in the prototype. The prototype is named Bloctrack.

4.1 REQUIREMENTS

In this section, the requirements for the prototype are introduced. As the prototype is developed in order to enhance trust and transparency in supply chain processes while maintaining scalability, it has to fulfill various requirements. In addition, the requirements reflect and address the research questions. The requirements can be divided into back end and front end requirements.

4.1.1 *Back end requirements*

- The back end shall provide an integrity-ensuring storing of data using OriginStamp.
- Using HTLCs, the tracking process itself shall be secure and traceable.
  Description:
  HTLCs shall be used to hold the payments of the customers until the shipment is completed and verified.
- The main data shall be stored off-chain, except the integrity-ensuring data.
- The mapping of products and users shall be unique and secured.
- In every point in time, every tracking process, which was initiated through Bloctrack, shall be traceable and completely verifiable.
- The API access must be secured by an email and password authentication.
- Creating an user account shall require an authentication through a master key.
- The API shall provide easy-to-integrate endpoints.
- The tracking data shall be stored using the JSON data format.

4.1.2 *Front end requirements*

- The front end shall be easily usable.
- The supply chain processes shall be clearly communicated and visualized.
- The tracking shall be possible by scanning the QR code of the item.

4.2 HASHED TIMELOCK CONTRACTS

Hashed Timelock Contracts (HTLCs) are one of the basic concepts used in the prototype. They secure and decentralize the whole payment process by locking the payment with an hashlock and a timelock. Both are useful security mechanisms for the party who creates the HTLC and strengthen the control for the contract creator. Figure 6 presents the concept of HTLCs, which are used in Bloctrack. An HTLC consists of a predefined timelock and a hashlock. As Figure 6, Bob needs the preimage of the HTLC in order to complete the payment. If the timelock expires, Alice can refund the money. This process enables trust optimizations for both parties because Alice keeps the control over her money and Bob can rely on the creditworthiness of Alice. In Listing A.2, the Solidity code used in Bloctrack is added. It is divided into check methods and methods to interact with the Smart Contract.

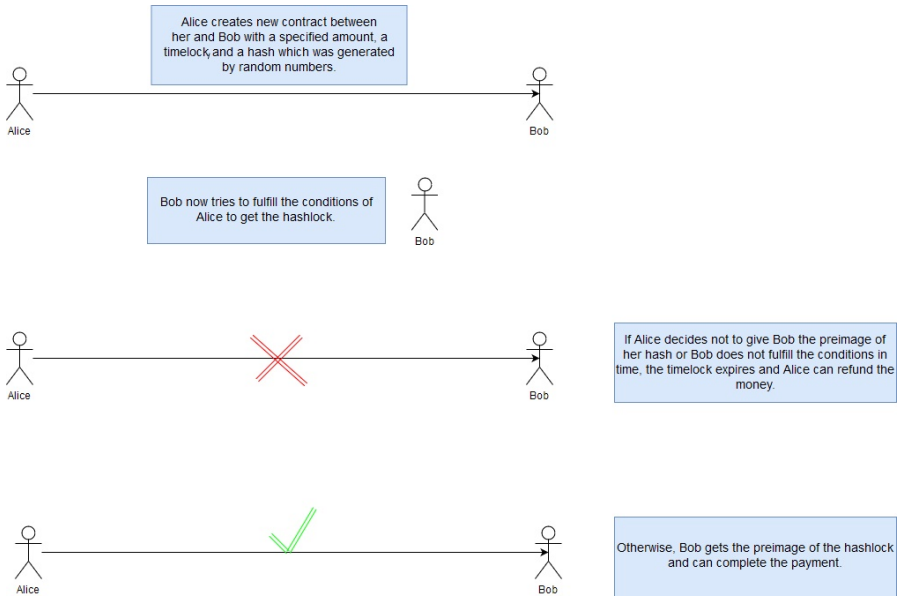


Figure 6: HTLCs in Bloctrack

4.3 STRUCTURE

Next, the technical structure and technologies in the prototype are explained. Furthermore, the system architecture is presented and different layers are introduced.The project of the prototype consists of two major parts, front end and back end. Through the front end, the user can interact with the back end. Bloctrack uses the Ionic framework[1] to create an up-to-date and appealing front end. Ionic is based on Angular[2] which is a front end framework that is built on TypeScript[3]. TypeScript is a superset of JavaScript. Packages are managed and included using the Node Package Manager[4].
Additionally, the actual tracking of data is done by an additional Ionic project which is based on the front end and compiled as an Android application. The app is able to scan a barcode of a tracking item and then specify the individual tracking parameters.

Spring Boot[5] is the framework used for the back end. It provides features like REST calls and creates a stand-alone Spring application.

4.3.1 *Microservices*

The back end consists of the main API and a microservice. The microservice is used for blockchain interactions like creating HTLCs. The methods and services for interaction with the blockchain are outsourced to a microservice. This enables easy adaptions for using other BTs or cryptocurrencies than Ethereum. Furthermore, multichain support can be supported to increase performance.

4.3.2 *System Architecture*

The system architecture of Bloctrack is visualized in Figure 7. The graphic divides the system into layers and their corresponding interactions. The system is designed as a two-party interaction between customer and seller. Additionally, the seller does not directly communicate with Bloctrack. In contrast, the customer only interacts with Bloctrack.

1 https://ionicframework.com/
2 https://angular.io/
3 https://www.typescriptlang.org/
4 https://www.npmjs.com/
5 https://spring.io/projects/spring-boot

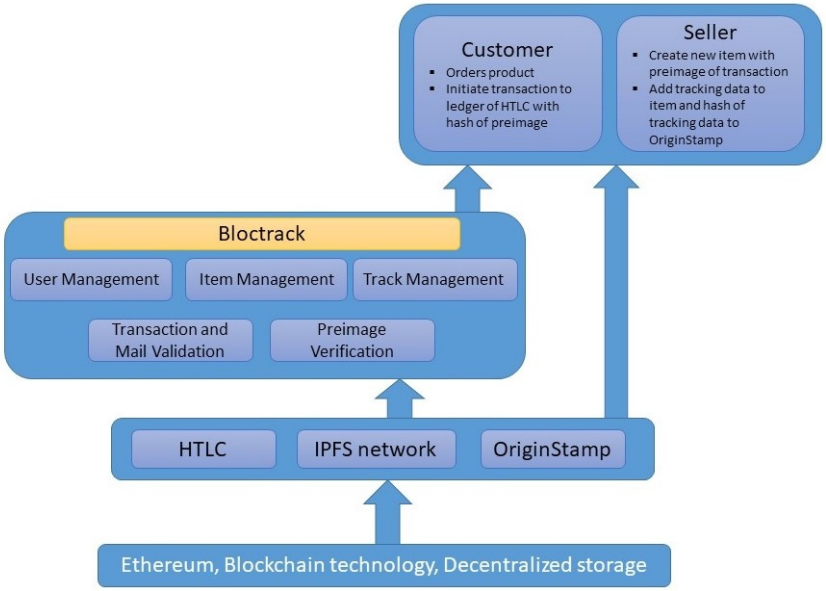


Figure 7: System architecture of Bloctrack

4.4 PROCESSES

Next, the processes and workflows in Bloctrack are introduced. They are very important concerning usability, but also performance of the system. One always has to keep in mind that supply chains are used in the industry and for this purpose, scalability is one of the most critical factors in supply chains.

4.4.1 *Ordering Process*

As shown in Figure 8, the ordering process is initiated by the customer. Further, the validation of the amount of the transaction and the data from the seller is done with Bloctrack. The seller has to include a hash value in the transaction, which is composed of the hash of a customer-specified password and the hash value of the customer's mail address. If the customer always uses another password, no external backtracking is possible, and Bloctrack fulfills the data privacy criterion here. If the seller wants to initiate a new item (new order), the decrypted (hashed) password and mail from the customer's transaction has to be transferred to Bloctrack by the seller. Bloctrack can then easily verify if the information from the seller is valid. Furthermore, a timestamp including the item ID of Bloctrack, the contract ID from the HTLC, and the transaction hash is submitted to OriginStamp for proof purposes and unique mappings. Additionally, an email is sent to the customer including the hashlock of the HTLC, the contract ID, the Smart Contract address, the used transaction hash, the item ID and the timestamp hash.

The preimage of the hashlock of the HTLC is transferred to the customer once a new item is created.

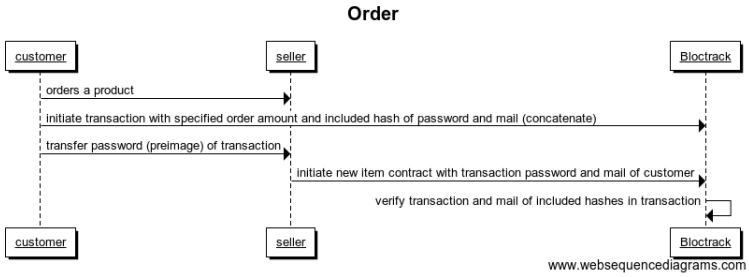


Figure 8: Ordering process in Bloctrack

4.4.2 *Tracking Process*

The sequence diagram in Figure 9 presents the tracking process in Bloctrack. Each hash of a complete track will be submitted to OriginStamp after uploading the data to IPFS. Thus, each track is timestamped. Additionally, each track includes the hash value, the IPFS address and the IPFS encryption password of the previous track. This leads to a "blockchain of tracks", actually a linked list of tracks, and makes it easy to verify the data. As all the necessary information about the previous track is included, it is enough to just own the last track to verify and get all tracking data. Listing A.1 contains the data structure of such a track.

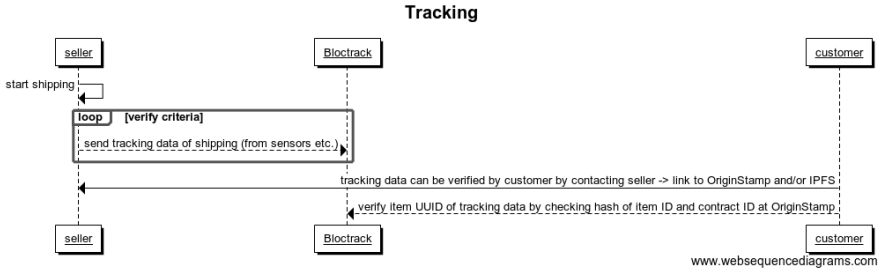


Figure 9: Tracking process in Bloctrack

Through the Android application, which interacts with the API endpoints, the user can add tracking data and specify the tracking parameters. This process can be designed very dynamically and automatically, as the app only needs the item ID of the tracked element and specify the tracking parameter(s) (if tracking is performed via the Bloctrack API).

4.4.3 *Payment Process*

Including HTLCs into payments, the decentralization of the payment process leads to secure conditional payments. The customer only transfers the password (the preimage of the hashlock from the HTLC) to the seller if the tracking data can be verified. In case the customer sends the preimage to the seller, the seller can complete the payment. Otherwise, the payment can be refunded to the customer after the timelock has expired.

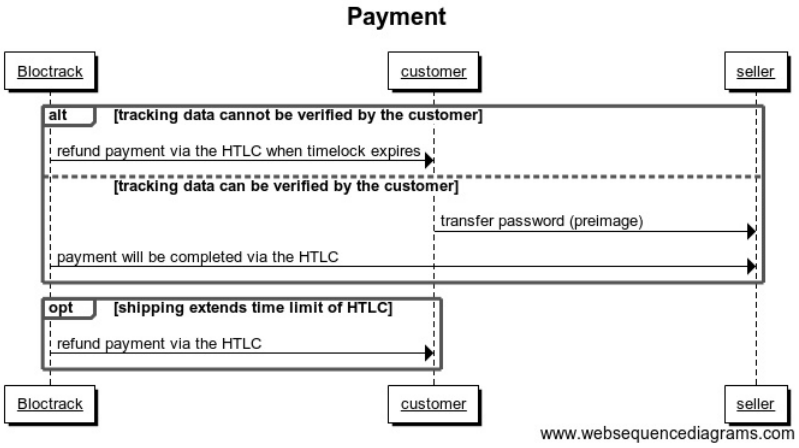


Figure 10: Payment process in Bloctrack

4.4.4 *Overview*

Figure 11 summarizes the processes and parties around the developed prototype. If a line crosses a cloud, like the IPFS cloud, the service in the cloud is essential for the process. This figure also explains which technology is used in a specific step and how the parties interact with each other.

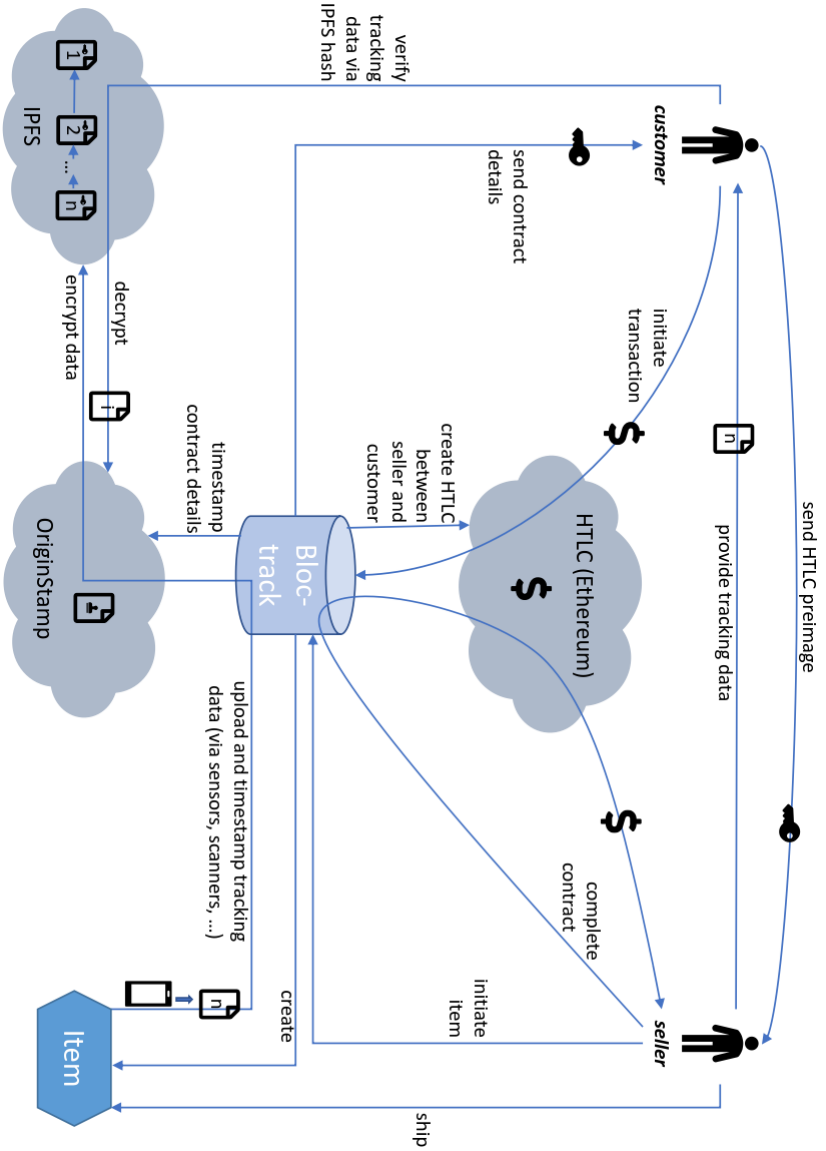


Figure 11: Overview of the prototype

4.4.5 *Verification Process*

As shown in Figure 12, the verification process of the HTLC can entirely be done without Bloctrack. The customer owns all information to verify the payment and the contract, because an email is sent from Bloctrack to the customer including all verification information once a new item is created. In the first step, the contract ID can be verified using the combination of item ID and transaction hash. Using this information, the created contract can be accessed using the contract ID and the public available Smart Contract address of Bloctrack. The publication of the Smart Contract address of Bloctrack (e.g. via email to the customer as implemented in Bloctrack) is a requirement for the verification. In the second step, the tracking data can be checked completely by knowing the IPFS hash and encryption password of the last track.

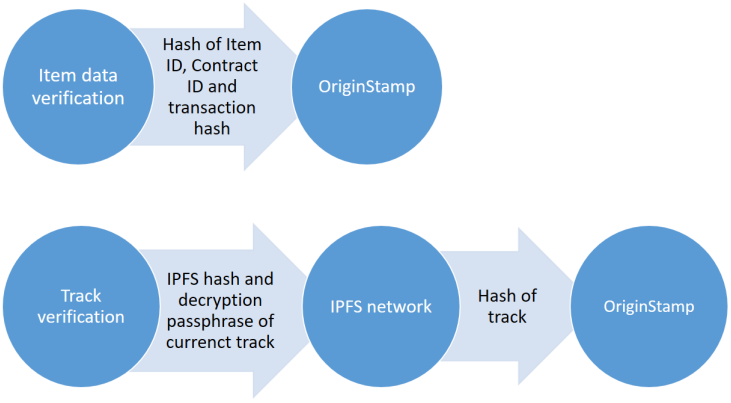


Figure 12: Verification process in Bloctrack

4.5 DESIGN

Within this section, several design decisions are presented. In order to develop an as generalized as possible prototype, only two parties are involved: customer and seller. Starting with a fundamental design decision, Bloctrack is used as a third party verifier. "A verifier is a third party that is trusted to provide some types of information about the external world." [104] In addition, Bloctrack creates the HTLC and acts as a middle ledger or holding ledger between customer and seller. In the problem section, this design element is picked up again. But the injection of manipulated data into the HTLC can be rejected, and further conditions like timelock ranges can be specified, validated and easily adapted. Especially, ambiguities and disagreements between participating parties are avoided because Bloctrack defines the conditions for the HTLC. Additionally, the connection to the Bloctrack API can be easily realized and integrated into existing solutions.

The HTLC is actually a contract between Bloctrack and seller. The customer is able to verify the created contract by the contract ID. If a payment should be refunded, the interaction of Bloctrack is not required. It is necessary to know the Smart Contract address, the HTLC ID and the preimage of the contract, everything known by the customer from the email. Bloctrack assumes that the customer should do less work. Therefore, the front end only provides the function for the seller to complete the payment. Nevertheless, nothing prevents a customer integration into the payment completion. Otherwise, if the seller has the possibility to complete the payment, the balance of power and trust is given. Without this possibility, there would be a clear power imbalance in favor of the customer.

"In a public blockchain, data privacy relies on encryption or cryptographic hashes." [104] The prototype uses both, hashes and data encryption for data privacy. Hashes are mainly used for timestamping reasons, and data encryption is used for the IPFS data storage. The combination of a public blockchain and data encryption ensures a high level of security and reliability because the positive aspects of public blockchains (accessibility, verifiability and high decentralization) are not lost.

Ensuring high flexibility concerning the tracking process, tracking parameters are not predefined and can be added or removed dynamically with each new track. In fact, the whole structure of the track can be modified and adapted in order to ensure applicability to many different use cases. As the tracking process is not connected to the payment process, the tracking could be performed completely without Bloctrack. But the aim of this prototype is to provide a general blockchain-based approach from a single source.

"A common practice for data management in blockchain-based systems is to store raw data off-chain, and to store on-chain just metadata, small critical data, and hashes of the raw data." [104] Raw data in Bloctrack is mainly the encrypted tracking data which is stored in IPFS. Hashes are stored on-chain using OriginStamp. Hash computations and submissions to OriginStamp are completely performed in the front end in order to minimize security lacks. The upload of data to IPFS is currently not possible in the Ionic framework[6] and has to be performed in the back end.

4.5.1 *Database Design*

The Bloctrack database has the following structure:

6 https://github.com/ipfs/js-ipfs/issues/834

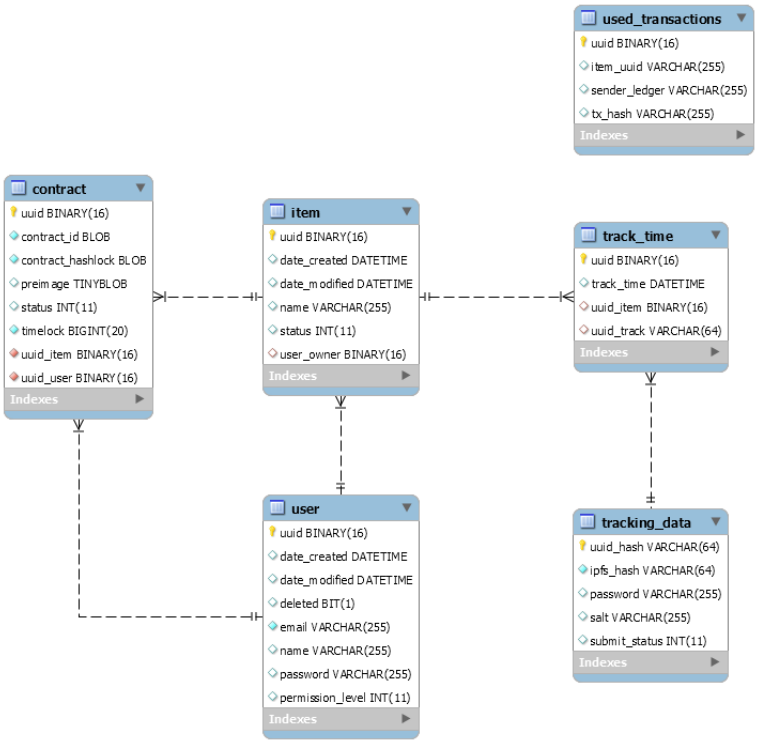


Figure 13: Database EER diagram

4.5.2 *Concepts Integration*

Different concepts are used in the prototype. The following shortly emphasizes the impacts of the used concepts.

Hashed Timelock Contracts in Bloctrack are used for the whole payment process between the customer and seller. They provide high data privacy on the one hand and security and trust for both participating parties on the other hand. Bloctrack as the creator of the contracts just plays the role of the mediator between customer and seller. The actual important data for the contracts are fully known by the customer. Therefore, the usage of HTLCs meets the safety criterion.

IPFS as decentralized storage is used to store the tracks. This storage solves the problem of possible crashes of Bloctrack. If the whole system crashes, the tracks can always be accessed and verified. Thus, this improves the reliability of the system enormously.

5

EVALUATION

Within this chapter, evaluation criteria are introduced and the prototype presented in Chapter 4 is evaluated and compared to other approaches selected in Chapter 3. Additionally, the results of the expert interviews are extracted.

5.1 EVALUATION CRITERIA

In order to answer the research questions, the performance of the prototype proposed in the following section has to be measured. As there exist many implementations and variants of blockchains, the overall performance measurement of the prototype and compared approaches will be based on design criteria for blockchain-based systems. Xu et al. introduce design criteria for blockchain-based applications [104]. The work of them is cited several times and thus is a reliable and proven work and will be used for this thesis [1]. The following summarizes the introduced criteria.
One core concept of these systems is the *immutability* of information to prevent manipulation of the data stored in the blockchain. This also includes how the system ensures or tries to ensure the immutability of the stored information. For a supply chain system and its transparency it is mandatory that the information is tamper-proof. Otherwise, it is not reproducible whether the stored information of a product was faked or changed incorrectly. This criterion also includes the problem of trusted authorities, because it must be guaranteed that only trusted parties can add or change information in a supply chain [71].

The *transparency* of a blockchain-based supply chain system focuses on how the information is available to the public and how closed and self-contained the system itself is. Does the blockchain-based system allow public access, or does it store part of the information privately? As another alternative, partial access to the data, e.g., through encryption could also be a possible solution to achieve transparency. This criterion is important regarding the overall transparency in the supply chain. If the used blockchain system does not support transparent access to the information or at least partial access, this can lead to a security leak and endanger the immutability of the information [50]. This can be the case if a participant can inject manipulated data to the blockchain caused by a lack of transparency. In order to protect

1 https://scholar.google.de/scholar?cites=17022868244333225 39&as_sdt=2005&sciodt=0,5

business secrets, the system should support encryption of the data for example through product-related encryption keys [103].

The *permission management* is mostly realized by a centralized identity management approach and entity-related permissions [71]. Do we have trusted authorities in our system or do we have another authentication process or method? Do some institutions or persons have more access or changing rights than others? This point often brings in the methods used for tracking physical assets, because the system may have a different permission management, e.g., automated tracking versus non-automated tracking [65]. A possible solution can also be a permissionless blockchain [81].

Scalability is one of the main problems of blockchain-based systems like cryptocurrencies [32, 70]. A supply chain system has to store a lot of information, and therefore the scalability of the blockchain is an important factor for the realization and implementation of a supply chain system. Scalability is strongly linked with transparency because the type of blockchain system (centralized vs. decentralized) mostly indicates the scalability factor and transparency. Decentralized systems have no central location or authority in contrast to centralized systems. The most centralized systems have a much higher transaction rate than most decentralized blockchains. The aim of the decentralized blockchains is the reason for a distributed consensus [66].

The *verification* process can be designed differently in blockchain-based systems. Does the system use a third-party institution for verification? A verifier can be, e.g., a Smart Contract or a central authority (CA). The drawback of a centralized verifier such as a CA is the single point of failure. If the verification from the CA fails, neither immutability nor security can be guaranteed. Additionally, *cost efficiency* plays an important role in the applicability to the industry. If the supply chain system is based on a publicly available blockchain like Bitcoin or Ethereum, the transactions which are used to store information in the blockchain, are not free [8]. Additionally, the development and implementation of an own blockchain-based system could be expensive, too. So, a cost analysis is another significant factor to rate the different system proposals.

High latency or an inappropriate consensus protocol can have a huge impact on the overall *performance* of a supply chain system. The performance can be interpreted as the entire workflow of capturing the lifecycle of a product.

Supply chains have wide-ranging use cases [9, 59, 91]. Therefore, the *flexibility* of a proposed supply chain system has to be also considered to rate the whole approach. As an example, Smart Contracts as an on-chain verification process are not flexible at all. A Smart Contract runs on the blockchain, possibly no changes can be made, and the contract cannot be stopped. [11] The applicability of the approach to other areas of supply chains is also an important factor.

Another challenge for blockchain-based supply chains is *computation*. The computational effort for transactions is either performed on-chain or off-chain. Default Bitcoin transactions are completed on-chain, whereby the Lightning Network [80] performs transactions off-chain. Ethereum's Smart Contracts can be partly executed off-chain [7, 11, 70]. Computation is also connected to the performance, because on-chain computation normally slows down the performance of the system [7].

The choice of the *consensus protocol* can influence the scalability, performance, and immutability of the data. Consensus-making in blockchains is a critical design decision concerning security and scalability. If the consensus protocol does not ensure a secure way of adding a block to the chain, the security cannot be guaranteed. But if the consensus protocol requires too much time to prove the changes made to the blockchain, there is a lack of performance and scalability [7, 11].

5.1.1 *Further Criteria of Supply Chain Systems*

Supply chain systems must also meet other challenges. Thus, some further criteria are introduced for the comparison of the systems: Considering Physical Unclonable Functions as digital fingerprints [44], the integration into the physical world also plays an important role in supply chain systems. As an example, RFID (Radio Frequency Identification) is a widespread technology which can identify objects via a radio frequency. Therefore, RFID is predestined for automatic product identification. It is a highly reliable technology and, consequently, offers many possibilities for supply chains. RFID increases the security in comparison to simple barcodes which can easily be manipulated [92]. But the technology itself does not ensure a good integration into the whole system. There must be high-secured interfaces between the system and the product, such as Physical Unclonable Functions (PUFs) [41]. Otherwise, sabotage cannot effectively be prevented [52]. For the overall transparency, the *transparency of the tracking process* must be especially considered for supply chains. The tracking process itself should be traceable and transparent. Otherwise, the correctness of the information stored in the blockchain cannot be proven. This criterion can be measured by evaluating the tracking process and security with respect to the workflow how information is added or updated in the blockchain [1, 50, 59].
Furthermore, the topic of lean and agile supply chain systems gains more and more importance. Lean supply chain systems focus on the necessary and essential tasks and parts of supply chain systems [18]. "Agility is concerned primarily with responsiveness. It is about the ability to match supply and demand in turbulent and unpredictable markets. In essence, it is about being demand-driven rather than

forecast-driven." [18] Lean and agile systems are both criteria that directly influence other aspects like scalability.

5.2 PROTOTYPE EVALUATION

Next, the prototype itself is evaluated. The structure of the evaluation is based on the criteria introduced above.

Immutable information. Bloctrack fulfills the challenge to ensure the immutability of the information. During the tracking process, the largest amount of data is produced. Through the linking of the single tracks with the previous hashes and the decentralized storage, a high immutability standard is already existing. Additionally, timestamps with OriginStamp secure the immutability of the tracking data. Thus, data immutability is ensured during the tracking process. Supposed someone tries to inject distorted tracks, the hash value verification will fail consequently. If the customer owns the last track hash and encryption password, the verification and data correctness of each track can be performed by the customer.
Considering the ordering process of Bloctrack, the relevant data is stored in the Smart Contract. Once created, a Smart Contract supports the same security level concerning immutability as the underlying blockchain system. In general, this paper assumes that large and popular cryptocurrencies such as Ethereum are protected against 51% attacks. Therefore, the ordering process in Bloctrack ensures data immutability. In addition, a timestamp of the contract address and additional information is submitted to prove the unique mapping between the contract and the used transaction of the customer.
During the payment process, no mutable data is generated. Therefore, Bloctrack ensures data immutability for each subsector.

Transparency. Transparency as a key feature of supply chain systems is one of the focal points of this work [65]. In Bloctrack, transparency is implemented on several levels. At the *tracking level*, the decentralized storage with IPFS and the timestamps of the tracks enable a transparent tracking process. The submitted timestamps and the tracking data are accessible, verifiable, and traceable from all over the world. The linked list of tracks enables an easy and transparent access to the data. Furthermore, business secrets are preserved by track encryption and transparency is guaranteed.
It is also important to ensure transparency during the ordering process. In Bloctrack, the ordering process is quite complex for easy transparency. In order to solve the double spending problem, the created timestamp can be used to validate if the transaction of the customer has already been used. Otherwise, it could be possible that a seller declares the same customer transaction twice. This would not lead to

problems for the customer but for Bloctrack, because the funds for the HTLC is taken from the account of Bloctrack.
Since the payment process is completely handled via the HTLC and can be verified by both customer and seller, this leads to a high level of transparency. The complete decentralization of the payment process also creates a high degree of transparency. Accordingly, transparency is given on the different levels in Bloctrack. The comparison in Section 5.4 completes the transparency analysis and allows further conclusions.

Permissions. Bloctrack is a user-related application. Sellers are registered as users and registration can only be performed by Bloctrack and not by sellers. Therefore, Bloctrack supports access rights for customers, and automatic registrations are not permitted. This limitation can also be seen as a feature because it increases security for access rights and prevents the creation of fake accounts. Access rights for the tracking data are controlled by the encryption passphrase. Those persons or institutions who know the encryption key of the latest track can decrypt it and gain access to the whole track chain. Assuming a two-party supply chain system, this would not cause any problems because the customer should have access to the tracking data.
The HTLC can only be accessed if the exact ID is known. Therefore, mainly the customer and the seller have access to the contract details.

Scalability. As stated above, scalability is one of the main challenges for cryptocurrencies and blockchain applications in general. Except for private and federated blockchains, storing any data in a blockchain leads to performance lacks [2]. In order to perform a comprehensive scalability analysis, each process in Bloctrack and corresponding technologies are evaluated. The ordering process starts with the customer's transaction to Bloctrack. Next, the seller has to create an item in Bloctrack and a new HTLC will be created. Considering this workflow, some bottlenecks could occur. The customer's transaction causes a bottleneck concerning the mining delay of Ethereum. Compared to the current bank transfer time of one to two hours for fast transfers in Germany [3], the mining time is almost negligible. Furthermore, the time for creating an item, respectively creating an HTLC, is based on the duration of the mining. Thus, scalability in the ordering process is given but can be improved.
Scalability performance in the tracking process mainly depends on the local IPFS node configurations respectively accessibility and workload of the node [5]. Thus, the upload to an IPFS node of such small data can be performed nearly in real-time. Timestamping with Ori-

2 https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
3 https://www.sparkasse.de/geld-leichter-verstehen/w/wie-lange-dauern-uberweisungen-deutschland.html

ginStamp also does not cause delays. Therefore, the tracking process is highly scalable.
Lastly, the payment process includes the created HTLC twice. First, the preimage of the hashlock has to be transferred to the contract and verified. Then, the payment has to be completed which depends on the transaction confirmation time of the underlying cryptocurrency. Scalability is also given for the payment process but can be improved.

Verification. Verification has a very high priority for this prototype since the decentralization of the prototype also includes the decentralization of verification. As stated in Chapter 4, the verification of the processes can be done without Bloctrack. Additionally, the timestamp verifications can also be computed without OriginStamp. Further verification mechanisms in Bloctrack are not necessary. Therefore, there is no need for central authorities and the implementation is completely decentralized.

Cost efficiency. Using public blockchains like cryptocurrencies is mostly accompanied by high costs for transactions. Apart from the costs of the blockchain fees, there is no need to expand the technical infrastructure of customers or sellers. Only the IPFS node has to be hosted, or costs for access to a publicly available node will arise. The usage of Ethereum does not cause high costs because the Smart Contract has to be called twice in the best and regular case (creation of the HTLC and completion of the payment) [4]. If Bloctrack had been realized using a private blockchain, the server infrastructure would have had to be established first. This would entail high costs.
Generally, Bloctrack is not a cost-intensive system and has nearly no maintenance costs except the IPFS node.

Performance. Performance of the overall workflow must be considered at different levels. From the customer's point of view, it is just necessary to calculate the hash value of the password and the hash value of the email address. Furthermore, only the transaction to Bloctrack is required and the transfer of the password and email address to the seller. Otherwise, from the customer's point of view, the workflow is simple and easy to manage, even so, the customer wants to validate the tracking data.
At the seller's level, the password and email address from the customer has to be transferred to Bloctrack. Finally, the seller has to complete the payment with the preimage of the hashlock of the HTLC. It gets a little more complicated if the customer wants to track data without using the Bloctrack API, because the previous IPFS hash, the previous track hash value, and the decryption password of the last

4 https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214

track has to be stored and included in the latest track. This makes the workflow more difficult for the seller.
Considering the workflow of Bloctrack, most work has to be done by Bloctrack. Bloctrack operates as the mediator between the parties in the supply chain and the blockchain and thus implements the more difficult workflow to interact with the HTLC and IPFS. But this leads to the fact that the workflow for sellers and customers are almost as simple as without a blockchain system.
In summary, it can be said that the workflow for sellers and customers are comprehensible and lead to good performance.

Flexibility. Flexibility as an important criterion for general supply chain systems is mainly realized with the flexible tracking data. Not only the tracking parameters can be customized, but also the whole track structure can be adapted at will. Furthermore, the concept of HTLC can be mapped to any cryptocurrency which supports Smart Contracts. This enables high flexibility concerning the concepts used in Bloctrack. IPFS as decentralized storage should not be replaced by any centralized storage management, because then the advantages of the decentralization would be lost.
Additionally, the Android app for the tracking process can be replaced by any other device which can interact with Bloctrack to add tracking elements. Later in Chapter 6, the tracking process without Bloctrack is also discussed.

Computation. The computational effort mainly depends on the usage of the HTLC. Certainly, the transaction time of the customer's transaction has to be considered as well, but the actual payment process is done within the HTLC. As the HTLC has to be called only twice, the computation effort of the whole system is low. Creating the timestamps with OriginStamp does not lead to any computational effort for Bloctrack. Third-party systems like OriginStamp are no longer taken into account for computation analysis because it does not affect the computational effort for the Bloctrack prototype.

Consensus protocol. The choice of the consensus protocol used for the HTLCs, the transactions, and timestamps affects the performance, costs, and scalability of the system enormously. Transaction confirmation time, Smart Contract access, and transaction costs vary depending on the consensus protocol of the cryptocurrency. As Bloctrack is based on Ethereum, transaction costs and time for computations are fairly low because of PoW and PoS as used in Ethereum [5].

Integration into the physical world. This prototype does not stipulate how to identify products. For testing purposes, QR codes are

5 https://etherscan.io/charts

used to track packages. Any other method can be used for product identification. Further usages of physical devices or techniques are not integrated.

5.2.1 *Workflow Issues*

From the presented workflows it is obvious that problems can occur. During the payment process, the following scenario is possible: the customer initiates the transaction to the Bloctrack account. If Bloctrack now crashes, there are no guarantees that the payment can be refunded.
Figure 14 illustrates the issue and the optional refund of Bloctrack.

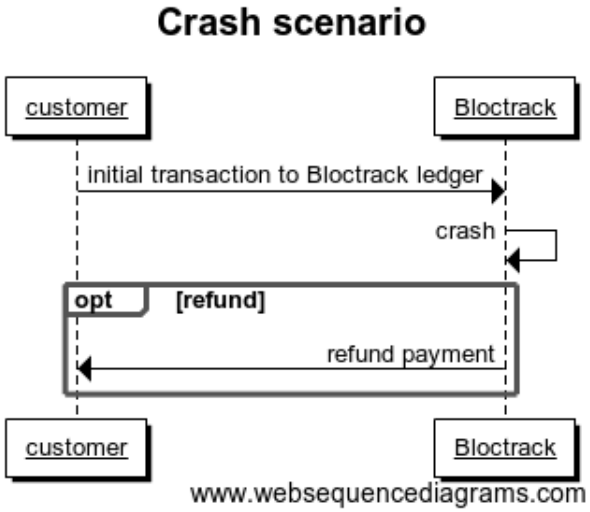


Figure 14: Possible crash scenario

There are several solutions to prevent this: first, a payment contract between Bloctrack and the customer could lead to more security. Secondly, the Bloctrack account can be accessible by governmental institutions for such cases. Then the independence and autonomy of the system are more restricted, but it also represents a trade-off between dependency and autonomy, which would be possible, since only an unlikely case would be legally protected.

In order to avoid complications in the tracking process, the seller should always store the information about the latest track (IPFS address and decryption passphrase). Additionally, the tracking process can be completely performed without Bloctrack, see Chapter 6.

5.3 EXISTING APPROACHES

As the prototype is designed to track physical assets, it can be classified in the "General" Physical Assets cluster in Table 1. Thus, approaches for the comparison are also taken from this cluster. Enrich-

ing the comparison, both technical and theoretical approaches are taken. Specifically, these are the following (including abbreviations): ACSC [2], PSC [9], AgriBlockIoT [12], EOS [27], and POMS [92]. Next, the different approaches are shortly presented.

Alzahrani et al. propose a new consensus protocol for supply chains. *ACSC* builds an own blockchain per product and stores all related information and tracking data in the blockchain. Each participant in the product's supply chain is a node in the network. Furthermore, a new block structure for the blockchain is introduced where all relevant information like validator signatures are stored. For the actual product tracking, NFC tags are used which are initialized by the manufacturer.

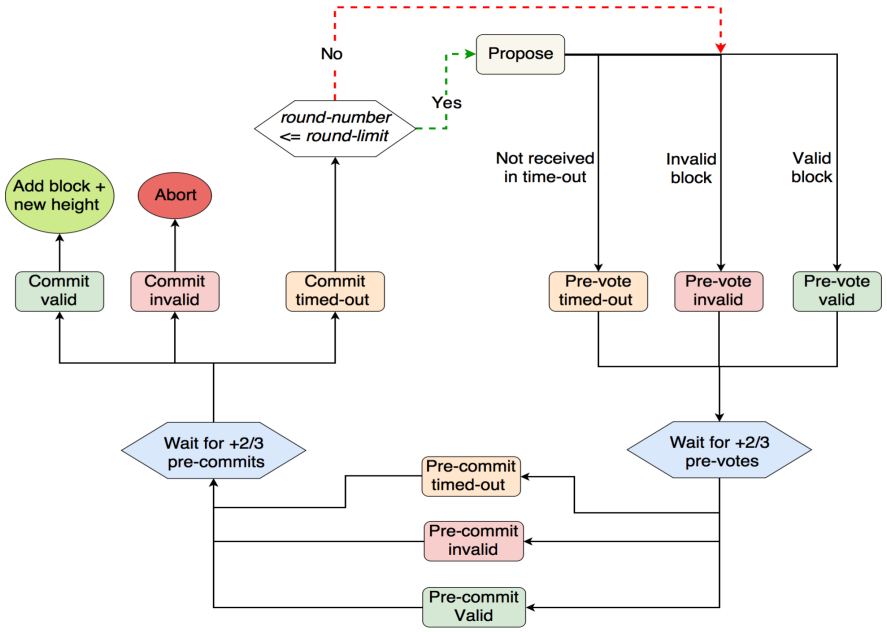


Figure 15: Consensus protocol of ACSC, taken from [2]

Starting with the "Propose"-step, Figure 15 presents how the consensus protocol works. It is based on Tendermint, but selects validators randomly on each block proposal. In their evaluation, the new protocol offers higher scalability and performance than Tendermint and keeps security [2].

A use case of supply chain systems with pharmaceutical products (*PSC*) is proposed by Bocek et al. [9]. Modum.io AG[6] is a startup from Switzerland which integrates the blockchain technology into the pharma supply chain. The paper presents an already implemented supply chain prototype which is designed for pharmaceutical products. Each pharmaceutical product has a unique serial number and

6 https://modum.io/

an appropriate QR code. The main purpose of the blockchain integration is to safely check whether the needed temperature for the product is kept during product transportation. Thus, the workflow of transportation is organized with Bluetooth sensors. Each QR code of the product is scanned, and a sensor's barcode is assigned to the serial number of the product or a package of products at the beginning of the packaging and initialization. Further, a Smart Contract on the Ethereum blockchain is generated with a specific identifier. During the delivery process, the temperature is measured and uploaded to a server, added to a database and validated with the Smart Contract running on the Ethereum blockchain. Then a report is created out of the Smart Contract which is sent to all included instances in the supply chain. Additionally, the system offers an offline feature which synchronizes the data with the blockchain as soon as a stable connection is available [9].

Concentrating on food, *AgriBlockIoT* is a blockchain-integrated prototype which uses Smart Contracts to automate verification processes. The authors suggest the usage of smart-tags like barcodes and sensors. They do not explicitly state how to use these technologies. Figure 16 shows the system architecture of AgriBlockIoT. It is divided into different layers to emphasize how BT is integrated into the system.

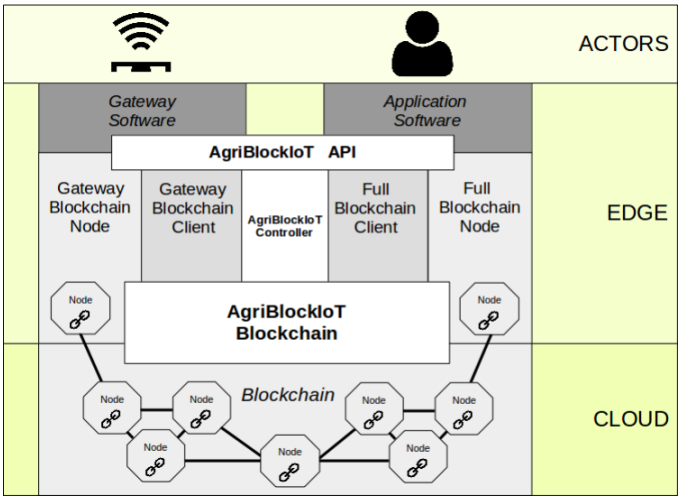


Figure 16: Layered system architecture of AgriBlockIoT, taken from [12]

Tracking and digital content are completely stored on-chain. Therefore, Hyperledger Sawtooth [7] as an enterprise blockchain solution is used as the underlying BT in AgriBlockIoT. Not surprisingly, Sawtooth outperforms Ethereum because of another consensus protocol [8]. But the authors also say that the choice of the blockchain system de-

7 https://sawtooth.hyperledger.org/
8 https://sawtooth.hyperledger.org/faq/consensus/

pends on many other aspects like possible integration into other systems.

Figorilli et al. make use of an Android app in their prototype (*EOS*). For their blockchain-based application, they use the Azure Blockchain Workbench [9], which is a framework of Microsoft to implement, design, and deploy blockchain-based applications. Figure 17 presents the implemented workflow in EOS "from standing tree to final user" [27]. As tracking technology of the wood, RFID tags, NFC, QR codes and barcodes are used, depending on the circumstances in each step of the wood supply chain. Furthermore, as shown in Figure 17, the blockchain technology (here Ethereum) is used to secure specific steps in the supply chain (timber mark hammered, cutting) [27].

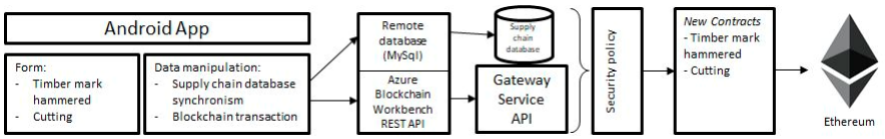


Figure 17: Interconnection diagram of prototype, taken from [27]

"An app (SmartTree) for the wood traceability data collection has been developed to support the in-field operation from the timber marking to cutting phases, providing operators with a simple and easy-to-use tool for smartphones."[27] This is very similar to Bloctrack, as both use mobile applications in at least some parts of the tracking.

POMS is designed to recognize counterfeits in the supply chain. Therefore, POMS stores product-related information like "shipped" and "received" in the blockchain. In a nutshell, POMS maps ownership and shipments of products to Smart Contracts which are deployed to the Ethereum blockchain.
Figure 18 summarizes the processes in the supply chain and the interactions with the Ethereum blockchain. It also shows the involved parties in the system. The tracking process (tracking data of products during the shipment) is completely ignored in this approach. POMS focuses on the detection of counterfeit products [92].

9 https://azure.microsoft.com/de-de/features/blockchain-workbench/

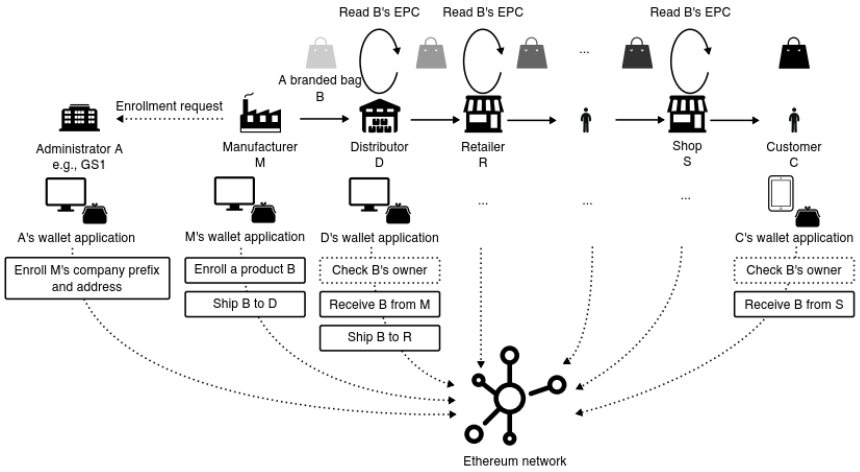


Figure 18: Interconnection diagram of prototype, taken from [92]

In their evaluation, the authors name open problems, costs and the performance of the prototype. The authors conclude that tracking a product with less or equal six owner transfers causes costs less than US$1 in POMS.

5.4 COMPARISON

Within this section, a comparative evaluation of the presented approaches with Bloctrack will be carried out.

5.4.1 *Evaluation of existing approaches*

In order to perform a comparison with Bloctrack, the existing systems are first evaluated using the criteria introduced in Section 5.1.

Immutable information. Starting with the ACSC approach, all relevant product information is stored in the blockchain, including tracking data. Furthermore, the proposed consensus protocol offers high reliability in detecting malicious nodes. This also depends on the number of nodes in the network and the number of validator nodes. Validators are nodes which are selected by the validation leader node to validate the current block. This means that ACSC is designed to reach scalability without losing fundamental features of blockchains [2]. As we assume that networks in supply chains are large, the data immutability is given in this approach. The temperature measurements and the upload in the PSC system are totally automated. The data is not stored in a blockchain; the blockchain is just the controlling instance that the temperature is not lower or higher than a given range. But the immutability of the stored information is not validated with a blockchain, and therefore PSC does not have a higher level of security against data manipulation than systems without a

blockchain integration. It is only guaranteed that the stored temperature fulfills the Smart Contract, but it is never validated if the stored measurements are modified. Therefore, additional security measures must be included like storing some verification data on the blockchain [96]. For Hyperledger Sawtooth as the technology proposed in AgriBlockIoT, the same assumption as for ACSC can be made: the size of the network is large enough that the consensus protocol works. As content is completely stored on-chain, data immutability is totally given. Data immutability in POMS has to be reduced to the product-related data which is stored in the blockchain. Tracking data is not relevant. Thus, POMS guarantees data immutability. Securing specific steps with Smart Contracts, EOS provides immutability at least for parts of the data. Further tracking data in other steps are just stored in a database. The authors introduce a security policy in order to secure important steps using Smart Contracts. Thus, data immutability is only partly guaranteed because database entries can be manipulated easily. Focusing on detecting counterfeit products, data to detect such products is stored in Smart Contracts. Therefore, the immutability of relevant data is given.

Transparency. Transparency in ACSC is mainly reduced to the consensus protocol. As immutability is given in large networks, transparency can also be presumed. The workflow, depicted in the consensus protocol, and its structure suggests that a network of blockchain nodes contains transparency in supply chains. However, further information on tracking is missing for a comprehensive analysis of transparency. The customer who buys the product can also request the report from the Smart Contract from the server of the PSC system. Furthermore, the rest of the tracking process is automated and traceable. Hence, the customer gets the relevant information in a very transparent way, and the transparency is comparatively high [1]. AgriBlockIoT stores the data in a private blockchain where only participants of the network can access the data. Assuming the network of participants in the supply chain is large, and the data can be accessed and verified by many participants including customers, transparency is also guaranteed in this system proposal. Smart Contracts further improve transparency. Essential steps in the supply chain can be reproduced and verified with Smart Contracts in EOS. The accessibility, traceability, and transparency for the rest of the data are not improved compared to conventional SCM systems. Therefore, transparency is at most partly given including cutting and hammered timber marks. In contrast to EOS, the target setting of POMS is clearly defined, and for detecting counterfeit products, transparent storage, and verifiability of the data are wholly existing.

Permissions. ACSC limits permission by modeling each node in the blockchain as a supply chain participant. Thus, access rights can be mainly managed by blockchain access, and data encryption and permission management are limited. PSC supports access rights as the customer can request the report and the tracking process can be fully automated. It also provides access rights to their server. Therefore, the quality level of permissions is quite high. Similar to ACSC, access rights in AgriBlockIoT can be managed through blockchain access and data encryption. Permissions in EOS can be mainly granted by giving access to the data in the local database. Smart Contracts, which are used for specific steps, are publicly accessible. Thus, EOS provides good permission management for data which is stored in Smart Contracts but not for data which is stored in the local database. POMS can handle permissions by access limitations to the data which is stored in Smart Contracts. This leads to transparent and efficient permission management.

Scalability. On-chain system solutions mostly suffer from scalability issues, especially if public blockchains are used [26, 34, 79]. ACSC overcomes this problem by proposing a scalability-improved consensus protocol. It is introduced for complete on-chain storage. In large networks with high throughput, this could lead to latency anyway. As Smart Contracts are used to store verification data, PSC cannot ensure high scalability but keeps a sufficient level of scalability for current use cases. Identical results for scalability can be observed in EOS, where Smart Contracts are mainly used for verification purposes. Using a private blockchain, AgriBlockIoT is not affected by scalability issues of on-chain storage. In contrast, POMS can get scalability issues if product-related data gets very large. Thus, scalability is not ensured in POMS.

Verification. Verification of data which is stored in the blockchain or off-chain should be verifiable and validatable [50, 104]. In ACSC, POMS, and AgriBlockIoT, data verification can be performed fully on-chain. Different in EOS, where only parts of the data are verifiable. On the one hand, as the Ethereum blockchain is used for Smart Contracts, the verification of the data itself is not implemented in PSC. This can lead to problems if the system gets compromised. On the other hand, without storing the data on a blockchain, there is no problem of high latency. Smart Contracts only verify the data coming from the database on the server. If we assume that this data is correct, the verification process is partly realized through the Smart Contracts [50].

Cost efficiency. Storing all the data on-chain typically causes high costs. Additionally, establishing a new blockchain network for sup-

ply chains is also associated with high costs (server infrastructure, development, maintenance). This also applies to ACSC, as a private network has to be established first. The same issue occurs in AgriBlockIoT. Therefore, both approaches cause high costs. Uploading of a Smart Contract to the blockchain in the PSC system is nearly the same as the fees for a transaction, but it depends on how often the contract is called [82]. The advantage in comparison to ACSC and AgriBlockIoT is that it is possible to upload many measurements at a time and therefore not that many requests reach the Smart Contract. Further, only one Smart Contract has to be initialized for one shipment. This reduces the costs enormously in comparison to the ACSC and the AgriBlockIoT systems. The Bluetooth senders used for the temperature measurements only have to be bought once. As a conclusion, PSC is a comparatively cost-efficient system. EOS mostly gets rid of on-chain storage costs but RFID and NFC tags are both relatively expensive [10]. Apart from that, EOS is also a cost-efficient system. In contrast to EOS, POMS is an on-chain storage based system approach and thus is a cost-intensive approach. In comparison to ACSC and AgriBlockIoT, no tracking data has to be stored, and the amount of data is not that large than in ACSC and AgriBlockIoT.

Performance. The performance of the ACSC approach is improved compared to on-chain storage systems that are based on Tendermint. Nevertheless, storing the data could lead to high latency. Consequently, the performance could be decreased. This is similar to AgriBlockIoT, where the BT could be a bottleneck for the overall performance. Hard forks of the Ethereum blockchain can lead to a lack of performance in PSC, EOS, and POMS, which, nevertheless, should not be the usual case. Uploading and running a Smart Contract should never decrease the performance of the system. There are no factors which decrease the overall performance of the system. Problems with the Internet connection in PSC are solved with the offline feature and the synchronization after the offline phase. Accordingly, this challenge do not lead to a performance lack [92, 103]. Further bottlenecks do not exist in EOS and POMS.

Flexibility. Concerning flexibility, ACSC and POMS do not have any product limitations and can be adapted to any use case in supply chains. The PSC system is flexible concerning the applications and the workflow. The applications running, for example, on mobile devices, are highly customizable. Nevertheless, the overall structure and design of the system should remain the same. In general, PSC is only applicable to pharmaceutical products. Adapting it to other use cases should be possible in the future [9, 59]. The AgriBlockIoT approach is specialized and limited to agriculture. Regardless, the approach can

10 https://www.ginstr.com/en/3-key-facts-about-rfid-and-nfc-technology/

also be mapped to other use cases as the single steps and the system design does not limit the use cases. This is different in EOS, where the approach is clearly limited to the wood supply chain. Single steps and the overall design is tailored to this special use case. In order to generalize the system, some parts like the security policy have to be adapted and generalized. Furthermore, other parts like the interaction with the blockchain can be maintained.

Computation. One of the main goals of ACSC is to decrease the computational effort. In comparison to the Tendermint protocol, the decrease is successful. But concerning the amount of data that should be stored in the blockchain, the computational effort is high, as well as in AgriBlockIoT with Sawtooth. In the future, Ethereum will migrate to the Casper protocol and finally introduce Proof-of-Stake, which reduces the computational effort [7]. The other parts of the PSC system do not require many computational resources. EOS does not need high computational effort, because the amount of information that is stored in the blockchain is low. Storing all data in the blockchain, POMS causes high computational effort.

Consensus protocol. ACSC itself is a proposed consensus protocol. In PSC, a consensus protocol is not necessarily needed as the data is not stored in a blockchain. The consensus protocol of Ethereum does not affect the usability of Smart Contracts. Hyperledger Sawtooth in AgriBlockIoT supports different consensus protocols which are mostly designed for private blockchain applications [11]. EOS and POMS are both based on Ethereum and therefore will use PoS in the future.

Integration into the physical world. AgriBlockIoT proposes the usage of tags like RFID tags and barcodes. EOS extends the usage of tags to NFC and QR codes. Thus, both system approaches are integrated into the physical world. In contrast, POMS does not have any suggested integration and ACSC proposes the usage of NFC tags. The usage of Bluetooth sensors, QR codes, and barcodes in combination with the mobile devices in PSC is proof of a high integration into the physical world. As the system is tested as a pilot project, the Modum.io AG has made first experiences and improvements with it [9].

5.4.2 *Comparison to Prototype*

Table 4 sums up the result of the evaluation of Bloctrack and the other evaluated approaches.

11 https://sawtooth.hyperledger.org/faq/consensus/

Table 4: Comparison of approaches

	Bloctrack	ACSC [2]	PSC [9]	AgriBlockIoT [12]	EOS [27]	POMS [92]
Immutable information [1, 103]	+	+	-	+	-	+
Transparency [1, 103]	+	o	o	o	-	+
Permissions [1, 103]	+	o	+	o	-	+
Scalability [103]	o	(+)	o	+	o	-
Verification [103]	+	+	-	+	-	+
Cost efficiency [59, 103]	+	-	+	-	+	-
Performance [103]	+	o	o	o	o	o
Flexibility [103]	+	+	o	o	-	+
Computation [103]	+	o	+	o	+	-
Consensus [103]	PoW [70]		PoW [70]	- not fixed - [75]	PoW [70]	PoW [70]
Ledger [50, 59]	Ethereum [11]		Ethereum [11]	Hyperledger Sawtooth	Ethereum [11]	Ethereum [11]
Tracking Feature [1]	QR codes	NFC	Bluetooth, barcodes, QR codes	smart-tags	RFID, barcodes, QR codes, NFC	
Ledger Technology [1]	Decentralized [103]	Decentralized [103]	Hybrid: Decentralized [103] Centralized Item Data [103]	Decentralized [103]	Decentralized [103]	Decentralized [103]

The matrix shows the similarities and differences between the compared approaches and classifies them according to the following characteristics: “+”: well-designed, “o”: can be improved, “-“: should be improved

PSC and EOS are both approaches that are already tested in a real-world environment. Table 4 illustrates that most of the existing approaches have severe weaknesses. Causing high costs, EOS and POMS are both approaches which will likely not be used in the industry. Furthermore, it is also obvious that Bloctrack performs much better than the other system proposals. PSC and EOS are both limited to specific use cases because their design is aimed at business areas. In comparison, Bloctrack is designed for general use cases in order to make it applicable to various business fields.

5.4.3 *Comparison Results*

Summarizing the evaluation of Bloctrack in comparison to other system approaches, strengths of Bloctrack has been clearly shown. Concerning basic criteria of blockchain-based systems, Bloctrack outperforms the other approaches. Many public blockchains slow down the performance of systems which store most of the data on-chain. Bloctrack overcomes this problem by timestamping the data to secure it and make it immutable. Thus, the tracking process is clearly improved concerning scalability and security in contrast to the other approaches. Another important aspect is the adaptability to other fields of application of supply chains. Apart from AgriBlockIoT, all the proposals are realized with Ethereum. Using a private or federated blockchain to improve scalability is always possible but mostly restricts transparency and permission management. For small networks, immutability cannot always be guaranteed [65].
Smart Contracts as a basic concept, which is used by every system approach including Bloctrack, is mostly used to store or secure product-related data in the supply chain. Therefore, the usage of blockchain systems is limited to blockchains which supports Smart Contracts (especially Bitcoin is excluded and cannot be used).

5.5 EXPERT INTERVIEWS

This section summarizes the results of the expert interviews.

REQUIREMENTS FOR SUPPLY CHAINS According to the expert in Section B.3.1, supply chains have to be fast, cheap and reliable. Furthermore, transparency should be one of the highest priority in supply chains, and counterfeit protection has to be considered too. Additionally, the definition of standards, for example for transports, is another challenge and requirement in supply chains (see interview in Section B.3.2). Furthermore, an uninterrupted data acquisition in combination with tamper protection is a critical issue and hard to solve (see interviews in Section B.3.4 and Section B.3.2). The implementation of transparency in supply chain processes is proving to be very

difficult, as companies are currently not striving for transparency in their processes (see interview in Section B.3.3). Nevertheless, there is a change to more transparency demanded by consumers and thus gains more importance as a requirement in supply chains (see interview in Section B.3.1). Concerning transparency, the preservation of non-transparency for non-participants in the supply chain is essential (see interview in Section B.3.4).
A general demand for supply chains is the accessibility of a real-time status of tracked items (see interview in Section B.3.6).

TECHNOLOGIES The technologies used in supply chains depend on the use case and the tracked products, according to all experts. Besides, costly tags like RFID or NFC tags have various advantages like easy update of the tag's data.

INDUSTRIAL CHALLENGES The challenges for an industrial integration and usage of such a prototype are mainly determined by cryptocurrencies. As some of the experts explain, the exchange between cryptocurrency and real currencies is a huge issue as well as the prevention of data privacy, because information possibly can be extracted by a meta analysis of the transactions in cryptocurrencies (see Section B.3.2 and Section B.3.5).
The willingness of enterprises to integrate cryptocurrencies and transparency is very low (see interviews in Section B.3.3 and Section B.3.1. Furthermore, the implementation of blockchain solutions continues to be viewed with skepticism (see Section B.3.3).

PROTOTYPE CHALLENGES Besides several limitations of the prototype (explained in Section 6.4), some further challenges for the prototype exist. According to the experts in the interviews in Section B.3.2 and Section B.3.4, the replication of the data which is uploaded via IPFS is a difficult challenge. It is mandatory that the data is replicated and accessed steadily. Otherwise, the data will get lost in the network. Due in part to the replication of data, incentives are to be created for sellers to make tracking transparent and ensure data replication in the IPFS network (see interview in Section B.3.2).
In addition, the data sharing in the prototype only depends on the seller. This could lead to discrepancies between seller and customer. In order to avoid this issue, a more balanced data sharing should be developed (see interview in Section B.3.6).
In case of failure, a fallback solution for blockchains has to be considered as well (see Section B.3.1). Furthermore, concrete use cases in B2B and B2C models have to be examined (see Section 6.4).

The results of the expert interviews support the criteria evaluation above. Critical criteria like transparency and trust between participat-

ing parties are clearly enhanced in the prototype according to the experts.
Apart from one interview (Section B.3.5), the feedback of the experts for the developed concept is positive. Nevertheless, applicability to business use cases needs further developments but the actual goals of the prototype for this work are reached.

6 DISCUSSION

This chapter discusses the previous evaluation and draws conclusions. It also provides an overview of the possibilities for improving the prototype and the limitations of the developed concept.

6.1 PROTOTYPE IMPROVEMENTS

Based on the evaluation in Chapter 5, a workflow issue occurring in Bloctrack is described in Section 5.2.1. In order to secure the payment process, the design of Bloctrack as a third-party verification system has to be rethought. The issue of the middle ledger and the workflow obstacle have to be solved while still maintaining security and trust between the parties. As a solution, an infrastructure of Bloctrack nodes can be built up. Each customer and seller has to maintain and run such a node, which can communicate to other Bloctrack nodes by unique IDs. The creation of the HTLC is done by the customer. Furthermore, to initiate an order, the customer sends the contract address, the Smart Contract address, and the preimage of the HTLC to the Bloctrack node of the seller. In Bloctrack, the data can be verified and the order initiated. This system adaption of Bloctrack solves the problem of the middle ledger, but causes other issues and open problems. As an example, the connection between the nodes has to be secured, and it has to be ensured, that fake nodes are identified and excluded from the network to prevent attacks against the network. Furthermore, the hurdles for customers and sellers to use the system are significantly higher than with the current Bloctrack design. This makes the usability and the integration of the prototype into existing systems much more difficult. Thus, Bloctrack is designed and implemented as a third-party system.

Concerning the tracking process in Bloctrack, a more decentralized and independent approach ensures higher security for the tracking and the tracking data. The current implementation is realized with RESTful interfaces for tracking via IPFS. Additionally, the encryption passphrase and the IPFS address is also stored in the Bloctrack database in order to provide a prototype which demonstrates the usage of the technology in an integrative, clear and simple way. Nevertheless, Figure 19 illustrates the workflow of the tracking process without Bloctrack and without storing tracking-related data in the Bloctrack database. There, $z_1, z_2, ..., z_n$ indicate randomly chosen encryption passphrases.

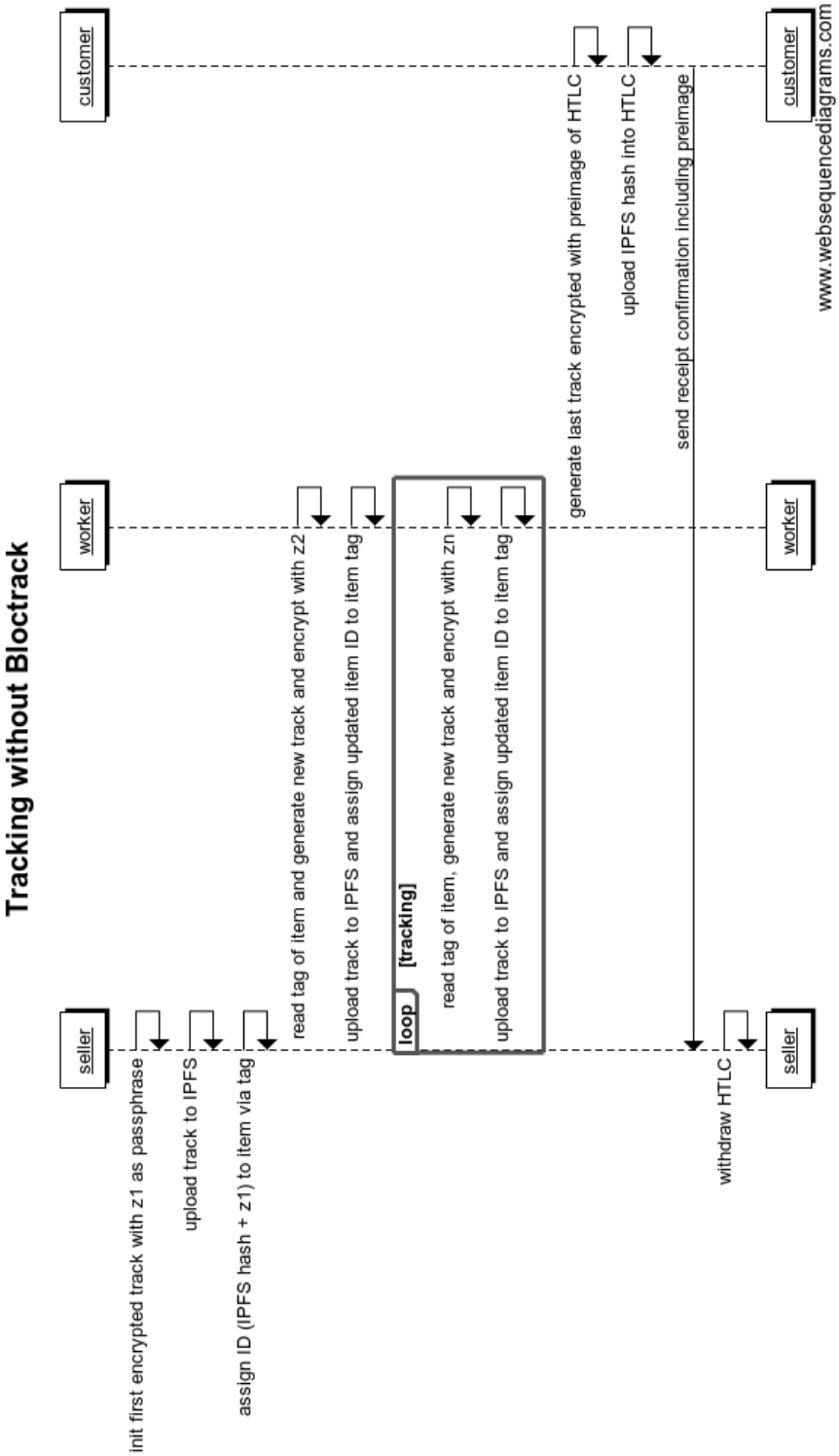


Figure 19: Tracking process realized without Bloctrack

Using the preimage of the HTLC as described in Figure 19, no disadvantages, especially for the customer, occur, because the HTLC can only be withdrawn if the customer transfers the preimage to the seller. With the transfer of the preimage to the seller, the seller gains access to the tracking data. This workflow is more complicated for both parties, customer, and seller. Moreover, the seller cannot access the tracking data during the actual tracking. On the one hand, this limitation is an advantage concerning the data integration and immutability of the tracking data because the seller cannot intervene in the tracking process. On the other hand, the seller cannot react to possible difficulties or changes during the tracking. As an example, sensors produce tracking data and the seller wants to verify the data automatically. If this is possible, the seller can react more quickly and possibly cancel or replace the delivery without the buyer being involved. If this is not possible, additional costs may arise due to the difficult reversal process, which should be avoided. Furthermore, problems can arise if the item tag gets lost or accidentally reset because the tracking data will be completely lost. Finally, this tracking approach in combination with HTLCs may overcome problems with the implemented approach, but also produces new issues and challenges.

6.2 TRUST ENHANCEMENT

In order to answer the second research question concerning trust in supply chains, first, the term trust has to be clarified in this use case as done in Chapter 2. Trust in supply chains is defined as *Contract Trust*, *Predictability* and *Dependability*. Therefore, areas and indication parameters can be defined for supply chain systems with blockchain integration, which enhance trust in such systems. Even though it always depends on the system and its design, general indication parameters can be defined. Consequently, HTLCs, as used in Bloctrack, provide contractual trust between customers and sellers. HTLCs also increase transparency of the whole payment process and enable decentralization for the payment process. In general, decentralization has the potential to build up predictability and transparency in the whole supply chain [28]. Additionally, the decentralization of the tracking process and the data protection through timestamps or Smart Contracts, as used in different approaches, offer verifiability and traceability of the data and thus enhance transparency and trust of participating parties. In addition, data accessibility is an important indication parameter for trust in supply chains. Through decentralization, it is possible to provide data accessibility, data integration, access rights, and permission management in a very transparent way. Therefore, BT is the key technology for decentralization and, correctly and useful applied, an indicator of trust in supply chains. HTLCs as a newly introduced feature enables trust enhancement in payment processes too.

6.3 SCALABILITY IN BLOCKCHAIN-BASED SUPPLY CHAINS

One of the major challenges concerning the integration of BT into supply chain processes is to keep scalability of the SCM system. Answering the first research question mainly results in the discussion of data storage. As it can be seen in Table 4, on-chain storage using public blockchains is not scalable. Either private or federated blockchains can be used instead of public blockchains. Further solution to prevent scalability is timestamping the data, like it is implemented in Bloctrack. Using off-chain storage requires additional timestamping and decentralization in order to maintain advantages of the BT and data integrity and immutability.
Thus, a design for a scalable blockchain-based supply chain system using public blockchains includes timestamps to secure the data. At best, a blockchain is used which can only store timestamps because it is sufficient to store only these on-chain. Transactions are overhead including the amount, fees and additional information which is not necessary anymore. Off-chain storage generally has no performance or scalability issues but is not always applicable to the supply chain use case. A coupling of the timestamp blockchain to a public blockchain (e.g. a cryptocurrency) would be ideal. Thereby, better scalability of the timestamps stored in the blockchain could be achieved, and the advantages of a public blockchain would still be applied.
Scalability is not the main performance factor for payments, because in principle every cryptocurrency that supports Smart Contracts (and thus HTLCs) can be used and payments can be distributed over many cryptocurrencies.

6.4 LIMITATIONS AND CHALLENGES

This sections summarizes the limitations of the prototype resulting from the evaluation and the expert interviews.

As explained in Section 6.1, the occurring problem with the middle ledger of Bloctrack is a limitation of the prototype. A general challenge for many third party systems are man-in-the-middle attacks, and Bloctrack can be also affected by it. Furthermore, throughput limitations of Ethereum can lead to a less scalable system. Automatically tracked data, for example from sensors, can be seen as another limitation because the data is only expected to be tracked correctly. This is not an issue in the prototype but a general problem in supply chains.
In addition, parameter verification and automated data processing have not been implemented yet in the current prototype. For later usage, this is an essential requirement (see also expert interview in Section B.3.5). Items cannot be split, merged or grouped directly as

a functionality of the prototype. Nevertheless, it would be possible to include IPFS hashes of previous items into the tracking parameter section of the first track.
Another challenge, which is also thematized in the expert interview in Section B.3.1, is the handling of private and public keys. Since Bloctrack acts as a trustee, money can theoretically also be mistakenly debited from the prototype account. Then, a person or institutions has to resolve the conflict and possibly needs the private key of the account. As suggested in the expert interview in Section B.3.1, using subkeys or another (decentralized) key management can solve the problem.

Further limitations of cryptocurrencies and Smart Contracts are various obstacles for the industrial applicability. Cryptocurrency exchanges for industrial purposes are hard to realize and behaviour patterns through meta analysis can be retrieved by every participant in the blockchain. This could lead to competitive disadvantages for enterprises (see expert interview in Section B.3.5). Additionally, the application to B2B processes could have less or no benefit of the integrated blockchain technology. Especially the current design of the HTLCs as an escrow account does not allow to map current processes of the industry to Smart Contracts ((see expert interview in Section B.3.5). As an example, HTLCs as implemented in Bloctrack do not support deferred payments or instalments. Nevertheless, for B2C processes and hierarchical supply chains, the design is still applicable (like in the automotive industry, see expert interview in Section B.3.6).
In order to avoid limitations by a centralization of password managements, an on-chain password exchange would be preferable (as stated in the expert interview in Section B.3.4). According to the expert, currently no solution for this issue is known. In the same interview, another challenge for the current prototype is stated. If transparency for participants and non-transparency for non-participants cannot be granted, the benefits of the prototype and its blockchain integration are lost. Another communication limitation to future customers of Bloctrack is the technological barrier. The explanation of the technologies and benefits of such systems are extremely difficult because the technologies, especially blockchains, can be only explained in an abstract way (see expert interviews in Section B.3.3 and Section B.3.1).
A centralized user management can be also seen as a limitation of the prototype. In case the prototype execution fails, or the prototype and the database has been reset, user-related data can get lost. In order to prevent the system from such failures, a decentralized user management can overcome this obstacle.
Various legal matters have to be clarified, like the point in time, when a good is actually owned by the customer. Further legal issues occur with the usage of cryptocurrencies and Smart Contracts like taxes (see expert interviews in Section B.3.5 and Section B.3.6).

A further general issue in the blockchain technology is the need for a fallback solution if the blockchain is not secure anymore (for example less miners, see expert interview in Section B.3.1).

7

CONCLUSION AND FUTURE WORK

The last chapter summarizes the contributions of this thesis and gives an outlook on future work. The aim of this thesis was to evaluate trust enhancement in blockchain-based supply chains. Therefore, an extensive literature review of existing approaches was carried out first. Secondly, a prototype of a blockchain-based supply chain system including HTLCs was designed, implemented, and evaluated based on the previous literature review. Finally, the proposed prototype was analyzed, compared, and evaluated against existing approaches.

7.1 CONTRIBUTIONS

Introducing the research questions in Chapter 1, terms and blockchain-related background information are explained in Chapter 2. The five approaches for the evaluation and comparison are selected within Chapter 3. Thus, followed by the evaluation in Chapter 5, the prototype is presented in Chapter 4.

Several contributions have been made in the context of this thesis. Starting with the proposed prototype, Table 5 illustrates the strength and performance of Bloctrack in comparison to the evaluated approaches focusing on relevant criteria in order to answer the research questions.

Table 5: Summary matrix

	Bloctrack	ACSC [2]	PSC [9]	AgriBlockIoT [12]	EOS [27]	POMS [92]
Trust	+	o	o	o	-	+
Scalability [103]	o	(+)	o	+	o	-
General Assessment	+	o	o	o	-	(+)

The matrix summarizes strength and weaknesses of the compared approaches and classifies them according to the following characteristics: "+": well-designed, "o": can be improved, "-": should be improved

Therefore, the main contribution is the development of the prototype, which outperforms existing approaches and allows conclusions concerning trust and scalability to be drawn. Integrating HTLCs in supply chain processes offers a new level of trust in payment processes in supply chains. Decentralization, transparency, and security are advantages of HTLCs which are realized using public blockchains like Ethereum.
Scalability in Bloctrack can be ensured because timestamps are used to guarantee data integration and data immutability. OriginStamp

provides the possibility of fully decentralized and secure timestamps. Thus, the balance between scalability and trust is maintained in the prototype. Compared to the other approaches, this balance is only given in Bloctrack.

Trust indication parameters are level of decentralization, permission, and data access management as well as transparency in general supply chain processes. Specific supply chain use cases may need further parameters for trust. In order to maintain scalability when integrating BT into supply chains, one option is to create a blockchain for timestamps. Scalability can be maintained as benefits of public blockchains and can be used by the timestamp blockchain.

7.2 FUTURE WORK

This thesis introduces a novel blockchain-based SCM approach which keeps trust and scalability at the same time. Nevertheless, several limitations of the current implementation exist. Next, the most important restraints and possible future researches are summarized.

THROUGHPUT In the prototype, throughput is mainly limited by the Ethereum blockchain. Therefore, multi-ledger payments and HTLCs can be used in order to overcome challenges in the payment process.

REFUNDS Currently, HTLCs are not refunded automatically. Thus, a scheduler, which tries to refund outdated contracts, should be used. This would decrease effort and costs for customers.

MANY-COMPONENTS-DESIGN The current design is limited to one component and does not allow more. Thus, further research can be done to evaluate the usage of semantic hashes in order to identify product groups. In addition, the usage of a tree structure of origins of components and tracking data can be possibly applied to the prototype. Further, a recall management system based on the many-components-design can be developed. The usage of semantic hashes can lead to better performance for recalls.

TRACKING Within Section 6.1, a new tracking approach is proposed and its limitations and problems are stated. Nevertheless, upcoming issues in the tracking process in the current Bloctrack implementation are overcome. Thus, further research should be done to increase data security during tracking.

Limitations and challenges stated in Section 6.4 should be also considered for future work. Additionally, the prototype and the concept behind should be contextualized and the usage of incentives should

be explored in order to encourage customers enhancing transparency in supply chains (according to the expert in Section B.3.2). According to the expert in Section B.3.6, a more balanced data sharing should be developed.

7.3 CONCLUSION

In this thesis, a blockchain-based supply chain prototype is proposed. It integrates HTLC and maintains scalability. Therefore, payments are secured, and an independent verification can be done by participating parties. The combination of HTLCs, IPFS, and timestamps with OriginStamp increases security, data immutability, verifiability, and decentralization in supply chains. Furthermore, the thesis investigates trust enhancement in supply chains and simultaneously scalability keeping.

The evaluation and comparison with other approaches demonstrate the benefits of the technologies and features used in the prototype. Additionally, the expert interviews show more requirements for supply chains, limitations, and challenges in the prototype. Further research is worthwhile because decentralization and BT have the potential to enormously increase trust and security for customers and sellers and revolutionize existing SCM systems.

A PROTOTYPE

A.1 TRACK DATA STRUCTURE

```
{
    "item_uuid":itemID,
    "owner_uuid":userID,
    "tracker_id":trackerID,
    "last_track_hash":lastTrackHash,
    "last_ipfs_hash":lastIpfsHash,
    "last_ipfs_passw":lastIpfsPassword,
    "tracking_time":trackingTime,
    "tracking_param":
    [
        {
            param:param_1,
            value:value_1,
        },
        {
            param:param_2,
            value:value_2,
        },

        ....
    ]
}
```

A.2 HASHED TIMELOCK CONTRACT (SOLIDITY)

```
pragma solidity ^0.4.24;

/**
 * @title Hashed Timelock Contracts (HTLCs) on Ethereum ETH.
 *
 * This contract provides a way to create and keep HTLCs for ETH.
 *
 * See HashedTimelockERC20.sol for a contract that provides the same
     functions
 * for ERC20 tokens.
 *
 * Protocol:
 *
 *  1) newContract(receiver, hashlock, timelock) - a sender calls this to
      create
 *      a new HTLC and gets back a 32 byte contract id
 *  2) withdraw(contractId, preimage) - once the receiver knows the
     preimage of
 *      the hashlock hash they can claim the ETH with this function
 *  3) refund() - after timelock has expired and if the receiver did not
```

```
 *      withdraw funds the sender / creater of the HTLC can get their ETH
 *      back with this function.
 */
contract HashedTimelock {

    event LogHTLCNew(
        bytes32 indexed contractId,
        address indexed sender,
        address indexed receiver,
        uint amount,
        bytes32 hashlock,
        uint timelock
    );
    event LogHTLCWithdraw(bytes32 indexed contractId);
    event LogHTLCRefund(bytes32 indexed contractId);

    struct LockContract {
        address sender;
        address receiver;
        uint amount;
        bytes32 hashlock; // sha-2 sha256 hash
        uint timelock; // UNIX timestamp seconds - locked UNTIL this time
        bool withdrawn;
        bool refunded;
        bytes32 preimage;
    }

    modifier fundsSent() {
        require(msg.value > 0);
        _;
    }
    modifier futureTimelock(uint _time) {
        // only requirement is the timelock time is after the last
            blocktime (now).
        // probably want something a bit further in the future then this.
        // but this is still a useful sanity check:
        require(_time > now);
        _;
    }
    modifier contractExists(bytes32 _contractId) {
        require(haveContract(_contractId));
        _;
    }
    modifier hashlockMatches(bytes32 _contractId, bytes32 _x) {
        require(contracts[_contractId].hashlock == sha256(abi.
            encodePacked(_x)));
        _;
    }
    modifier withdrawable(bytes32 _contractId) {
        // require(contracts[_contractId].receiver == msg.sender);
        require(contracts[_contractId].withdrawn == false);
        require(contracts[_contractId].timelock > now);
        _;
    }
    modifier refundable(bytes32 _contractId) {
        // require(contracts[_contractId].sender == msg.sender);
        require(contracts[_contractId].refunded == false);
```

```
        require(contracts[_contractId].withdrawn == false);
        require(contracts[_contractId].timelock <= now);
        _;
    }

    mapping (bytes32 => LockContract) contracts;

    /**
     * @dev Sender sets up a new hash time lock contract depositing the
         ETH and
     * providing the reciever lock terms.
     *
     * @param _receiver Receiver of the ETH.
     * @param _hashlock A sha-2 sha256 hash hashlock.
     * @param _timelock UNIX epoch seconds time that the lock expires at.
     *                  Refunds can be made after this time.
     * @return contractId Id of the new HTLC. This is needed for
         subsequent
     *                    calls.
     */
    function newContract(address _receiver, bytes32 _hashlock, uint
        _timelock)
        external
        payable
        fundsSent
        futureTimelock(_timelock)
        returns (bytes32 contractId)
    {
        contractId = sha256(abi.encodePacked(msg.sender, _receiver, msg.
            value, _hashlock, _timelock));

        // Reject if a contract already exists with the same parameters.
            The
        // sender must change one of these parameters to create a new
            distinct
        // contract.
        if (haveContract(contractId))
            revert();

        contracts[contractId] = LockContract(
            msg.sender,
            _receiver,
            msg.value,
            _hashlock,
            _timelock,
            false,
            false,
            0x0
        );

        emit LogHTLCNew(
            contractId,
            msg.sender,
            _receiver,
            msg.value,
            _hashlock,
            _timelock
```

```
        );
    }

    /**
     * @dev Called by the receiver once they know the preimage of the
         hashlock.
     * This will transfer the locked funds to their address.
     *
     * @param _contractId Id of the HTLC.
     * @param _preimage sha256(_preimage) should equal the contract
         hashlock.
     * @return bool true on success
     */
    function withdraw(bytes32 _contractId, bytes32 _preimage)
        external
        contractExists(_contractId)
        hashlockMatches(_contractId, _preimage)
        withdrawable(_contractId)
        returns (bool)
    {
        LockContract storage c = contracts[_contractId];
        c.preimage = _preimage;
        c.withdrawn = true;
        c.receiver.transfer(c.amount);
        emit LogHTLCWithdraw(_contractId);
        return true;
    }

    /**
     * @dev Called by the sender if there was no withdraw AND the time
         lock has
     * expired. This will refund the contract amount.
     *
     * @param _contractId Id of HTLC to refund from.
     * @return bool true on success
     */
    function refund(bytes32 _contractId)
        external
        contractExists(_contractId)
        refundable(_contractId)
        returns (bool)
    {
        LockContract storage c = contracts[_contractId];
        c.refunded = true;
        c.sender.transfer(c.amount);
        emit LogHTLCRefund(_contractId);
        return true;
    }

    /**
     * @dev Get contract details.
     * @param _contractId HTLC contract id
     * @return All parameters in struct LockContract for _contractId HTLC
     */
    function getContract(bytes32 _contractId)
        public
        view
```

```
178         returns (
                address sender,
                address receiver,
                uint amount,
                bytes32 hashlock,
183             uint timelock,
                bool withdrawn,
                bool refunded,
                bytes32 preimage
            )
188     {
            if (haveContract(_contractId) == false)
                return;
            LockContract storage c = contracts[_contractId];
            return (c.sender, c.receiver, c.amount, c.hashlock, c.timelock,
193                 c.withdrawn, c.refunded, c.preimage);
        }

        /**
         * @dev Is there a contract with id _contractId.
198      * @param _contractId Id into contracts mapping.
         */
        function haveContract(bytes32 _contractId)
            internal
            view
203         returns (bool exists)
        {
            exists = (contracts[_contractId].sender != address(0));
        }
    }
```

B

EXPERT INTERVIEWS

B.1 INTERVIEW GUIDELINE (GERMAN)

Teil 1: Einführende Fragen

- Wie werden Produkte bei Ihnen verfolgt? Welche Technologien werden eingesetzt?
- Wo und wann fängt die Lieferkette eines Ihrer Produkte an? Wie viele Stationen durchläuft ein Produkt durchschnittlich?
- Überprüfen Sie zugekaufte Produkte und/oder verfolgen deren Lieferketten? Müssen Ihre und zugekaufte Produkte gewisse Transportstandards und Bedingungen erfüllen? Wenn ja, wird die Einhaltung derer überprüft und sichergestellt?
- Welche Kosten fallen bei einem Produkt nur für dessen Nachverfolgbarkeit im Verhältnis zu dessen Wert an?
- Welche Anforderungen stellen Sie an Lieferkettenprozesse und deren Abbildung?
- Welchen Stellenwert hat Transparenz und Vertrauen gegenüber Kunden in Bezug auf Lieferkettenprozesse?
- Welchen Stellenwert haben Lieferketten für Sie und Ihre Kunden und wie wird dieser versucht zu optimieren? Wird dieser überhaupt optimiert?
- Werden Lieferkettenprozesse bei Ihnen selbst entwickelt und optimiert oder ausgelagert?
- Sind Sie durch Ihre Arbeit oder privat schon mit der Blockchain-Technologie in Berührung gekommen? Wenn ja, inwiefern?
- Ist Ihr Unternehmen an der Blockchain-Technologie für eigene Entwicklungen interessiert?

Teil 2: Präsentation des entwickelten Konzepts

- Kurze Vorstellung der Eigenschaften der Blockchain und Smart Contracts
- Einführung der im Prototyp benutzten Technologien: IPFS, HTLCs und OriginStamp
- Vorstellung der abgebildeten Prozesse im Prototyp durch Abbildungen aus Kapitel 4 und Screenshots des Prototyps

  - Zwei-Parteien Modell mit Kunde und Verkäufer
  - Unterteilung in Bestellung, Tracking und Bezahlung
  - Fokus auf Preimage des HTLCs und dessen Übergabe an Verkäufer sowie Timestamping
- Kurze Erläuterung der Vorteile und Unterschiede zu konventionellen Ansätzen
  - Dezentralisierung
  - Transparenz und damit einhergehendes Vertrauen
- Verbleibende Fragen abklären

Teil 3: Fragen zum entwickelten Konzept

- Wie ist Ihr erster Eindruck des vorgestellten Prototyps?
- Wie schätzen Sie die Integration des Konzepts in bestehende Prozesse ein? Was müsste wie angepasst werden?
- Welche Schwächen oder Limitierungen sehen Sie im vorgestellten Konzept?
- Welche Bedenken bezüglich des vorgestellten Konzepts und Datensicherheit haben Sie?
- Haben Sie Bedenken, auf einer öffentlichen Blockchain zu operieren?
- Wie stehen Sie zur Modellierung als Drittanbietersystem?
- Haben Sie den Eindruck, dass das vorgestellte Konzept Transparenz und damit Vertrauen zu Kunden sowie unternehmensinterne Prozesse optimieren oder verbessern kann?

B.2 INTERVIEW GUIDELINE (ENGLISH)

Part 1: Introductory questions

- How do you track products? Which technologies are used?
- Where and when does the supply chain of one of your products start? How many stations does a product pass through on average?
- Do you check purchased products and/or track their supply chains? Do your products and purchased products have to meet certain transport standards and conditions? If so, is compliance with these checked and ensured?
- What are the costs of a product only for its traceability in relation to its value?

- What requirements do you place on supply chain processes and their mapping?
- How important is transparency and trust towards customers in relation to supply chain processes?
- What value do supply chains have for you and your customers and how do you try to optimize them? Are supply chains optimized at all?
- Do you develop and optimize or outsource supply chain processes yourself?
- Have you already come into contact with blockchain technology through your work or privately? If so, to what extent?
- Is your company interested in blockchain technology for its own developments?

Part 2: Presentation of the developed concept

- Short presentation of the properties of Blockchain and Smart Contracts
- Introduction of the technologies used in the prototype: IPFS, HTLCs and OriginStamp
- Presentation of the depicted processes in the prototype using graphics from Chapter 4 and screenshots of the prototype
  - Two-party model with customer and seller
  - Subdivision into purchase order, tracking, and payment
  - Focus on preimage of the HTLC and its handover to the seller as well as time stamping
- Brief explanation of the advantages and differences to conventional approaches
  - decentralization
  - Transparency and trust associated with it
- Clarify remaining questions

Part 3: Questions about the developed concept

- What is your first impression of the presented prototype?
- How do you rate the integration of the concept into existing processes? What needs to be adapted and how?
- What weaknesses or limitations do you see in the presented concept?

- What concerns do you have about the presented concept and data security?
- Do you have concerns about operating on a public blockchain?
- What do you think of modeling as a third-party system?
- Do you have the impression that the presented idea can optimize or improve transparency and thus trust in customers as well as internal company processes?

B.3 INTERVIEWS

The "A" in the interviews stands for author, the "E" stands for the interviewed expert.

B.3.1 *Expert Interview 1*

A: Ich würde erstmal generell mit ein paar einleitenden Fragen anfangen. Und zwar geht es ja um Produktverfolgung und -tracking. Wie würdest du Produktverfolgung gestalten und welche Technologien würdest du einsetzen und auf welche Merkmale würdest du besonders achten?
E: Also prinzipiell finde ich, ist Produktverfolgung heute sehr individuell implementiert. Es gibt keine DIE supply chain. Du musst natürlich sehen: jedes Produkt hat völlig andere Kriterien und es bedingt auch ein völlig anderes Handling. Das heißt, jetzt musst du das runterbrechen von den vielen Möglichkeiten auf Gemeinsamkeiten. Und Produkte an sich haben ja eine Gemeinsamkeit, die jedes Produkt teilt: entweder ist es original oder gefälscht. Das ist mal ganz unten. Es kann jetzt sein, dass es dich gar nicht interessiert in der supply chain, aber es ist eine Eigenschaft, die jedes Produkt hat. Jedes Produkt ist auch funktional oder nicht (mehr) funktional, das heißt, es gibt nochmal die Auftrennung, dass das Produkt noch gut ist (funktional) oder nicht mehr. Auch nochmal extrem wichtig und hat auch nochmal Auswirkungen auf die Modularität in der supply chain. Wenn du jetzt im Food-Bereich oder Pharma-Bereich bist und etwas muss zwischen 5 und 10 Grad gelagert sein, dann ist das „gut“ oder „nicht gut“ mindestens so wichtig, wie ob es echt oder falsch ist. Da gibt es ganz viele Kriterien, die von unten rauf eine Rolle spielen und dann geht eine supply chain über viele Stellen hinweg. Du hast neben dem Prozess der Herstellung einen Prozess der Lieferung an die verschiedenen Orte, wo verarbeitet wird beziehungsweise die Herstellung weitergeführt wird. Und du hast einen parallellaufenden Prozess wegen dieser Lieferung, den Transport. Du musst also den Transport als parallele Aufgabe anschauen neben der Produktion. Eine supply chain ist insofern immer mehrschichtig. Wenn du jetzt noch zusätzlich sicherstellen willst, dass das Produkt nicht verdorben, kaputt oder unbrauchbar ist und dass es original ist, dann fügst du da

noch zusätzliche Schichten dazu. Heute hast du im Regelfall einen Barcode. Und der Barcode wird über die Lieferkette verfolgt. Er geht von Stufe A bis Stufe X und wird von den verschiedenen Ebenen gleichermaßen verwendet. Das heißt, du hast die Transportebene, die mit dem Barcode arbeitet und die Produktionsebene, die mit dem Barcode arbeitet. Der Barcode wird erneuert, wenn man zum Beispiel das Paket aufreißt.

A: Jetzt haben wir uns die Produktgestaltung angeschaut, wie sieht es mit den eingesetzten Technologien aus?

E: Das große Problem ist, dass du komplett verschiedene Anforderungen hast. Du hast in der supply chain generell industrielle Anforderungen. Du hast aber zum Beispiel auch Farmer als Gruppe für sich, die jetzt teilweise gar nicht industrialisiert sind und teilweise hoch industrialisiert sind. Das heißt, du hast Prozesse, wo du dich faktisch anpassen können musst auf das Niveau des Lieferanten oder den Lieferanten dazu bringen musst, dass er sich auf dein Niveau anpasst. Das ist natürlich eine große Herausforderung und der Aufwand ist dementsprechend viel kleiner oder viel größer. Wenn du jetzt hingehst und alles mit Smart Contracts machst, wird jeder Prozess neu gestaltet. Du kannst auch hingehen und sagst, wir machen das jetzt über eine andere Technologie, die einfacher zu integrieren ist (beispielsweise in einem zusätzlichen Layer mitlaufen lässt wie OriginStamp mit Hashes, die einen Zeitstempel in der Blockchain bekommen). Dann kannst du zumindest mal sagen, dass der Zustand so war. Du kannst immer noch nicht eine Aussage über die Originalität treffen. Aber du kannst immerhin sagen, dass die digitalen Daten, die zu dem Zeitpunkt von dem physischen Objekt gemacht wurden, nicht verändert wurden. Ich habe dann eine gewisse Dokumentation. Dabei musst du nicht zwingend jeden Prozess anfassen. Es kommt drauf an, wie man versucht, eine supply-chain-Lösung zu bieten und wie bereit man ist, auf bestehende Prozesse einzugehen oder eben neu zu verlangen. Und alles ist natürlich auch eine Frage der individuellen Integration und deshalb sehr aufwendig.

A: Was ist einfacher für Unternehmen: bestehende Prozesse zu verändern oder zu überschreiben und neu zu definieren?

E: Verändern von bestehen Prozessen ist im Normalfall die Hölle. Du fängst nicht mit einem Problem an, sondern du weckst ein Problem oder x Probleme. Derjenige, der 10 Jahre lang den Prozess so gemacht hat, der muss jetzt umlernen. Und jetzt kommst du noch vielleicht mit neuer Hardware und es funktioniert etwas nicht. Plus du hast vielleicht den neu durchdachten Prozess in der Praxis noch gar nicht getestet und er funktioniert gar nicht. Das heißt, du hast auf einmal eine etwa fünf-dimensionale Problematik, die unausgetestet ist. Und das führt natürlich auch zu entsprechender Frustration. Deshalb auch ganz klar: bestehende Prozesse übernehmen ist immer besser, was die funktionalen Risiken angeht. Es führt aber nicht zwingend zum

besseren Prozess. Was ganz wichtig ist, ist die einfache Anwendung. Warum sonst werden Barcodes eingesetzt? Barcodes gibt es sicher schon 60 Jahre, das ist ja nichts richtig Neues. Aber er ist immer noch da und erst jetzt eigentlich wirklich da. Wie viele Produkte gab es vor 20 Jahren, die noch keinen Barcode hatten? Wahrscheinlich noch ziemlich viele. Die Anlaufzeit ist ja riesig und insofern brauchst du gute Lesegeräte auf jeden Fall, damit die Objekte gut erkannt werden und Leute, die das gut bedienen können. Und das ist in der supply chain schon ein heißes Eisen. Was ein großes Problem in der supply chain für das Individuum ist: wenn wir in der supply chain tätig wären; du bist zuverlässig und ich nicht. Aber ich habe meine Schicht nach deiner Schicht. Und ich bin der, der gut quatschen kann und war nie schuld. Dann bist immer du angeschmiert. Jetzt möchtest du gerne mal beweisen, dass es nicht so ist. In der supply chain ist es also wichtig, dass man quality assurance hat, dass man Optimierungsmöglichkeiten hat und deswegen, dass man detaillierte Informationen gewinnt über das, was wirklich abläuft. Und diese Informationen sind im Moment wahrscheinlich noch nicht so zuverlässig wie sie sein könnten, wenn du eine normale supply chain von einem industriellen Produkt mit einem Wert unter 20 Euro nimmst. Sobald du in die hochwertigen Produkte gehst, hast du tags. Und bei den tags sieht es ganz anders aus. Da sieht es natürlich viel besser aus. Da hast du schon viele von den besprochenen Punkten sowieso schon gelöst. Einzige Punkte, die du noch nicht gelöst hast: der tag ist immer noch nicht Bestandteil vom Objekt. Bedeutet: du hast immer noch das Fälschungsproblem. Aber du kannst zum Beispiel mit dem Smart Sensor lösen, ob das Produkt noch gut ist oder nicht gut ist.

A: Produkte müssen zum Beispiel auf dem Transportweg Bedingungen und Standards erfüllen, zum Beispiel muss ein medizinisches Produkt bestimmte Temperaturen einhalten. Wie würdest du die Überprüfung von den Sensordaten sicherstellen?

E: Das ist eine ganz zentrale Frage. Es gibt meines Erachtens zwei Vektoren. Der eine Vektor ist, dass die ausgelesenen Daten sofort unveränderbar gemacht werden. Nicht, dass jemand im Nachhinein die Daten verändern kann. Dann ist der ganze Prozess vom Auslesen nichts. Der zweite Punkt ist, dass du auch eine Verbindung schaffst zwischen dem, was du misst, und zwischen dem, was gemessen wurde. Nicht nur was temperaturmäßig gemessen wurde, sondern das, was es betrifft. Als Beispiel hast du eine Palette mit Impfstoffen. Der Fahrer geht an der Tankstelle pinkeln und vergisst die Kühlung an zu lassen. Das Ding wird warm. Die ganze Palette kannst du wegwerfen (mit der heutigen Technologie). Problem ist allerdings, dass wahrscheinlich zwei Drittel von den Impfstoffen problemlos einsetzbar gewesen wäre. Vielleicht sogar 100% noch einsetzbar gewesen wären. Aber die äußersten zwei Schichten hätten beispielsweise ein Verfallsdatum gehabt, was 10% dem ursprünglichen Verfallsdatum

entsprochen hätte. Wenn man das sofort benutzt hätte, wäre es noch gegangen. Mit diesem Wissen hätte man vermeiden können, dass sie weggeworfen hätten werden müssen. Man hätte sie einfach schneller einsetzen können. Und je weiter du innen in die Palette reinkommst, desto stärker ist es isoliert und desto weniger hat es dem Zeug ausgemacht. Desto länger ist es auch haltbar. Das bekommst du heute nicht gemessen. Das ist natürlich im Prinzip das, was man eine Intelligenz nennt. Zusätzlich zu den Sensoren wäre es durchaus auch möglich, dass man Dinge ausliest, die zum Objekt selber gehören. Du hast einen Sensor, der misst und Daten schickt oder du hast eine bildliche Erfassung eines Umstandes und generierst daraus digitale Daten (physischer Zustand, den du digital dokumentierst) oder du hast beispielsweise eine Videoüberwachung, die einen Prozess dokumentiert. Ein Sensor ist nur ein Teil der Erfassung verschiedener Varianten von Zuständen oder Prozessen. In der supply chain, idealerweise, sollte mit diesen Daten optimal umgegangen werden können, damit jeder, der in einem Teilbereich tätig ist, optimal und schnellstmöglich seine Arbeit machen kann, ohne, dass er über irgendwas stolpert. Ganz schlimmes Beispiel bei der Bahn. Da gab es noch vor ein paar Jahren die Situation, dass die gar nicht mehr wussten, wo ihre Waggons stehen. Die mussten also Leute, die schon in Pension waren, fragen, wo die Waggons stehen. Das erklärt einem bildlich, wo die Probleme liegen können. Weil früher sind sie über Mittag Karten spielen gegangen und haben sich untereinander ausgetauscht und auf den neuesten Stand gebracht. Jetzt sind die aber in Pension. Und die Neuen spielen nicht mehr Karten und das System funktioniert nicht mehr. Jetzt musst du es technologisch ersetzen und kommst zu smarten Sensoren, die dir das innerhalb eines Datenflusses mitteilen.

A: Okay. Welche Anforderungen stellst du an Lieferkettenprozesse und deren Abbildung?

E: Geht es konkreter?

A: Wir hatten vorher ja schon, dass man die Fälschungssicherheit in Lieferketten berücksichtigen sollte. Was gibt es da sonst noch?

E: Also im Prinzip gibt es zwei ganz sichere Ansprüche. Es gibt einmal den Anspruch der Geschäftsebene, dass man einen möglichst schnellen, günstigen und verlässlichen Prozess hat. Und dann gibt es aber auch neu den Anspruch des Endkonsumenten. Und der möchte idealerweise einen transparenten Prozess, wo er erkennen kann, dass er nicht hinters Licht geführt wurde. Er glaubt nicht mehr per se was er gesagt bekommt. Dass die Biomilch wirklich Bio ist und nicht irgendwann zwischendrin der Container gewechselt wurde. Solche Dinge werden jetzt natürlich zu neuen Herausforderungen von supply chains. Da sind die teilweise gar nicht vorbereitet. Im Gegenteil, die schotten sich bewusst ab und wollen den Endkonsumenten nicht drin haben. Damit verschenken sie sich eine unglaubliche Marketing-Möglichkeit, weil sie ja Endkonsumenten-Daten umgekehrt eben schon

wollen. Das ist eigentlich ein totaler Widerspruch: sie wollen die Daten aber sie wollen nicht, dass der Endkunde Einsicht in die Daten hat. Und das funktioniert so nicht, weil die Leute heute nicht mehr so naiv sind, dass sie sagen, dass du alle meine Daten haben kannst und ich nichts sehen darf. Da musst du liefern. Deswegen sind alte supply chains nicht wertfördernd für das Endprodukt. Man kann keine zusätzliche Wertschöpfung machen, weil der Endkunde gar nicht in Berührung kommt in dem Maße, dass er tatsächlich einen zusätzlichen Wert dem zuschreiben würde. Das ist natürlich eine Chance, wenn einer das dann umsetzt und du hast, ganz banal, zwei Schachteln Pralinen vor dir. Bei der einen siehst du, dass sie beim gesamten Transport in 15 Grad Temperatur gehandelt wurde, dass keine 4G drauf eingewirkt haben und dass sie vor 3 Tagen produziert wurden. Und die andere Schachtel ist gleichwertig an für sich. Da siehst du gar nichts. Da stellt sich dann schnell die Frage: wenn du für dich kaufst, kaufst du doch die günstige. Dann gewinnt natürlich sozusagen die billigere Lösung. Aber wenn du es spätestens mal für dein Kind kaufst, dann ist dir das sehr viel mehr Wert und wichtiger (vor allem auch bei Babynahrung beispielsweise). Dann nimmst du auf jeden Fall das Zuverlässige und sicher nicht das, das 50 Cent weniger kostet. Sonst kaufst du im schlimmsten Fall ein Gläschen weniger, dafür das bessere. Das ist natürlich der Trend, der so langsam sich über die Bereiche, wo das Schmerzempfinden besonders hoch ist, sichtbar wird. Aber das wird sich über alle Bereiche ausrollen. Das wird zur Gewohnheit werden. Du wirst die Gewohnheit haben, dass du Klarheit haben willst, weil die Technik dir das liefern kann. Dieser Anspruch an die Technik wird gestellt werden (als Hypothese).

A: Sehr interessant. Da entnehme ich, dass Transparenz einen sehr hohen Stellenwert haben sollte in Lieferkettenprozesse.

E: Einer der höchsten Stellenwerte sollte Transparenz sein, weil schlussendlich die Endkonsumenten davon profitieren, weil der Prozess sich besser optimieren lässt und von der Firma her sieht, wo es klemmt. Und weil neben der Prozessoptimierung die quality assurance viel besser funktionieren kann. Das heißt, es ist nicht nur ein Grund, sondern es sind ganz viele Gründe, die dafür sprechen das transparent zu gestalten.

A: Jetzt noch ganz kurz bisschen Background-Informationen. Wann und wie bist du mit der Blockchain-Technologie in Berührung gekommen und wie hast du da weiterverfolgt?

E: Blockchain-Technologie grundsätzlich kenne ich solange seit sie es gibt, weil ich vor 10 Jahren ein Patent mit einem Verfahren patentieren lassen. Das Patent stellt ein Verfahren dar, das die Notariatsfunktion digitalisiert. Und das Hochinteressante an der Blockchain ist ja gerade, dass genau dieser Prozess aufgegriffen wird, in seiner Abfolge fast identisch abgebildet ist mit dem einzigen Unterschied, dass ich als Notarvertrauensinstanz eigentlich ein Publikationsorgan

habe. Das bedeutet: Die Bestrebungen, Lösung zu finden für die Problematik für das „Superadminproblems“, das Vertrauen zu demokratisieren. Da gab es natürlich viele Bestrebungen und man muss dazu sagen: die Blockchain-Lösung von Anfang an wurde belächelt wegen der Begleiterscheinung der Kryptowährungen. Jeder hat natürlich gesagt, dass das jeder könne. Du erfindest Geld, was nichts wert ist und für das Geld darfst du dann arbeiten. Was soll das? Das Versprechen ist, dass es dann mal ganz viel Wert wird, super. Das war natürlich die allgemeine Meinung. Die dahinterstehende Technologie hat man dann immer etwas kritischer betrachtet hat als es korrekt gewesen wäre. Eigentlich wird man ja fast schon bisschen ausgenutzt, wenn man da mitmacht. Das sieht man natürlich jetzt heute mit anderen Augen. Wobei die Gesellschaft immer noch ganz ähnlich reagiert. Der Wert der Kryptowährung führt letztlich dazu, dass man das entweder als coole oder nicht so coole Sache sieht. Jetzt wo sie runter gegangen sind, sind ganz viele Leute kritisch. Die Technologie ist aber die gleiche. Die Blockchain ist wirklich eine unglaublich gute Lösung für dieses eine Problem. Und wenn dieses eine Problem gelöst wird, dann kannst du natürlich sehr viel Transparenz schaffen. Ob das Problem so nachhaltig gelöst ist, das ist noch nicht bewiesen. Wir sind hier im Konsensus und der Konsensus hat jetzt funktioniert die letzten Jahre. Aber das sind auch noch nicht hunderte von Jahren. Es wird vielleicht noch andere Konsensus-Varianten geben. Vielleicht in Kombinationen und es wird vielleicht sogar auch wieder den Weg zurück in die physische Welt geben. Es ist vielleicht etwas vermessen, das zu sagen. Aber es könnte durchaus passieren, ohne den Prozess als solchen allzu stark zu verändern.

A: Das war ein sehr interessanter einleitender Teil. Jetzt würde ich meinen Prototyp vorstellen. Zur Information: ich habe Blockchains, Smart Contracts und OriginStamp verwendet. IPFS sagt dir was?

E: Ja.

A: Das hab ich auch verwendet. Jetzt kommen wir noch zu den HTLCs. Und zwar ist das nur was, was in einem Smart Contract abgebildet wird. Du hast zwei Parteien, Person A und Person B. Person A erstellt diesen Vertrag mit einem Timelock und einem Hashlock. Wenn der Timelock ausläuft, dann passiert gar nichts. Wenn der Hashlock beziehungsweise das Preimage zu Person B kommt, kann Person B den Smart Contract ansprechen und die Transaktion von Person A zu Person B durchgeführt (mit dem Preimage) und Person B bekommt sein Geld. Wenn etwas schiefläuft (Person B macht nicht das, was Person A will), dann gibt Person A einfach dieses Passwort nicht an Person B und es passiert gar nichts (Timelock läuft aus). Da haben wir den Vorteil gerade für Person A, dass sie sicherstellen kann, dass Person B erst die Bedingungen erfüllen muss, bevor Geld fließt. Person B wiederum weiß, dass er das Geld sicher bekommt, wenn er die Bedingungen erfüllt.

E: Weil das Geld da ist.

A: Genau. Dieses Prinzip benutze ich. Dann habe ich meinen Prototyp in

drei Teile aufgeteilt: das ist die Bestellung, das Tracking und der Bezahlvorgang an sich. Die Bestellung funktioniert so: Der Kunde bestellt zuerst bei dem Verkäufer das Produkt und bekommt dann einen Preis. Dann überweist der Kunde an Bloctrack (Prototyp) den Betrag und inkludiert in diese Transaktion noch einen Hash, der sich aus einem Passwort vom Kunden und seiner Mailadresse zusammensetzt.

E: Das ist ja die Transaktions-ID sozusagen.

A: Genau, das funktioniert wie eine Transaktions-ID, weil ich nachher sicherstellen will, dass diese Transaktion nur einmal verwendet wird. Als nächstes ist es so, dass der Kunde dem Verkäufer dieses Passwort aus der Transaktion gibt. Dann kann der Verkäufer die Bestellung initiieren und muss das Passwort, die Mailadresse des Kunden und den Transaktionshash Bloctrack mitteilen. Dann wird das im Prototyp gecheckt, ob die Informationen stimmen. Wenn ja, dann erstellt Bloctrack diesen HTLC zwischen dem Kunden und dem Verkäufer. Der Timelock wird auch über den Verkäufer spezifiziert. Da ist es aktuell aber so realisiert, dass der Timelock höchstens 14 Tage sein kann. Das ist nur eine Beispiel-Obergrenze, damit der Verkäufer keinen zu hohen Timelock eingeben kann. Die Mail für den Kunden, die der Kunde nach Erstellung des HTLC bekommt, beinhaltet alle nötigen Informationen über den HTLCC, damit der Kunde die vollständige Kontrolle über sein Geld behält. Zusätzlich wird noch ein Zeitstempel über OriginStamp erstellt, der die ID von dem HTLC, den Transaktionshash und die interne item ID von Bloctrack beinhaltet. Warum? Weil diese Kombination dient dazu, damit der Kunde immer eindeutig nachweisen kann, wann welcher contract mit welcher Transaktion benutzt wurde. Zum Beispiel: wenn jetzt ein Verkäufer behauptet, dass die Transaktion noch nicht benutzt wurde, dann kann ich mit meinem Zeitstempel das Gegenteil beweisen. Den HTLC kann ich dann auch wieder nachprüfen. Das ist der sichere Bestellvorgang, den ich modelliert habe.

E: Mir ist noch nicht ganz klar, was es mit der Verifikation der item creation auf sich hat. Das wird irgendwo in einer Blockchain-Adresse hinterlegt?

A: Das wird über OriginStamp submitted.

E: Das wird dann auch verifizierbar über einen root hash.

A: Richtig. Das Tracking funktioniert so, dass nach dem Verschicken von einem Paket Tracking-Daten erstellt werden und diese werden automatisch getracked.

E: Kurze Zwischenfrage. Du generierst hier jetzt Smart Contracts ohne Einsatz von private/public keys. Warum?

A: Letztendliche ist es so, dass nicht viele Smart Contracts erstellt werden, sondern es wird genau ein Smart Contract erstellt (verwaltet über den Prototyp) und in diesem werden die HTLC verwaltet. Aber das ist tatsächlich ein Problem, was in diesem Prototyp existiert, nämlich die Verwaltung von private und public keys. Vor allem vom private key. Der liegt beim Prototyp und der ist eine zentrale Instanz. Da haben wir das Problem, dass wir eigentlich wieder Vorteile der Dezentralisierung verlieren. Da gibt es mehrere

Ansätze, die ich schon bedacht habe. Zum Beispiel könnte man sagen, dass der Prototyp den private key hat und dieser private key ist bei einer öffentlichen Institution hinterlegt und kann dann nur bei Bedarf oder Problemen angefordert und benutzt werden. Ansonsten ist er nicht bekannt.
E: Das ist hochkritisch.
A: Stimmt. Ich habe in meiner Arbeit auch noch eine andere Variante betrachtet. Da ist Bloctrack kein Drittanbietersystem mehr, sondern dass im Prinzip jeder Käufer und jeder Verkäufer ein eigener Knotenpunkt im Netzwerk ist. Also dass der Prototyp keine Drittanbieterinstanz mehr ist, sondern dass es sozusagen ein Netzwerk von Bloctracks gibt und die dann untereinander kommunizieren. Und zum Beispiel auch, dass Käufer den HTLC immer bei sich erstellt. Dann hat man dieses Problem mit den private keys nicht mehr.
E: Super gut durchdacht. Ich denke, dass man sich vielleicht noch überlegen kann, ob es nicht sinnvoller wäre, die private-key-Situation dahingehend zu lösen, dass man sich davon etwas löst. Ein Ansatz wäre eine Mischung aus private key und transaction key. Ich habe dann einen private key, der in der Lage ist, sogenannte sub-private keys zu generieren, die ich auch nicht raus gebe. Aber im Notfall hätte ich den fallback auf eine übergeordnete Ebene vom private key. Und den könnte ich dann zum Beispiel wieder notariell irgendwo hinterlegen. Und der wüsste ja noch nicht mal, für was er eingesetzt werden kann, weil dem würde ich ja zum Beispiel nicht sagen, wo er eingesetzt wird. Der hat den zwar bei sich liegen, aber der weiß nicht, wofür er den anwenden kann. Das ist wie wenn du eine Schraube bei dir liegen hast und die eminent wichtig, aber du weißt nicht wozu. Das Problem vom private key ist: Ich weiß, wo ich ihn finde wie ich ihn anwenden muss. Wenn er jetzt irgendwo anders liegen würde und jetzt keinen Zusammenhang hat und ich den Zusammenhang nur in einem Notfall konstruieren kann mit zusätzlichen Informationen, die aber kein Dritter hat, dann ist er per se wertlos. Das ist ein anderer Denkansatz von der Sicherheitsarchitektur her. Die eigentliche Sicherheit des private keys bleibt bestehen und wird noch sicherer gemacht, weil er sozusagen wie unkenntlich gemacht wird, zu wem er überhaupt gehört. Das können dann wirklich nur zwei Leute rausfinden, die den Tresor öffnen. Die Information ist dann nicht mehr an einem Ort, der potentiell komprimiert werden könnte, weil ich theoretisch durch einen Trojaner ausgespäht werden könnte. Dann löst der mir tausend Smart Contract aus.
A: Dann mach ich jetzt beim Tracking an sich weiter. Das funktioniert so, dass die getrackten Daten getimestamped werden (Rohdaten) und dann verschlüsselt über IPFS hochgeladen. Das erleichtert nachher die Verteilung der Daten. Was zusätzlich dazu kommt: Wir stellen eine Blockchain von Tracks her und hinterlegen im aktuellen Track den IPFS hash und das decryption password vom vorherigen Track. Wenn ich den aktuellsten Track hab, kann ich die gesamte Blockchain von Tracks ansehen. Beim Bezahlvorgang am Ende wird der HTLC noch vollständig abgebildet. Wenn der Kunde die

Tracking-Daten verifizieren kann, dann gibt er dem Verkäufer das Preimage aus dem HTLC und der Verkäufer kann dann das Ganze vervollständigen und bekommt sein Geld. Hier ist es so, dass „Ware gegen Preimage" gilt. Da haben wir die Sicherheit für beide Seiten, insbesondere für den Kunden, der seine Daten erst verifizieren kann. Es können jegliche Daten, sei es Tracking oder auch der gesamte Bezahlvorgang, ohne den Prototyp verifiziert werden. Das gilt sowohl für den Kunden, als auch für den Verkäufer. Für die Verifizierung von den gesamten Prozessen in der Lieferkette haben wir keine Abhängigkeit vom Prototyp. Jegliche Information hat der Kunde und der Verkäufer. Hast du noch Fragen dazu?
E: Ne.
A: Dann wäre es super, einen ersten Eindruck von dir zu hören zum Prototyp.
E: Finde ich gut. Sehr funktional, schlank.
A: Wie schätzt du jetzt die Integration von dem Konzept in bestehende Prozesse ein? Darum anfangs die Frage nach dem Drittanbietersystem. Wie schwierig oder einfach wäre das?
E: Du bindest es ja ganz normal ein über eine API (RESTful API). Also ist die Einbindung ja denkbar einfach. Immer vorausgesetzt, dass der einen Integrationslayer hat. Wenn der natürlich keinen Integrationslayer hat, dann hast ein großes Problem.
A: Du hast es vorher schon angesprochen: Siehst du irgendwelche Schwächen oder Limitierungen in dem vorgestellten Konzept?
E: Das ist jetzt zu schnell geschossen. Ich finde es nett, weil es total transparent ist. Man hat das double-spending Problem gelöst, was sicherlich dank dem Ablauf soweit abgesichert ist. Und du hast niemanden, der als Mittelmann agieren müsste. Immer vorausgesetzt, dass du auch entsprechende Blockchain benutzt, wo kein Mittelmann drin ist.
A: Öffentliche Blockchain vorausgesetzt.
E: Das einzige, was ich als generelles Problem für den Smart Contract ansehe, ist: Wenn du den Fall hast, dass die Blockchain tatsächlich zusammenbricht (es gibt kein Mining mehr), dann bist du doch in einem realen Prozess und hast kein Sicherheitsnetz. Dann fällst du sehr tief. Wenn du jetzt als Firma 100000 Smart Contracts laufen hast und irgendwas ist mit Ethereum, dann hast richtig Probleme. Und da ist es meines Erachtens extrem wichtig, dass man sich überlegt, ob sich ein alternatives Konzept für so einen Fall überlegt werden muss. Dann muss ich sicherstellen, dass die Prozesse immer noch ausführbar bleiben.
A: Wie ein fallback letztendlich.
E: Genau. Ein fallback, wo ich aber nicht auf einmal in das doublespending Problem reinlaufe. Aber wo ich trotzdem in der Praxis jemandem, bei dem seine ganze Existenz dranhängt, glaubhaft versichern kann, dass auch in diesem Fall er seine Prozesse wie geplant ablaufen. Man baut immer auf die Sicherheit hin, aber es ist ja der

Normalfall, der der dich normal begleitet. Normalerweise funktioniert ja alles zu 98%. Das heißt, die 98% müssen abgesichert werden, auch wenn was mit den neuen Technologien holpert (zum Beispiel alle Miner streiken). Der Fall ist noch nicht eintreten, vielleicht wird es auch nie eintreten. Aber sagen wir mal, die spielen Deutsche Bahn. Was machst du dann? Da bist du voll angeschmiert mit deinen Smart Contracts. Da ist natürlich die Frage der Intelligenz, zu sagen: Für diesen Fall haben wir ein anderes Handling für die hashes vorgesehen.
A: Zusammenfassend hast du schon den Eindruck, dass der Prototyp Transparenz und Vertrauen schaffen kann?
E: Auf jeden Fall. Sehr gut und super gemacht.

B.3.2 *Expert Interview 2*

A: Wenn du jetzt ein Produkttracking gestalten würdest: auf was soll man da besonders achten und welche Technologien würdest du da bevorzugt einsetzen?
E: Naja es kommt immer drauf an auf das Einsatzszenario. Grundsätzlich: es ist ja stark unterschiedlich. Wenn du zum Beispiel Produkte tracken willst, die ein öffentliches Gut sind, dann muss die ganze Historie von dem Produkt transparent sein. Das heißt, auch öffentlich zugänglich sein. Wenn du jetzt allerdings irgendwie Produkte trackst, beispielweise Produktaustausch zwischen zwei Unternehmen, ist die Frage: Muss diese Information öffentlich sein oder nicht? Auf der einen Seite muss man eben von Fall zu Fall unterscheiden, ob das öffentlich durchsuchbar werden soll oder nicht, das heißt transparent. Das ist auf jeden Fall ein Merkmal. Ein weiteres Merkmal, was auch mit Transparenz zu tun hat: kann man Transparenz erreichen, aber trotzdem die Privatsphäre schützen? Das ist auch ein wichtiges Thema. Stellen wir uns mal vor, wir haben ein Unternehmen, was viele Produkte produziert und der Konkurrent schafft es irgendwie an Zeitreihendaten zu kommen. Da kann er schon irgendwelche Rückschlüsse ziehen auf die Produktionskapazität oder wie auch immer auf andere Dinge. Von der Technologie selbst: wie gesagt, es ist immer anwendungsspezifisch. Es gibt ja neuerdings den Hype um Blockchain-Technologie. Da ist allerdings die Frage, wie kann die überhaupt im unternehmerischen Umfeld eingesetzt werden? Es gibt ja unterschiedliche Technologieansätze bei dem Ganzen. Wie willst du was tracken? Da gibt es ja RFID tags, Bluetooth low energy, irgendwelche Physical Unclonable Functions (PUFs) oder Barcodes oder QR codes. Das ist einfach anwendungsspezifisch. Wo ist was das Beste? Ich mein, PUFs kann man jetzt zum Beispiel auch benutzen, nicht unbedingt als Trackingmerkmal, aber auch als Schutz vor Fälschungen.

A: Produkte müssen teilweise Transportstandards erfüllen oder weitere Bedingungen zum Beispiel auf dem Transportweg. Und wie kann man das am besten realisieren. vor allem die Überprüfung von den Daten zum Beispiel von Sensoren?
E: Also zum einen müssen diese Standards ja irgendwo definiert werden. Da sehe ich schon das erste Problem. Ist das irgendwie ein RFC-Standard, der irgendwie öffentlich zugänglich ist? Oder ISO? Oder ist das nur quasi ein Vertrag zwischen zwei Unternehmen? Wo dann zum Beispiel sagt: Ich bin ein Hotelbewertungsportal. Das geht dann hin zu einem anderen Dienstleister, zum Beispiel ein Hotelbuchungsportal. Und dann muss irgendwie spezifiziert werden: wie sehen meine Daten aus im Datenformat? Das heißt, da ist erstmal die erste Schwierigkeit, diesen Standard zu definieren. Wie das Datenformat aussehen muss: Das muss auf jeden Fall maschinen- und menschlesbar sein im Prinzip, wenn man an die ausgetauschten Daten irgendwie denkt. Zusätzlich sollte es möglichst ein offenes Datenformat sein.
A: Und wenn man jetzt an die Speicherung von den Daten noch denkt und deren Verteilung? Also wenn ich jetzt zum Beispiel irgendwelche Sensordaten habe, die an den Kunden weitergereicht werden sollen. Wie wäre das zu realisieren?
E: Da gibt's ja unterschiedliche Ansätze. Man kann es entweder über eine Schnittstelle bereitstellen, das heißt, wir geben dem Kunden einen Zugang zu unserer Datenplattform. Das heißt, er muss sich dann immer aktiv darum kümmern, dass die Daten bei ihm sozusagen landen. Man könnte aber auch sowas wie ein Peer-to-Peer-Netzwerk mit dem Kunden aufbauen zum einfachen Dokumentenaustausch und so weiter. Und man könnte ein Peer-to-Peer-Netzwerk einfach nutzen. Es hat den Vorteil, dass es eben verteilt ist. Zum Beispiel ein Kunde, ein Zulieferer zum Beispiel, der hat mehrere Standorte. Mit den mehreren Standorten kann eben eine Datei redundant gespeichert werden. Da ist es auch wieder zu überlegen, welche Daten werden verschlüsselt und welche halt nicht beispielweise. Das ist auch ein wichtiger Faktor, wenn wir jetzt irgendwie sagen: es geht um eine NDA zum Beispiel zwischen einem Automobilzulieferer und einem Getriebehersteller. Dann kann die NDA ja jetzt nicht irgendwie öffentlich drinstehen, sondern es sollte verschlüsselt sein, dass nicht jeder das lesen kann.
A: Okay, jetzt hatten wir es gerade eben von Datenplattformen. Wie könnte da die Verwaltung der Zugriffsrechte aussehen?
E: Die Verwaltung der Zugriffsrechte...
A: Oder generell Zugriffsrechte?
E: Es ist ein sehr schwieriges Thema. Da gibt's auch unterschiedliche Modelle. Auf was zielst du da genau ab? Auf die Technologie? Ich mein, man könnte das Ganze zum Beispiel über OpenID machen. Darüber könnte man das zum Beispiel verwalten. Man könnte das

im klassischen, herkömmlichen Sinne irgendwie über so Sachen wie LDAB oder Active Directory theoretisch machen, was aber halt den Nachteil hat, dass das irgendwie alles zentral von uns verwaltet werden muss und das ist nicht wirklich öffentlich einsehbar. Und da ist halt auch die Frage: möchte ich irgendwelche Kundenzugänge bei mir pflegen? Das ist auch irgendwie fragwürdig, finde ich. Deswegen, da sehe ich auf jeden Fall eine Lücke, wie man sowas machen kann. Ich habe auch von approaches schon gelesen, die blockchain-basiert sind. Allerdings sehe ich da bis jetzt noch viele Fragezeichen, vor allem was Skalierbarkeit und so weiter angeht. Beispielsweise ist da ja auch wieder Frage: Wenn man irgendwie ein Unternehmen hat wie Daimler und da würde so eine Software ausgerollt werden. Wir rollen das aus und wenn sich bei Daimler irgendjemand einloggt, wird es jedes Mal in eine Blockchain geschrieben. Da wirst ja theoretisch verrückt. Da müsste irgendwie so ein approach gefunden werden, der ähnlich wie single-signon, also OpenID, funktioniert, aber blockchain-basiert. Warum blockchain-basiert? Es hat den Vorteil, man kann eben hierarchische Strukturen in Smart Contracts abbilden. Das heißt, ich kann sagen, okay, die und die Mitarbeiter (public key) gehören zu meiner Organisation dazu. Und dann kann ich zum Beispiel auch nachgucken: ich hab eine Datei bekommen und da find ich den und den public key drin und kann nachgucken, von welcher Firma war das eigentlich und kann das theoretisch wieder zurückverfolgen.

A: Okay, gut. Nochmal eine allgemeinere Frage: Welche Anforderungen stellst du an Lieferketten generell und deren Abbildungen, losgelöst von irgendwelchen use cases?

E: Also generell ist mir da wichtig, dass versucht wird, das Produkt möglichst lückenlos zu erfassen. Das heißt, dass man eine konsistente Historie von einem Produkt oder von einem Asset eben hat, ob das jetzt irgendwie digital oder physisch ist. Das ist der eine Punkt. Das ist eigentlich für mich das Hauptmerkmal. Und eben dahingegen muss das auch skaliert werden natürlich. Das ist ein wichtiger Punkt, dass die ganze Last, also die Daten [verarbeitet werden.] Nehmen wir an, wir würden die Medikamentenverpackungen tracken oder so, jede einzelne Packung. Wenn du da so 10 Fertigungsstraßen hast, wie viel da pro Sekunde schon durchgehen. Das muss ja auch irgendwo erstmal verarbeitet werden. Es ist wichtig, dass man irgendwie schafft, ein einheitliches Format zu machen. Und in diesem Format sollte es eben halt Möglichkeiten haben, dass es irgendwie lückenlos ist, weil dann können eben die Geschäftsprozessen zum Beispiel intern verbessert werden. Zum Beispiel wird dann erkannt, okay, da und da haben wir irgendwelche Probleme oder brauchen zu lang.

A: Gut. Transparenz, so als neues Schlüsselwort, sollte ja eigentlich generell auch einen hohen Stellenwert in Lieferketten haben. Es hat Vorteile für Kunden und Verkäufer. Trotzdem gibt es da immer wieder Probleme beziehungsweise in der Industrie wird sich dagegen gesträubt größtenteils. Wie

könnte man dennoch die Transparenz erhöhen in Lieferketten?
E: Also die Grundfrage ist ja immer so: Beispielsweise nehmen wir an, wir haben eine Blockchain. Unabhängig von Bitcoin, da siehst du jede einzelne Transaktion durchgehen und kannst nachvollziehen, wer wie welches Geld bekommen hat und so weiter. Und das könnte man ja theoretisch mit Produkten auch. Ich weiß auch, dass das für Unternehmen nicht praktikabel ist und die Leute das auch nicht wollen. Beispielsweise hast du auf der einen Seite Unternehmen, die wollen sich natürlich gegen irgendwelche Rechtsansprüche absichern. Aber wenn sie das selber verbockt haben, dann steht das eindeutig in der Blockchain drin. Das heißt, man muss da irgendwie mehrere Optionen sozusagen machen. Das heißt, sowas wie optionales Zeitstempeln oder sowas von irgendwelchen Daten. Auch wenn wir jetzt gerade versuchen, den Transparenzbegriff runterzuarbeiten. Ich versteh die Wichtigkeit daran, aber ich weiß, dass das viele Unternehmen so sehen als starken Kritikpunkt vom Ganzen. Transparenz kann ja nur gewährleistet werden, wenn sich alle dazu verpflichten. Und wie schaffst du das, dass alle sich dazu verpflichten? Beispielsweise schafft man einen incentive. Das kann dann beispielsweise so aussehen: ich hab jetzt ein Zulieferer und der verkauft seine Produkte an mich. Aber ich will natürlich auch wissen, woher seine Produkte kommen und ob die auch Qualitätsstandard oder irgendwelchen Zertifizierungsstandards entsprechen, ob die korrekt verarbeitet wurden. Und da müsste er mir ja theoretisch die Daten rausrücken. Und da ist halt quasi die Idee, dass man dadurch Transparenz schafft, indem man einfach incentives anbietet. Das heißt, der rückt mit den Daten raus und bekommt dafür Geld. Das ist eigentlich der Hauptgrund, warum er überhaupt auch anfängt, das zu tracken.
A: Wie bist du mit der Blockchain bislang in Berührung gekommen?
E: Das Ganze hat angefangen während meinem Informatik-Studium an der Universität Konstanz, beziehungsweise eigentlich schon früher. Ich hab irgendwann mal 2010 herum überlegt, wie kann man im Internet eigentlich Geld verdienen und bin dann auf das völlig neue Bitcoin gestoßen. Und da hatte ich einfach mal spaßeshalber meinen Rechner ein paar Tage laufen und hab mal gemined und so weiter. Keine Ahnung, wo die Coins jetzt sind. Die liegen jetzt halt irgendwo im Nirvana. Das war so mein allererster Kontaktpunkt, hab mich aber nicht weiter damit auseinandergesetzt, weil ich auch einfach zum damaligen Zeitpunkt (das war sogar noch vor meinem Abitur) nur den Computer [gesehen hab], nichts weiter. Aber mit dem Thema Blockchain habe ich mich nicht weiter mit auseinandergesetzt. Da war Bitcoin für mich nichts anderes als irgendwie PayPal oder so. Das war mein erster Kontaktpunkt. Als es dann bekannter wurde, war dann zum Ende vom Masterstudium, wo ich dann meine Abschlussarbeit bei Professor Gipp (Zweitgutachter) geschrieben hab. Da hab ich mich konkret mit der Visualisierung von Datenhistorien

auseinandergesetzt. Er hat mich darauf aufmerksam gemacht, dass die Daten von Blockchains auch eine Historie haben und das ebenfalls visualisiert werden kann. Und seit November 2016 arbeite ich richtig daran. Da hab ich dann angefangen, einen Forschungsprototypen zu entwickeln, wo jetzt ein Startup draus geworden ist.
A: Okay, in diesem Fall wird da die Blockchain-Technologie eingesetzt und auch mit ihr entwickelt. Dann gehen wir jetzt mal über zur Präsentation von dem Prototypen. Blockchains, Smart Contracts, IPFS, HTLCs und OriginStamp sind bekannt.
E: Ich hätte gerne nochmal eine Einführung in die HTLCs.
A: Kein Problem. Wir haben im Prinzip zwei Parteien, hier Alice und Bob. Person A erstellt den contract, der über einen Smart Contract realisiert ist. Kann dabei dann die Höhe von der Überweisung letztendlich, die vielleicht durch geht oder nicht, spezifizieren. Kann dann noch einen Hashlock (bzw. preimage) spezifizieren und einen Timelock.
E: Wird der Hashlock im Smart Contract hinterlegt?
A: Was in dem Smart Contract hinterlegt wird, ist lediglich der Hashwert, aber mit was der Smart Contract vervollständigt werden kann, ist das Preimage von dem Hashwert, mit dem woraus der Hashwert berechnet werden kann.
E: Wer generiert das Preimage in diesem Fall? Der Verkäufer oder der Käufer?
A: In unserem Fall kreiert das der Prototype und dann wird vom Prototyp aus eine Mail an den Käufer gesendet.
E: Und der weiß im Prinzip ganz genau, sobald das Preimage im Smart Contract eingetragen wurde, dass er das Ding auch wirklich erhalten hat.
A: Genau.
E: Also eine Empfangsbestätigung.
A: Sozusagen, ja. Aber diese Empfangsbestätigung löst dann die Überweisung aus. Das sind die HTLCs. Wir haben drei verschiedene Prozesse im Prototyp: die Bestellung, das Tracken an sich und die Bezahlung. Die Bestellung funktioniert so, dass der Kunde erstmal eine Transaktion an Bloctrack initiiert (nach Kontakt mit Verkäufer). In der Transaktion selber haben wir noch einen Hashwert drin, der sich aus einem von dem Kunden festgesetzten Passwort und der Mail vom Kunden zusammensetzt. Dann kommt der Kunde wieder ins Spiel. Der Kunde übermittelt das Passwort aus der Transaktion an den Verkäufer. Das hat den Sinn, dass sichergestellt werden kann, dass keine Transaktion zweimal benutzt wird. Danach kommt der Verkäufer und initiiert jetzt im Prinzip den HTLC. Er übermittelt an Bloctrack das Passwort, die Mail und den Transaktionshash und das item wird erstellt mit einem Timelock, der wiederum vom Verkäufer festgesetzt ist. Allerdings ist es aktuell so im Prototyp, dass der maximal 14 Tage sein darf. Das wäre so ein Punkt, wo man später variabler gestalten könnte.
E: Kannst du mir einen Anwendungsfall nennen für: wann will ein Verkäufer garantieren, dass das Produkt bei einem Kunden ankommt?

A: Ja es geht nicht um den Verkäufer, es geht um den Kunden wieder. Hier ist der Gedanke, dass der Kunde die Sicherheit hat, dass der Verkäufer den Lieferzeitraum einhält. Aber wenn der Kunde sagt, „ich möchte es in einem Tag erhalten" und es ist einfach nicht möglich, dann hätten wir das Problem, dass der Verkäufer den Prozess schon initiiert hat. Dann läuft der contract aus, was für den Verkäufer ein wirtschaftlicher Totalschaden ist.
E: Verliert er dann alles Geld? Ich mein, wenn es einen Tag zu spät kommt beispielsweise.
A: Theoretisch bekommt er tatsächlich gar nichts, er muss das Produkt aber nicht aushändigen. Die Übergabe vom Preimage aus dem HTLC muss gleichzeitig mit der Übergabe von der Ware sein. Das könnte man dann automatisiert gestalten, dass direkt versucht wird, diesen HTLC zu vervollständigen.
E: Könnte man dann nicht so etwas machen, wie: Ich bin jetzt Automobilhersteller und ich möchte Batterien bestellen von irgendeinem Batteriehersteller. Und dann wird ausgemacht, dass die Lieferung in 14 Tagen läuft, also bis in 14 Tagen ist es da, dass man das wirklich wie einen Vertrag hält, wo dann zum Beispiel direkt eine Konventionalstrafe angewendet wird. Das heißt, nehmen wir an, das Preimage wird jetzt irgendwie zwei Tage zu spät eingelesen, das heißt, dass man irgendwie 15% Nachlass bekommt. Da ist dann halt wieder das Problem: Wie stellst du sicher, dass der Kunde ehrlich ist und der Kunde das Preimage direkt ausliefert und direkt im Wareneingang scannt und nicht erst drei Tage liegen lässt? Wie könnte das unterbunden werden?
A: Das ist eine gute Frage.
E: Vielleicht sind die Daten ja irgendwie gezeitstempelt. Wenn der Typ von der Post die Daten übergibt, dann ist das eindeutig nachweisbar, weil das Event ja da ist. Oder beim LKW-Fahrer von der Logistik mit Tracking-Daten, da ist es ja eindeutig nachvollziehbar, dass das Produkt zu einem gewissen Zeitpunkt an einem gewissen Ort gewesen sein muss.
A: Ja, das geht schon. Nichtsdestotrotz wäre es sinnvoller (einfach für die Sicherheit), das schon so abzuwickeln, dass es Ware gegen Preimage gehandhabt wird. Dann bekommt man dieses Problem nicht. Man könnte schon sagen mit dem Zeitstempel. Aber das ist wieder ein riesiger Prozess, der da angestoßen wird.
E: Ware gegen Preimage seh ich auch so. Aber du musst ja die Person auch unter Druck setzen und sagen „es gibt ja auch noch einen Zeitstempel, wie ich hier vor Ort gewesen bin" und die Konventionalstrafe ist nicht rechtmäßig.
A: Der Kunde bekommt dann die Email von Bloctrack und kann das dann auch alles verifizieren.
E: In der Email steht auch das Preimage drin?
A: Genau. Hier haben wir ein Beispiel von der Form, die der Verkäufer bekommt, um das item und den HTLC zu erstellen. Die Mail, die der Customer bekommt, beinhaltet Preimage, contract ID, Smart Contract Adresse vom

HTLC, Transaktionshash (für das item) und einen Zeitstempel über OriginStamp, der die Verifizierbarkeit sicherstellt, dass der contract erstellt wurde, welcher Transaktionshash benutzt wurde, um folgendem Problem aus dem Weg zu gehen: Wenn der Verkäufer behauptet, dass die Transaktion noch nicht benutzt wurde, kann der Käufer eindeutig nachweisen, dass sie schon benutzt wurde. Dann kommen wir als Nächstes zum Tracking an sich. Das Tracking wird so gestaltet, dass jeder Track, der irgendwie (automatisiert) getracked wird, dass die Daten verschlüsselt in IPFS hochgeladen werden. Zusätzlich, von den unverschlüsselten Daten, wird ein Zeitstempel über OriginStamp erstellt.

E: Und warum wird das jetzt zum Beispiel bei IPFS hochgeladen und nicht über S3 Cloud Storage oder sowas?

A: Weil IPFS den Vorteil der Dezentralisierung hat. Heißt, wir haben einfach unsere Daten und können von überall durch den IPFS hash zugreifen. Sie liegen ja verschlüsselt vor, deshalb ist das kein weiteres Problem. Und zum Beispiel in IPFS haben wir die verschiedenen Knotenpunkte und zum Beispiel hat auch ein Knotenpunkt dann die Möglichkeit zu pinnen. Wenn ich jetzt Kunde bin und weiß, dass die Daten an 100 IPFS hashes liegen, kann ich diese Daten pinnen und die Daten werden dupliziert. Dadurch haben wir die Dezentralisierung und die Datensicherheit. Das ist der Vorteil von IPFS, warum das hier eingesetzt wird. Wir haben die Zeitstempel, die Verschlüsselung von den Daten und wir haben eine Blockchain von den Track-Daten, weil in jedem Track der vorherige IPFS hash und encryption password gespeichert wird und so kann man die ganze Kette betrachten. Wenn ein Hersteller sagt, er möchte irgendwelche Trackingparameter, die firmenintern sind, nicht preisgeben, dann kann man die noch zusätzlich verschlüsseln und hat die Datensicherheit dann weiterhin gegeben. Als letztes zum Payment-Prozess (Bezahlvorgang): Da haben wir nur abgebildet, was der HTLC eigentlich macht. Der Verifikationsprozess kann zusätzlich komplett ohne Bloctrack durchgeführt werden, sowohl vom Bezahlvorgang als auch vom Tracking an sich.

E: Um eine Trackverifikation durchführen zu können, muss ich auch im gleichen Netzwerk drin sein, wo die Daten herhoben sind. Es gibt ja auch die Möglichkeit, dass ich ein IPFS-Netzwerk nur mit meinen Partnern erstell. Da gibt's bestimmt auch Konfigurationsmöglichkeiten und/oder ich nehm einfach IP tables und block einfach alle IPs, außer die von meinen Partnern. Dann haben wir Eautomatisch nur unter uns sozusagen ein Netzwerk. Das heißt aber, um das verifizieren zu können, brauch ich Zugriff zu diesem Netzwerk.

A: Genau, hier ist aber davon ausgegangen worden, dass es das öffentliche Netzwerk ist. Da haben wir den Vorteil, dass es auch relativ groß ist.

E: Das kann ja groß sein, aber es pinnt ja eh kein Mensch, wenn die Daten für ihn nicht relevant sind. Das ist eh kein Grundproblem dieser Technologie. Wenn das irrelevante Daten sind (unternehmensspezifisch und verschlüsselt), dann liegen die halt einmal vor im ganzen Netzwerk. Warum soll ich die auch reproduzieren.

A: Da gäbe es aber die Möglichkeit, dass, wenn man ein Netzwerk zum Beispiel von 50 Unternehmen hat und man verpflichtet sich, dass man so eine node bereithält und dass man dementsprechend die Daten von anderen repliziert.
E: Oder man hat halt einen Hersteller, der mehrere Filialen hat und dann hast du automatisch dadurch die Verteilung.
A: Genau, das erhöht die Datensicherheit extrem gegenüber herkömmlichen Datenbanken, die auf irgendwelchen zentralen Servern laufen.
E: Daten aus IPFS kann ich ja eh nicht verarbeiten (langsam), deshalb müsste ich die Daten, wenn ich sie verarbeiten möchte, in meine lokale Datenbank sperren. IPFS hilft im Prinzip nur, um Daten halt zu tauschen und um zu verteilen. Aber schlussendlich müssen diese Daten trotzdem in der Datenbank vorliegen aus Performancegründen.
A: Ja, genau. Jetzt kommen wir kurz zum letzten Teil. Dein erster Eindruck vom Prototyp?
E: Es ist natürlich schwierig, weil ich das Ganze noch nicht durchgeklickt hab, aber man merkt, dass da viel Gedanken gemacht wurden. Wo ich noch ein bisschen Schwierigkeiten hab oder was ein generelles Problem ist, mit dem man irgendwie kämpfen muss in Zukunft, dass man es schafft, dass Leute außerhalb von Informatik mit so Buchstaben- und Zahlenketten umgehen können; mit hashes hantieren können. Es ist schon abschreckend, wenn du einfach nur einen Datensatz hast, der nur aus Buchstaben und Zahlen besteht. Das ist auf jeden Fall ein Punkt. Was mich noch interessiert: Du hast ja den Prototypen entwickelt. Wie kriegst du die Daten da rein und wie trackst du die?
A: Da gibt's noch eine App, die trackt.
E: Das funktioniert dann einfach über Barcode oder QR code?
A: Genau, der QR code wird gescannt.
E: Also im Prinzip hast du einfach so ein Tracking-Protokoll entwickelt, aber nicht ein Datenerfassungsprotokoll bzw. Sensorprotokoll. Was danach passiert sozusagen.
A: Genau, ich bekomm getrackte Daten rein und verarbeite die dann weiter.
E: Ein Punkt, den wir vorher schon irgendwie angesprochen haben, war mit der Skalierbarkeit. Wie sieht es denn da aus? Ist die gewährleistet oder was gibt's denn da noch offene Punkte? IPFS hash of last track: Ist das dann im Smart Contract drin oder in einer Datenbank?
A: Das ist aktuell so, dass das Tracking über den Prototyp läuft. Es gab mehrere Gründe das so zu machen, vor allem, weil es zu Präsentationszwecken so relativ gut zu gestalten war und das Gesamtsystem gut zu präsentieren.
E: Ich finde das auf jeden Fall gut, das Protokoll. Über die Smart Contracts und so weiter kann man das eben nachvollziehen, wer hat was bestellt. Und mit der Regel „Ware gegen Preimage", wird dann quasi die Empfangsbestätigung wird sichergestellt. Das heißt, der seller weiß, dass sein Produkt beim Kunden angekommen ist. Durch den Einsatz der unterschiedlichen Technologien ist das ziemlich flexibel

das Ganze. Wo ich noch eine große challenge seh, ist, auf der einen Seite die Unternehmen so weit zu bringen, auf öffentliche Blockchains auch zu vertrauen. Ich habe den Eindruck gewonnen, dass die meisten das lieber in einer privaten Blockchain machen wollen, aber dann frag ich mich halt, was das bringt. Dann kann ich es gleich bei mir in eine lokale Datenbank reinklopfen. Das ist das größte Problem. Ich find cool, dass man die Daten austauschen kann über IPFS, dass das berücksichtigt wurde und dass das Payment irgendwie an eine Kondition drangebunden ist. Das heißt nicht, dass beispielsweise, wenn ich mir bei Ebay was kauf und überweis das Geld, ich die Ware nicht bekomme. Das ist auf jeden Fall aus Käuferschutzperspektive ist das ziemlich cool. Wo ich in Zukunft noch richtig viel Arbeit seh ist das Ganze mit Authorizaton, also wer bekommt welche Daten, wie kann man irgendwie das sinnvoll abbilden, wie kann man sich authentifizieren mit Blockchain, solche Geschichten.

A: Es gibt sicherlich noch einiges an Optimierungsbedarf. Siehst du generell eine komplette Limitierung, was das gesamte System gefährden kann?

E: Naja, Limitierung ist das Internet. Das heißt, eine Grundvoraussetzung ist, dass alle Beteiligten Internetzugriff haben, was in Deutschland mittlerweile einigermaßen funktioniert, aber auch nicht so wirklich. Das ist für mich ein Problem. Ein weiteres Problem ist, aber da wird es halt sehr speziell, dass man schauen muss, wo man das System idealerweise einbettet. Stell dir vor, man trackt irgendwas auf Schiffen und jetzt schippern die auf dem Atlantik rum. Die haben da kein Internet, beziehungsweise die haben so Internet wie wir '95 hatten. Und da können die nicht einfach diese Daten so einfach übertragen. Da sieht das Tracking dann zum Beispiel wieder ganz anders aus. Die können vielleicht mehrmals am Tag eine Zeichenkette von 64 Zeichen übermitteln, aber mehr halt auch nicht. Das ganze System muss halt in einen Kontext gesetzt werden, finde ich. Das ist so der Faktor, der Kontext einfach. So allgemein, wenn man das allgemein anschaut: okay, das kann funktionieren, aber da sieht man auch viele Limitierungen. Was halt irgendwie wichtig ist, ist halt Internet und die Daten, die man erfasst und die Trackingdaten, dass die sicher und vertrauenswürdig sind. Wo ich noch weitere challenges sehen würde, ist die Architektur von dem Ganzen. Blockchain ist ja ursprünglich da, um Mittelsmänner aus dem Weg zu räumen. Warum haben wir dann diese drei entities: Verkäufer und Käufer und in der Mitte steht noch Bloctrack, was ja eigentlich die Blockchain selbst sein sollte im Prinzip. Und da wäre die Idee, ob das irgendwie ein Open-Source-Protokoll werden soll, das jeder benutzen könnte oder soll das ein Service sein wie zum Beispiel Amazon, der gehostet wird.

A: Wenn man jetzt den Gedanken noch weiterverfolgt: wenn man das später wirklich mal integrieren möchte in irgendwelche Firmen und dann da Anbindungen sucht, müsste man unter Umständen die gesamte Infrastruktur umstellen. Und nur weil man das Tracking oder den Bezahlvorgang umstel-

len möchte, ist der Aufwand extrem hoch und die Hürde ist extrem hoch. Die Wahrscheinlichkeit, dass das jemand umsetzt, ist sehr niedrig. Und da war der Gedanke, dass es eventuell einfacher ist, als Drittanbieter wirklich anzubieten, um den Unternehmen die Integration von dem Service einfacher zu gestalten.
E: Da musst du aber direkt mit der These ran und direkt mit incentives zu arbeiten. Wenn man daraus eine Firma machen würde, dann wäre das Geschäftsmodell, dass diese Technologie bereitgestellt werden würde und dass wir das Incentive-Modell pflegen würden.

B.3.3 *Expert Interview 3*

A: Dann hätte ich erstmal ein paar einleitende Fragen und zwar: wie würdest du Produktverfolgung gestalten und welche Technologien würdest du einsetzen?
E: Jetzt ganz allgemein oder geht es um spezielle Produkte?
A: Ganz allgemein.
E: Produktverfolgung gestalten ist natürlich ein schwieriges Thema. Ich meine, da kommt es sicherlich zum einen auf die Produkte selber an, zum Beispiel auf die Herkunft, auf die Lieferkette und so weiter. Es ist sehr sehr schwierig das pauschal zu sagen, weil jede Branche, jedes Produkt, jedes Gebiet hat natürlich unterschiedliche Anforderungen an ein Produkttracking und daher pauschal das jetzt zu sagen ist schwierig. Wenn du mir jetzt vielleicht ein konkreteres Beispiel nennen könntest, irgendein Produkt oder irgendeinen Bereich, dann kann man das natürlich etwas spezifizieren.
A: Ja ok. Wenn man jetzt zum Beispiel davon ausgeht, dass ein Unternehmen ihre Produkte verschickt mit Paketen, sei es in der Metallverarbeitung irgendwelche Zahnräder zum Beispiel, fällt mir jetzt spontan ein. Wie gestaltet sich die Produktverfolgung an sich und welche Technologien würdest du da eventuell einsetzen?
E: Ok. Wenn man das spezifiziert, sagen wir jetzt mal Zahnräder, dann ist es so: Am Anfang ist es ganz ganz wichtig sich einen Lebenszyklus zu überlegen. Woher kommt das Ganze (Herkunft)? Es ist wichtig, sich erstmal zu überlegen: Wie wird das Eisenerz abgebaut? Wo wird es abgebaut? Unter welchen Bedingungen? Wie wird es dann zu mir transportiert (das Rohmetall vielleicht, weil ich die Zahnräder gieße)? Dann ist es wichtig, wie ich die selber verarbeite und dann kommt natürlich der nachgelagerte Prozess: die Transportwege, zum Beispiel Kunden (zum Beispiel Windkraftwerk). Und dort ist natürlich dann auch wichtig, ja, wie ist die Nutzung, wie ist die Rückverfolgbarkeit, wenn zum Beispiel Schaden auftritt und dann später nach der Nutzung. Was passiert dann? Gibt es irgendwelche Rücknahmekonzepte? Gibt es irgendwelche Anforderungen von mir selber (dass ich beispielsweise versuch das Material zurück-

zugewinnen)? Und auf Basis dieser Informationen, also dieses Lebenszyklus, den jeder definieren sollte, kann er natürlich dann auch spezielle Anforderungen definieren. Angefangen von irgendwelchen, vielleicht auch nur eine Nummer auf dem Element bis hin natürlich zu individuellen kleinen Chips, sei es RFID, sei es irgendwelche NFC Chips, was auch immer in dem Bauteil selber, um dann auch diese Wege nachverfolgbar zu machen. Also das heißt: jede Station wird dann sozusagen dokumentiert, wird dort gespeichert und dadurch hab ich natürlich die Möglichkeit, über den Lebenszyklus auch die Informationen zu tracken, zu sagen, okay, keine Ahnung, 2015 war eine Wartung, 2017 gabs einen Ersatz von dem Bauteil, weil es defekt war, 2019 wieder eine Wartung, also wirklich das auch sauber dokumentiert. Und wie gesagt, es kann von einer einfachen Nummer, die unique ist, also individuell vergeben wird bis hin zu irgendwelchen Chips, die Dateninformationen speichern und irgendwo zentral ablegen oder dezentral (Blockchain, Cloud oder wo auch immer), oftmals dann auch sozusagen revisionsicher abgelegt werden. Das heißt dann, ich kann zum Beispiel über lange Jahre das Ganze nachverfolgbar machen. Und das ist natürlich immer so ein Vorteil an einem Chip: da kannst du ja Informationen speichern, die normale Nummer, die gibt natürlich nicht viel her. Das ist vielleicht das Herstellungsjahr, Herstellort, vielleicht sogar wer es gefertigt hat, aber das wars dann auch schon.

A: Und das Speichern von den Daten: Welche Anforderungen sollte die Speicherung erfüllen? Zum Beispiel wie effektiv sollte das gestaltet werden und welche Anforderungen an das Speichern an sich gibt es da?

E: Gut, also auch hier ganz einfach gesagt. Am Anfang die Datenbank, oder noch rudimentärer die Excel-Datei, wo alle Nummern hinterlegt sind. Das heißt, ich hab zum Beispiel meine verschiedenen Seriennummern, die ich jedem Bauteil vergebe. Das ist auch gefordert teilweise, zum Beispiel vom Qualitätsmanagement, dass ich sag ich hab hier Nummer 1,2,3,4,5, die leg ich in einer Excel-Tabelle ab und notiere mir einfach die Nummer steht für Fertigungsdatum, die Fertigungsbedingungen, vielleicht die Legierung was ich da mit drauf schreib und so weiter. Und so kann ich es entweder in eine Excel-Datei speichern oder natürlich in eine Datenbank (SQL, MySQL, wie auch immer), um dann eben diese Informationen auch mehreren Personen, die da Zugriff haben sollen, zugänglich zu machen. Das ist die einfachste Lösung. Dann kann man ja überlegen, wenn es bisschen komplexer wird zu sagen, man kann auch eine Plattform nutzen und die Daten dort hinterlegen. Dahinter steht natürlich wieder eine Datenbank, kann ja auch eine Blockchain oder ein P2P-Netzwerk sein. Die Daten werden dort gespeichert. Vorteil ist natürlich einer Plattform, dass ich verschiedene Informationen zusätzlich hinterlegen kann, das heißt zum Beispiel, wenn ich jetzt nur eine kleine Nummer hab, dann kann ich ja trotzdem sagen: im Jahr 2015 hab

ich nur die Legierung oder nur die Lieferanten und so weiter. Das kann ich dann alles dort hinterlegen. Man könnte auch Zugriffsrechte vergeben, was auch wichtig ist. Jemand, der nur die Wartungen durchführt, der bekommt nur bestimmte Zugriffsrechte, dass er nur sieht, wann die letzte Wartung war und wann kommt die nächste Wartung oder auch zum Beispiel der Hersteller selber, der braucht alle Informationen. Der sieht dann alles. Und so ist es natürlich auch je nach Bauteil, je nach Anforderung ganz ganz unterschiedlich, wie so eine Datenspeicherung auszusehen hat. Wichtig ist natürlich, dass die Daten mindestens über den Lebenszyklus, meistens auch darüber hinaus, auch gespeichert werden und dort hinterlegt werden. Früher gab es ja immer die Vorgabe der Aktenablage mindestens 10 beziehungsweise 30 Jahre und das am besten im Keller archiviert auf Papier. Heute mit der Digitalisierung ist das alles kein Problem mehr. Das Hauptproblem ist meistens, wenn externe Lösungen verwendet werden und der Hersteller da eigentlich keine Macht hat. Schlimmstenfalls fällt der Server aus, die Daten werden nicht redundant gespeichert (Redundanz ist sicher auch ein Thema) oder zum Beispiel der Provider von der Lösung meldet Insolvenz an und schlimmstenfalls sind die Daten weg. Also das heißt, immer wirklich diese Datenspeicherung muss gegeben sein in einer redundanten Art und Weise. Dann Revision sicher und dann sicherlich auch über mehrere Jahre auch nachverfolgbar sein und dort auch hinterlegt sein.

A: Wunderbar. Dann gehen wir mal zur nächsten Frage. Und zwar Produkte müssen ja teilweise Transportstandards oder Bedingungen einhalten. Wenn man zum Beispiel an die Medizin denkt, dann müssen irgendwelche Temperaturen beim Transport eingehalten werden. Hattest du schon einmal einen derartigen Fall? Unabhängig davon: Wie würdest du die Überprüfung der Daten realisieren?

E: Gut, also ich kenne es hauptsächlich wir haben einen Kunden, die machen Blutproben (Entnahme von Blutproben) und die untersuchen mehrere tausend Proben pro Tag. Und die haben es so gelöst, weil sie natürlich sagen "Transportwege sind immer so ein Risiko", dass die möglichst kurze Transportwege realisieren. Das heißt, wirklich beim Kunden vor Ort sitzen (Kunden in dem Fall sind meistens Krankenhäuser oder Ärzte). Das heißt, ein Arzt hat irgendwie eine kritische Blutprobe und die haben es zum Beispiel so gelöst: eigene Transportunternehmen oder wenn es wirklich heikel ist transportieren die es auch selber. Da wird jetzt nicht groß Temperatur überwacht oder sonstiges, weil es einfach so kurze Transportwege sind (teilweise 10,15 Minuten) oder beim Krankenhaus selber per Rohrpost. Die Laborantinnen meistens übernehmen die Probe und untersuchen die dann gleich. Also das kann natürlich eine Möglichkeit sein, die Transportwege so kurz wie möglich zu halten, gerade bei kritischen Transporten. Im Lebensmittelbereich ist es natürlich bei Weitem nicht so kritisch. Da muss einfach nur eine ununterbrochene Kühlkette gege-

ben sein. Aktuell passiert das ja relativ klassisch. Das Fahrzeug selber ist gekühlt und das war es dann. Da gibt es keine große Überwachung oder sonstiges. Ich weiß, worauf du hinauszielst. Du zielst natürlich auf die Live-Überwachung ab. In der Live-Überwachung gibt es zwar schon ein paar Ansätze, aber das ist alles noch nicht wirklich umgesetzt. Klar, man kann natürlich irgendwo Sensoren einbinden, die live tracken lassen und dann zum Beispiel in einer Blockchain, was immer wieder auch diskutiert wird, dort auch abspeichern. Ich fand es nur sehr interessant (ich hab ja auch im Blockchain-Bereich promoviert) und ich hab mit jemandem gesprochen, der in Blockchains für Industrie promoviert. Er hat mir gesagt (er ist schon fast fertig), dass er bis heute keine Lösung gefunden hat, in einer Blockchain, was Vorteile hat gegenüber einer klassischen Serverspeicherung. Klar, natürlich, wesentlicher Vorteil könnte Fälschungssicherheit sein, wenn man Live-Tracking macht und versucht, die Daten auch hier wirklich fälschungssicher abzuspeichern. Aber grundsätzlich geht es darum, irgendwo die Daten zu speichern und wie das Ganze durchgeführt wird und umgesetzt wird bleibt eigentlich jedem selber überlassen. Also klar, es gibt irgendwelche Ansätze, dass man die Sensoren einbindet. Zum Beispiel jede Sekunde oder jede halbe Sekunde versucht man, Datenlog zu machen. Was da auch wichtig ist und was da auch vergessen wird: theoretisch, wenn ich was fälschen will kann ich es auch fälschen. Was weiß ich, ich hab eine Kühlbox, hab da einen Temperatursensor drin und jetzt theoretisch fällt mir meine Kühlung aus dann leg ich halt einen Kühlakku drauf, was mir trotzdem diese Temperatur vorspielt. Oder ich pack das Ding schnell in Kühlschrank oder ins Gefrierhaus. Es gibt nie eine hundertprozentige Fälschungssicherheit. Vielleicht von der Software eher, ja, aber irgendwo ist immer eine Schnittstelle zwischen Hardware und Software und spätestens diese Schnittstelle kann ich manipulieren, wenn ich das will. Und jemand der sich auskennt, der kann das auch unerkannt tun. Es ist immer die Motivation: Warum will ich fälschen? Warum will ich irgendwas manipulieren? Also Ansätze gibt es da sicherlich.

A: Jetzt mal noch eine generellere Frage. Welche Kosten fallen durchschnittlich bei einem Produkt nur für dessen Nachverfolgbarkeit an im Verhältnis zu dessen Wert?

E: Kann ich dir gar nicht sagen. Wüsste ich auch gar nichts dazu, weil ich in der Lieferbranche nicht so drinstecke.

A: Okay. Wir haben generelle use cases durchgesprochen. Jetzt eine allgemeinere Frage: Welche Anforderungen so generell würdest du sagen soll man an Lieferkettenprozesse stellen und deren Abbildung? Generelle Merkmale?

E: Ganz einfach: die Transparenz. Die fehlt heute immer noch. Einige versuchen die Transparenz zu erhöhen mit irgendwelchen Herkunftsnachweisen. Aber das machen bei Weitem nicht alle. Ich mein im Supermarkt, kauf mal einen MSC-zertifizierten Fisch, dann hast du irgendwo ein Herkunftslabel. Dann kannst du dir vielleicht anschau-

en, der Fisch kommt aus Aquakultur aus Norwegen, aber du hast eigentlich keine Ahnung, wie der Transport durchlaufen ist, wo genau zum Beispiel dann die Farm liegt, weil du hast vielleicht ein Gebiet, was dir angegeben ist, wann wurde der Fisch irgendwo gefischt und geschlachtet (ausgenommen) usw. und es fehlt einfach die Transparenz nach wie vor. Sie wäre da, aber bewusst entscheiden sich natürlich ganz viele dagegen. Selbst große Biolabels wie Demeter oder Alnatura oder wie auch immer. Die wollen gar nicht so richtig ihre Prozesse transparent machen. Zum einen natürlich aufgrund von Wettbewerbssituationen, weil es andere ähnlich machen könnten oder natürlich auch, weil sie nicht wollen, dass sie sich angreifbar machen. Also, nur zum Beispiel, ich hatte jetzt einen Bericht gesehen von Frosta, die machen zum Beispiel Pfannengemüse und Frosta selber baut irgendwo in Sachsen an. Und dann gibt es so viel Untermarken, wie zum Beispiel von Rewe, von Penny, von irgendwo anders und alle Untermarken haben genau das gleiche Gemüse. Der einzige Unterschied ist die Gewürzmischung, aber ansonsten ist das das gleiche Gemüse. Meistens sind diese No-Name- oder Eigenprodukte von Rewe, die auch durch Frosta produziert werden, sind vom Preis her halb so teuer. Aber es ist kein Qualitätsverlust. Aber der Endkunde, der weiß es nicht mal. Der weiß nicht, dass zum Beispiel Frosta-Produkte selber oder auch No-Name-Produkte vom gleichen Hersteller sind. Das sieht er vielleicht, wenn er sich anschaut "produziert von"(steht meistens drauf) und nebeneinanderlegt und vergleicht. Aber schon da fängts an. Also selbst den eigenen Herstellern fehlt die Transparenz. Frosta will natürlich gar nicht, dass ein Endkunde weiß, dass das Rewe-Produkt jetzt das Gleiche ist wie das Frosta-Produkt, weil vielleicht kommt er dann auf die Idee, nur noch das günstige zu kaufen, weil die Qualität und das Anbaugebiet gleich ist. Das ist das Hauptproblem, dass die Transparenz immer noch nicht gegeben ist und bewusst auch nicht gegeben wird.

A: Okay. Das greift gerade in die nächste Frage mit ein, und zwar: Welchen Stellenwert hat Transparenz und Vertrauen gegenüber Kunden in Lieferkettenprozessen? Relativ hoch also?

E: Ja, genau richtig. Das ist meiner Meinung nach das höchste Gut. Selbst Aldi fängt an, irgendwelche Alnatura- und Demeter-Produkte einzuführen. Warum? Weil das die Verbraucher fordern. Die wollen keine Chemikalien in ihren Lebensmitteln, die wollen keine E-Stoffe mehr und keine Zuckerzusätze mehr. Die wollen einfach transparente Produkte. Und das ist eben immer noch ein Problem, dass die Transparenz nicht gegeben ist. Und da müssen die Hersteller einfach ansetzen und müssen auch umdenken, auch überlegen: Wie kann ich meine Produkte so transparent gestalten, vielleicht nicht alle Sachen. Das ist immer so dieser schmale Grat zwischen Transparenz und alles verraten bis hin zu irgendwo zu sagen ökay ich gebe zwar meine Hauptlieferwege an und meine Lieferanten an und so weiter", aber

hab dadurch nach wie vor noch irgendwo eine Firmenvertraulichkeit. Also nur als Beispiel: wir haben jetzt einen großen Kunden, die sitzen in der Schweiz und die machen für Nespresso das Aluminium, die Kapseln. Und selbst im Unternehmen selber haben die Mitarbeiter eigentlich gar keine Ahnung, wo das Material herkommt. Die wissen zwar schon ökay, ich kauf jetzt irgendwo Aluminium ein". Aber das war es dann auch schon. Ich kenne meine Lieferanten, aber ich weiß eigentlich gar nicht: wo kommt mein, zum Beispiel, Bauxit her? Wie wurde das abgebaut? Unter welchen Bedingungen? Selbst die Hersteller selber von dem Material wissen gar nicht so richtig über die Lieferkette hinweg, wo die einzelnen Rohstoffe herkommen. Also das fehlt völlig. Es geht vielleicht zu Tier-1-Lieferanten, sozusagen die Erstlieferanten vor mir. Aber was da dahinter passiert, das wissen die nicht, da haben die keine Nachverfolgbarkeit. Deswegen fehlt einfach die Transparenz.

A: Jetzt hab ich es schon herausgehört: in diesem Fall werden bei euch die Lieferkettenprozesse auch selber entwickelt?

E: Ja.

A: Gut. Ich hab das schon auf eurer Website gesehen: ihr kommt auch immer wieder in Berührung mit der Blockchain-Technologie. Und wie ist da das Interesse beziehungsweise wie oft arbeitet ihr mit der Blockchain? Wie ist da das Interesse generell von den Unternehmen da?

E: Interesse ist sehr hoch, aber Umsetzung geht sehr gegen null. Es gibt sehr viele Kunden, die sich dafür interessieren, weil es eine neue Technologie ist. Es gibt aber sehr wenige, die das verstehen und es gibt noch weniger, die das dann umsetzen. Hauptproblem ist einfach, dass gerade deutsche Unternehmen, selbst bei der Cloud, die ja schon seit Jahren auf dem Markt ist, bei irgendwelchen Online-Lösungen usw. sehr risikobewusst sind. Die haben keine Lust auf Risiken, die haben keine Lust auf neue Lösungen. Mach ich ja schon immer so, warum soll ich meine Prozesse anfassen, warum soll ich was Neues integrieren. Deswegen informiert man sich immer, man bleibt am Ball, aber umsetzen: sehr, sehr selten. Also wie gesagt, lieber es ist ein Excel-file als eine Cloud-Lösung geschweige denn als eine Blockchain-Technologie oder KI oder Machine Learning. Es sind halt eigentlich alles neue Technologien, die sehr bizarr sind. Die Unternehmen bleiben informiert, die schauen sich das an. Wir haben auch Newsletter zur Digitalisierung. Da kann man nachverfolgen, wer wo wie hin klickt. Und gerade solche neuen trendigen Themen werden immer gern gelesen, aber in der Umsetzung fehlt es dann einfach. Weil viele einfach diese "German Angst"haben. Viele haben Angst, neue Technologien einzuführen und denken ës ist ein riesen Aufwand, ich muss alles umkrempeln und schlimmstenfalls verliere ich wertvolle Mitarbeiter, weil die dann nichts mehr zu tun haben". Es sind eigentlich eher Angstfaktoren oder Risiken als Chancen, die die Unternehmen sehen.

A: Gut, das war schon sehr informativ. Jetzt würde ich kurz meinen Prototypen, den ich im Zuge meines Bachelor-Projekts realisiert hab oder entwickelt hab, vorstellen und dann hätte ich da noch ein paar Fragen dazu. OriginStamp ist dir bekannt?
E: Ja.
A: IPFS hab ich auch noch verwendet. Sagt dir das auch was?
E: Ja.
A: Dann noch HTLCs. HTLCs sind im Prinzip über einen Smart Contract realisert. Dabei kommt ein Vertrag zwischen zwei Parteien zustande. Person A kann dann, wenn er oder sie den Vertrag erstellt, einen Hashlock (Preimage) und einen Timelock spezifizieren. Heißt, der Hashlock ist wie ein Passwort und der Timelock beträgt zum Beispiel zwei Tage. Dann passiert folgendes: Wenn zum Beispiel nach zwei Tagen der Hashlock (Preimage) noch nicht an Person B übermittelt wurde, läuft der Vertrag sozusagen aus und es passiert mit der angegebenen Menge an Geld nichts. Wenn jetzt aber Person A entscheidet ökay, ich geb jetzt Person B das Passwort", dann kann Person B den Vertrag vervollständigen beziehungsweise diese Zahlung anfordern und bekommt dann den vorher spezifizierten Betrag von Person A. Der Sinn ist der, dass Person A die Sicherheit vom Hashlock hat, sprich: Person B muss zuerst das machen, was Person A möchte und erst dann bekommt Person B den Hashlock. Der Timelock verhindert eine Endlosschleife, damit das Geld nicht irgendwo im Vertrag hängen bleibt. Das hab ich in meinem Prototypen auch so abgebildet. Ich bin davon ausgegangen im Prototyp, dass es immer zwei Parteien gibt: Kunde und Verkäufer. Dann hab ich das Ganze in den Bestellvorgang, das Tracking und den Bezahlvorgang untergliedert. Es ist ein sehr genereller Ansatz und es ist nicht auf einen bestimmten use case beschränkt. Die Bestellung funktioniert so: Bloctrack heißt mein Prototyp, der als Drittanbietersystem modelliert ist. Dann fängt der Kunde, indem er beim Verkäufer etwas bestellt. Dann passiert folgendes: Der Kunde bekommt den Preis vom Verkäufer und der Kunde überweist an das Konto von Bloctrack über Ethereum diese Menge an Geld. Der Kunde inkludiert in die Transaktion einen Hash-Wert von einem frei gewählten Passwort und seiner Mail-Adresse. Folgendes passiert dann: Das Geld ist dann bei Bloctrack. Als nächstes kommt der Verkäufer ins Spiel. Er bekommt vom Kunden das Passwort von der Transaktion. Das hab ich so modelliert, weil das Passwort, das zusammen mit der Email-Adresse hinterlegt ist, soll sicherstellen, dass der Verkäufer keine anderen Transaktionen für sich abziehen kann. Der Verkäufer kontaktiert den Bloctrack (request) und schickt den Transaktionshash, Passwort vom Kunden und Mail-Adresse des Kunden mit. Dann wird der HTLC zwischen dem Verkäufer und dem Kunden erstellt. Der Sinn dahinter ist der, dass der Bezahlvorgang transparent ist und sowohl für den Kunden und für den Verkäufer abgesichert ist. Der Verkäufer kann dann auch den Timelock spezifizieren (aktuell bei Bloctrack bei höchstens 14 Tagen abgeriegelt). Länger als 14 Tage darf der Verkäufer nicht brauchen, das Produkt an den Kunden zu transportieren. Im Tracking selber verschickt der Verkäufer zum Beispiel das Paket und ein Tracking über irgendwelche Senso-

ren beispielsweise beginnt. Du hast vorher ja auch schon gemeint, dass diese Vorteile der Blockchain immer bisschen fraglich sind, was die im Tracking wirklich zu suchen haben. Es gibt ja ganz viele Ansätze, die einfach die kompletten Tracking-Daten in Blockchains speichern, was natürlich nicht performant ist und noch weitere Probleme mit sich bringt. Und hier kommt jetzt OriginStamp ins Spiel, weil was ich jetzt mache ist, dass die Tracking-Daten getimestamped über OriginStamp und auf IPFS verschlüsselt hochgeladen. Und bei IPFS haben wir den Vorteil, durch den dezentralisierten Speicher, dass die Freigabe und die Erreichbarkeit der Daten sichergestellt wird. Was zusätzlich noch passiert, ist, dass die Tracking-Daten als eine Art Blockchain von Tracking-Daten vorliegen, gespeichert in IPFS. Wenn ich jetzt zum Beispiel den letzten Tracking-Datensatz hab (unverschlüsselt), steht der letzte IPFS Hash vom vorherigen und das dazugehörige encryption password drin. Und so kann ich mich bis zum Tracking-Ursprung vorarbeiten und habe Zugriff auf die gesamten Tracking-Daten. Wenn man jetzt möchte und als Verkäufer nicht möchte, dass nicht alle Daten preisgegeben werden, kann man zusätzlich noch Trackingparameter zusätzlich verschlüsseln. So stelle ich die Integrität der Daten sicher und die Unveränderbarkeit der Daten durch OriginStamp und das Timestamping. Am Ende, wenn das Paket versendet wird an den Kunden und der Kunde bekommt das dann, kann der Kunde die Tracking-Daten vom Verkäufer verlangen und bekommt diese. Diese kann er verifizieren, zum Beispiel automatisierte Sensordaten wie Temperatur. Klar gibt es immer die Möglichkeit der Manipulierbarkeit. Letztendlich die Daten, die nachher vorliegen, sind verifizierbar durch den Timestamp bei OriginStamp. Auf jeden Fall kann der Kunde die Daten verifizieren und wenn alles im gewünschten Zeitrahmen passiert ist, schickt er das Preimage vom contract an den seller. Nachtrag: Wenn der HTLC erstellt wird, wird dem Kunden jegliche Informationen rund um den HTLC bereitgestellt, damit er die volle Kontrolle über sein Geld behält. Der Verkäufer kann letztendlich mit dem Preimage des Hashlocks den Bezahlvorgang beenden beziehungsweise vervollständigen und bekommt sein Geld. Ansonsten kann es sein, dass das Timelimit nicht eingehalten wird und der Kunde wiederum kann einen request an den contract schicken und bekommt sein Geld wieder. Worauf ich Wert gelegt habe, ist, dass die Verifikation von den Vorgängen in der gesamten Lieferkette ohne Bloctrack durchgeführt werden kann (Timestamps, HTLCs, etc.). Der Fokus wurde auf die Vertrauensoptimierung zwischen Kunde und Verkäufer gelegt und auf die Transparenz. Dabei hab ich versucht, die positiven Eigenschaften der Blockchain zu integrieren und die negativen Eigenschaften (Performance, Skalierbarkeit) zu überwinden (nur die Timestamps werden übermittelt). Zudem sind die Daten dezentralisiert gespeichert und die Verifikation ist komplett dezentralisiert. Hast du erstmal noch Fragen?

E: Soweit verstanden.

A: Gut, dann kommen wir zum letzten Teil. Ich hab noch ein paar Fragen zum Prototyp. Was ist dein erster Eindruck, wenn ich dir das so erläutert hab?

E: An sich spannende Ansätze. Zwei Lösungen, einmal der ganze Zahlungsverkehr und das ganze Tracking. Letztendlich muss beides auch zusammen funktionieren. Aber es sind trotzdem zwei grundlegend verschiedene Bereiche, die auch Kunden separat angehen. Natürlich stimmen die sich miteinander ab die einzelnen Abteilungen, aber gerade in großen Betrieben ist es voneinander getrennt. Der ganze Lieferverkehr und die Zahlung haben an sich nichts miteinander zu tun. Die Prozesse, ja, sind spannend gelöst. An sich, auch hier: es gibt schon die Möglichkeit, es gibt die Ansätze. Es ist nur nach wie vor schwierig, die Kunden zu überzeugen, solche Lösungen zu nutzen. Es ist tatsächlich so, dass die Motivation zum transparent werden nicht sehr hoch ist. Wenn ich das Beispiel mit den Aluminiumkapseln bei Nespresso aufgreifen darf: selbst dieser Hersteller hat schon ziemliche Schwierigkeiten, von einer normalen Nummer (Material) zu individuellen Nummer zu wechseln für ein Zertifizierungssystem. Selbst da setzt es eigentlich aus, weil die Möglichkeit gar nicht gegeben ist. Er kann gar nicht wirklich die Nummer individuell vergeben. Er müsste seinen kompletten Prozess umstellen. Was sich so vielleicht einfach anhört geht in die hunderttausenden Euros. Angefangen von irgendwelchen Laser-Scannern bis über irgendwelche Printer bis irgendwelche Schulungen für die Mitarbeiter, ERP-Umstellungen und so weiter. Es ist ein riesen Aufwand. Ich denke, dass wir in Zukunft andere Lösungen brauchen, um die Transparenz zu gewährleisten. Die Frage ist nur, wer nutzt solche Systeme und wie werden die benutzt. Spannender Prototype, gerade das Thema Zahlungsverkehr. Was da auch noch Problem ist: die Industrie hat keine Lust, irgendwo in Kryptowährungen zu zahlen. Die sind einfach viel zu instabil und man weiß nicht, wo es hingeht. Und wenn die ganzen Zahlungsverkehre, die noch nicht so geregelt sind, in Kryptowährungen passieren, dann ist es natürlich schwierig für die Industrie, angefangen von Steuerzahlungen (zum Beispiel Mehrwertsteuer in Kryptowährungen). Es fehlen einfach noch Grundlagen, um auf solche Lösungen in Zukunft zu gehen. Das heißt Regulierungen, Transparenzerhöhungen und so weiter muss alles erstmal gegeben sein. Und wenn das der Fall, das wird sicherlich noch mehrere Jahre dauern, dann erst kann auf solche Lösungen zugegriffen werden. Beispiel PayPal: die haben nichts eigentlich anders gemacht, als dass sie als Drittanbieter Zahlungsverkehre anbieten in Realwährungen. Wenn du die Geschichte von PayPal durchliest: wie lange die dafür gekämpft haben, dass PayPal genutzt wird. Die haben wirklich lange Zeit gebraucht, um das System irgendwo zu etablieren. Ähnlich ist es natürlich bei Blockchain.

A: In Bezug auf den Prototyp und das Konzept dahinter: klar, die Umsetzbarkeit für industrielle Zwecke ist natürlich sehr schwierig. Abgesehen davon, sind dir irgendwelche Schwächen und Limitierungen direkt aufgefallen?

E: Ja, muss man auf Kryptowährungen setzen oder kann man Realwährungen einbinden? Wäre sicherlich ein höherer Anreiz, zum

Beispiel PayPal. Klar, Blockchain bietet die idealen Voraussetzungen. Ich glaube, die Bereitschaft in Kryptowährungen zu investieren, geschweige denn zu zahlen, ist sehr gering.
A: Jetzt noch zwei verbleibende Fragen. Es wurde ja als Drittanbietersystem modelliert, unter anderem auch deswegen, weil es für Firmen einfacher sein wird, einen Drittanbieter in deren Systeme zu integrieren. Kann man das so sagen?
E: Schwer zu sagen. Kommt immer auf die Systeme drauf an, die die so haben. Nur als Beispiel, hat zwar nichts mit Blockchain zu tun aber DATEV ist ein Softwareanbieter für Lohn, Buchhaltung, Bilanzen usw. Eigentlich der führende Anbieter in Deutschland. Die haben ein Ünternehmen onlineünd da ist es so, dass der Steuerberater meistens Buchhaltung und Finanzierungen macht. Ünternehmen online"bietet den Vorteil, dass die Unternehmen selber dann Zugriff haben. Hier schon allein die Nutzung von dem Ünternehmen online"geht gegen null, weil die Unternehmen ihre eigenen Prozesse und ihre eigenen Systeme haben (Buchhaltungsoftware, Zahlungssoftware,
usw.). Dann haben die auch noch eine Angebotserstellung als neues Modul integriert. Das heißt, ich könnte aus DATEV heraus Angebote für meine Kunden erstellen und die denen dann schicken. Und da hat auch der Steuerberater gemeint, das wird eigentlich nicht angenommen, weil jeder hat so seine eigenen Systeme und Software. Die machen das Jahren so und nur weil ein neuer Anbieter kommt, steigen die da nicht um. Die haben keine Lust, das zu ändern. Ich hab viele Gespräche geführt, auch zum Beispiel mit einem Freund von mir. Die haben komplett umgestellt für die Distribution auf Microsoft VX (?). Auf jeden Fall haben die auf ein neues System umgestellt und haben gemeint, dass die Umstellung sehr aufwendig und sehr schwierig ist, sodass sie wieder auf ein altes MS-DOS Programm wieder umstellen. Das hat funktioniert und die brauchen nicht mehr. Das reicht denen. Die sind 400 Mitarbeiter groß und die brauchen nicht irgendwo ein Online-System, wo ein Vertriebler jetzt im Auto Zugriff hat, sondern denen reicht ein DOS-System was funktioniert. Mit der Umstellung haben die so viele Ressourcen verwendet und Aufwand betrieben, und es hat sich einfach nicht gelohnt. Da siehst du schon, dass gerade neue System oft Schwierigkeiten machen. Auch SAP als führender Anbieter. Auch Aldi und Lidl haben versucht auf SAP umzustellen, haben aber am Ende entschieden, auf das alte System zurückzugehen. Da gibt es zahllose Beispiele.
A: Abschließend die Frage, ob du den Eindruck hast, dass der Prototyp Transparenz, aber auch Vertrauen zu den Kunden verbessern kann oder verbessert?
E: Ja, auf jeden Fall. Man muss es nur den Kunden so erklären, dass sie es verstehen. Das ist eben das Hauptproblem, dass viele das nicht verstehen können. Das fängt schon an mit irgendwelchen Hashes. Ich sag mal 90% der Industrieunternehmen haben keine Ahnung, was

ein Hash ist, geschweige denn was IPFS oder OriginStamp oder sonstiges ist. Die wissen es nicht, die haben keine Ahnung. Wem erklärst du das? Erklärst du das der IT, die vielleicht davon Ahnung haben, aber es nicht transportieren können zu den Bereichen, die damit arbeiten können oder erklärst du das jetzt irgendeinem, der die Lieferkette transparent machen will, aber keine Ahnung von der Technik hat. Deswegen: Es kann Vertrauen schaffen, ja, auf jeden Fall und es ist sicherlich auch eine Zukunftslösung. Aber die muss dem Kunden genauso transparent erklärt werden, wie er dann die Transparenz auch steigern kann in seinem Prozess.

B.3.4 *Expert Interview 4*

[Erläuterung des Prototyps und des Konzepts vor dem Interview]
A: Wir starten mit einem einleitenden Teil. Produktverfolgung – was fällt dir ein? Wie würdest du die am besten gestalten und auf was würdest du besonders achten? Welche besonderen Merkmale würdest du ansetzen? Würdest du bevorzugt Technologien einsetzen?
E: Bei der Produktverfolgung ist es ganz wichtig, einmal dass die einzelnen Verfolgungsschritte oder die einzelnen Schritte, die ein Produkt nimmt, so abgelegt werden, dass sie manipulationssicher sind (keine nachträglichen Änderungen) und dass sie von allen Parteien auch einsehbar sind. Und für diese Einsehbarkeit ist es wichtig, dass die einzelnen Parteien auch eine gewisse Zugriffssicherung für bestimmte Informationen haben, zusätzlich zu den Informationen, die für alle einsehbar sind. Und man eben auch bestimmte Informationen verbergen kann vor bestimmten Teilnehmern. Es muss da irgendwie verschiedene Ebenen des Zugriffs geben können, das ist wichtig. Jetzt habe ich deine weitere Frage vergessen.
A: Würdest du irgendwelche Technologien bevorzugt einsetzen?
E: Also momentan wird das primär gemacht, indem es letztendlich ein Konsortium gibt, also unterschiedliche Teilnehmer von so einem Trackingsystem wie zum Beispiel DHL und einen entsprechenden Produzenten erstmal. Ohne dass der Kunde da einbezogen ist, zumindest als Endkunde. Und die machen es dann letztendlich in einer Datenbank. Entweder in einer zentralen Datenbank oder in einer ver-teilten Datenbank, wo sich immer das Problem ergibt, dass diese Daten eben nicht manipulationssicher sind. Sie sind eben nur so manipulationssicher wie man den Leuten beim Administrieren vertraut. Das ist ein großes Problem aktuell und da wäre natürlich wünschenswert, dass diese Manipulationssicherheit sichergestellt ist. Da bietet sich eben die Blockchain an.
A: Okay. Da kommen wir nachher nochmal drauf zurück. Produkte müssen ja teilweise Transportstandards oder Bedingungen erfüllen. Wie würdest die Überprüfung der Daten, die da zum Beispiel getrackt werden, sicherstellen?

E: Das habe ich jetzt nicht ganz verstanden. Du hast einmal davon gesprochen, dass Qualitäts- oder Sicherheitsstandard sichergestellt werden sollen, wo sich für mich auf das Produkt beziehen. Und dann nochmal die Daten das Tracking betreffend.
A: Ja, das kann man als zwei verschiedene Prozesse sehen. Du kannst es auch zusammen betrachten, zum Beispiel bei medizinischen Produkten, die versendet werden und auf dem Produktweg muss eine gewisse Temperatur eingehalten werden. Dann musst du ja sicherstellen, wie diese Bedingung auf dem Transportweg sichergestellt wird. Wie würdest du das machen?
E: Letztendlich sind die einzelnen Schritte, wo das Produkt gescannt wird oder auch diese Bedingung überprüft wird, sind ja erstmal für sich einzelne Datenpakete. Aber diese Nachvollziehbarkeit und im Gesamten die Sicherheit, dass die Qualitätsstandard wie Temperatur eingehalten worden sind, ergeben sich vor allem dadurch, dass man das im ganzen Prozess verknüpft überprüfen kann und die Daten zusammenhängend sind. Da ergibt sich wieder die Anforderung, dass man diese Daten irgendwie für die Leute mit Berechtigung zugreifbar macht in einer Datenstruktur, die auch manipulationssicher aber auch zugreifbar ist. Wie eine Blockchain.
A: Der Kreis schließt sich.
E: Der Kreis schließt sich. Von den Daten an sich ist das eine verkette Liste. Und man muss eben von dem aktuellen Datenpaket, das einem vorliegt (unique ID), muss man eben vor allem diese Rückverfolgbarkeit haben. Also Schritt für Schritt rückwärts in der List. Und da muss die Verknüpfung zu dem vorherigen Schritt existieren wie in einer linked list. Bei solchen Sachen sind ja auch immer sensitive Daten und Parameter am Start (wie eine Chargennummer von einem Impfstoff zum Beispiel) oder in anderen use cases noch sensiblere Daten. Da muss eben sichergestellt sein, dass nur die Parteien den Zugriff haben (wenn es eben so eine öffentliche Speicherstruktur ist). In gewisser Weise muss das verschlüsselt erfolgen oder eben so, dass ein Dritter, der auch Zugriff auf diese öffentliche Struktur hat, nicht durch Ausprobieren (Bruteforce) an die Daten kommt.
A: Gut. Jetzt mal noch ein bisschen weg vom Technischen. Welche Anforderungen stellst du an Lieferkettenprozesse und deren Abbildung (wie die letztendlich in Software abgebildet werden)?
E: Wie die in Software abgebildet werden?
A: Nicht so technisch. Teil 1: Welche Anforderungen stellst du allgemein an Lieferketten, wenn du das aus verschiedenen Sichtweisen betrachtest und die Abbildung in Software (hatten wir schon teilweise).
E: Das Wichtigste beim Lieferkettenprozess eines einzelnen Produktes ist die Nachverfolgbarkeit. Und die große Herausforderung ist ja, dass in der Lieferkette unterschiedliche Teilnehmer dabei sind, die auch unterschiedliche Systeme haben. Eine große Herausforderung ist eben diese Nachverfolgbarkeit anhand einheitlicher Standards über die verschiedenen Teilnehmer abzubilden in diesem Pro-

zess. Das eben auch einfach zu gestalten und bei der Anbindung ein einfaches Interface zu haben, weil es momentan sehr hinkt. Du hast die unterschiedlichen Teilnehmer des Lieferkettenprozesses, jeder hat sein ei-genes System und an diesen Systemgrenzen muss es ja irgendwie übergeben werden. Es kommt von der einen Repräsentation von Lieferant 1 in die neue Repräsentation von Lieferant 2. Wenn man dann aber das große Ganze betrachtet, ist es schwierig die einzelnen Schritte nachzuvollziehen, weil die Teilnehmer untereinander irgendwelche Qualitätsstandard verhandelt haben, die dann auch bei der Übergabe gecheckt werden. Aber für den Endkunden ist das nicht mehr ganz nachvollziehbar. Der hat vielleicht die Zusage und die Möglichkeit, den Zustand von dem Produkt vom letzten Lieferanten anzuschauen, aber diese Nachverfolgbarkeit im Einzelnen ist nicht unbedingt gewährleistet. Und das ist eben eine wichtige Anforderung, dass der ganze Prozess anhand von einheitlichen Datenformaten und Trackingschritten verfolgbar ist.

A: Du hast es nicht explizit gesagt, aber letztendlich geht die Nachverfolgbarkeit einher mit der Transparenz in den Prozessen.

E: Ja, das ist impliziert.

A: Das kann man schon auch getrennt betrachten teilweise.

E: Genau. Transparenz soweit wie notwendig und für die berechtigten Parteien. Das ist das Wichtige. Wenn man jetzt ein Lebensmittel nimmt und der Hersteller oder Verkäufer sagt, dass du die einzelnen Lieferschritte online verfolgen kannst als Marketing, dann ist das super, wenn das jeder ohne Zugriffsschutz einsehen kann. Aber in den meisten Lieferketten ist ja das Wichtige, dass nur die beteiligten Parteien einsehen können und das transparent ist. Grund: Wenn du dir jetzt zum Beispiel überlegst, dass du eine Lieferkette in einer öffentlichen Datenstruktur abgebildet hast, wo zwar die Inhalte nicht lesbar sind, dann kann man schon mithilfe von Analysemethoden (Visual Analytics, Datenmanipulation) vielleicht anhand der Verknüpfung die Trackingschritte zuordnen. Woher kommt das und wer arbeitet mit wem zusammen? Das ist nachher der Super-GAU, weil man dann seinen Wettbewerbsvorteil oder lässt andere in die eigenen Karten reinschauen was die Lieferkettenprozesse angeht. Auf der einen Seite ist es halt die Transparenz, die wichtig ist (mit der Einschränkung für die berechtigten Parteien) und auf der anderen Seite muss es schon auch eben für die nichtberechtigten Parteien trotzdem intransparent bleiben.

A: Noch kurz zu deinem Background. Wie bist du mit der Blockchain-Technologie in Verbindung geraten und wann? Wie verfolgt du es weiter?

E: Ich kam damit vor 3 Jahren in Berührung über eine Vorlesung an der Universität Konstanz. Seitdem habe ich mich damit private intensiv beschäftigt und seit anderthalb Jahren beruflich intensiv, weil ich an der Uni in dem Bereich arbeite und promoviere und parallel in einer Firma arbeite, die Blockchain-Lösungen um Timestamping aktiv

ausrollt und entwickelt. Hingegen ist mein supply chain Hintergrund als solcher nicht unbedingt logistischer Natur als dass ich da bei einer Firma gearbeitet hab wie Lieferanten. Ich kenne das viel mehr aus der Warenwirtschafts-Sicht. Ich habe lange Zeit Consulting für eine Firma, die ERP-System vertreibt und eben auch sehr viel Customizing gemacht hat, gemacht. Da ist eben supply chain und die Nachverfolgbarkeit zu einzelnen Lieferungen und Bestellungen sehr wichtig. Da ist die Problematik von den Systemgrenzen die größte, weil jeder einzelne Lieferant hat auch seine eigenen Produkt-IDs und Artikel-IDs und das mapping an den Systemgrenzen ist sehr viel Aufwand. Wenn das hiervon reinkommt, wo wird das uns zugeordnet. Die Systemgrenze ist nachher die Warenannahme und da werden so viel beschäftigt allein, um dieses mapping sicherzustellen. Auch weil die Qualitätssicherung aufgrund von nichteinheitlichen Standards nicht gewährleistet ist, was eben auch wichtig ist bei einem Produkt, das man über Systemgrenzen hinweg einsetzen kann. Es ist so, dass die in der Warenannahme zumindest Stichproben machen oder bei teureren Teilen jedes einzelne Teil auspacken und nochmal intern prüfen, weil man dem Lieferanten davor nicht vertraut. Das zu automatisieren ist ein großes Zeit- und Geldersparnis und es würde vieles einfacher gestalten.

A: Wir haben vorher schon die Vorstellung vom Prototyp gemacht. Jetzt hätte ich noch ein paar Fragen. Was war dein erster Eindruck vom Konzept dahinter?

E: Finde ich sehr interessant. Geht auch schon in die Richtung, wo es eben um die Transparenz und die Vereinheitlichung von den Lieferkettenprozessen geht und das Automatisierungspotential finde ich auch gut. Das zwar in abgesteckten Grenzen, aber dass die einzelnen Teilnehmer automatisiert die einzelnen Trackingschritte nachvollziehen können, ohne dass man zum Beispiel noch mal telefonieren muss und irgendwelche Lieferscheinnummer abgleichen muss (sondern direkt mit dem Handy/online nachvollziehbar). Sobald ein Trackingschritt in dem System hinterlegt, ist er nicht wiederrufbar. Das finde ich schon sehr interessant. Ich glaube, es hat großes Potential.

A: Sind dir nach dem ersten Eindruck irgendwelche Schwächen/Limitierungen aufgefallen?

E: Dieses off-chain-Weitergeben von dem Preimage ist noch so ein Knackpunkt, wo es natürlich auch schön wäre, das on-chain zu automatisieren. Das geht momentan nicht oder ich kenne die keine Lösung dafür, weil sobald man was on-chain hinterlegt, ist es erstmal öffentlich für alle einsehbar. Deswegen ist eine on-chain password-exchange eine große Problematik zwischen unterschiedlichen Partnern. Da denke ich, dass man noch Zeit investieren muss. Sonst war es für mich ein bisschen schwierig. Vielleicht könnte man Anfang nochmal in die Thematik als solche einführen. Ich weiß nicht, ob das gewünscht ist aber das hat mir am Anfang bisschen gefehlt. Was ich

ja auch schon gesagt hab, wo man sich noch Gedanke machen muss: Wie werden so Qualitäts- oder Prozessstandards definiert und wie können die validiert werden? Wie schafft man den Spagat zwischen Transparenz für berechtigte Teilnehmer und Intransparenz für unberechtigte Teilnehmer? Also letztendlich Zugriffsschutz. Wenn man über Lieferketten nachdenkt, so wie ich das verstanden habe, ist das eine sequentielle linked list, die hier aufgebaut wird. Was man ja in einem Lieferkettenprozess hat, sind ja Weggabelungen in beide Richtungen im Prinzip, dass mehrere Produkte zu einem in einem manufacturing Schritt zusammengeführt werden oder dass man aus einem Rohstoff zum Beispiel Stahl Wellblech macht. Das wäre noch interessant.
A: Darf ich ganz kurz einhaken?
E: Ja.
A: Da gäbe es zum Beispiel die Möglichkeit, in die Trackingparameter zum Beispiel einen IPFS hash vom vorhergehenden Produkt einfügen.
E: Was IPFS angeht: Das ist für den Prototyp eine ganz interessante Sache. Was ich da als großes Problem sehe, ist, dass IPFS pinning ist. Wenn man ein Dokument oder was auch immer hinterlegt ist, dass die Anhand der Zugrifffrequenz im Netz verbleibt. Wenn es eine Weile nicht mehr zugegriffen wird, ist die Datei weg. Man kann es natürlich sicherstellen, wenn man automatisierte Skripte hat, die die aufrufen oder man eigene Server hat, die die pinnen unabhängig von der Zugriffsfrequenz. Das kann aber nicht Sinn der Sache sein. Wenn man eben erstmal ein autonomes verteiltes Netz hat, dass man wieder selber Instanzen, die nicht notwendig sind, aufbaut. Ich weiß nicht, wie sich das weiterentwickelt aber das sehe ich noch kritisch, dass eigentlich essentielle Informationsteile plötzlich verloren gehen, weil bestimmte Zugriffsparameter nicht gewährleistet sind.
A: Teillösung: Aktuell ist es ja so, dass in das öffentliche IPFS-Netzwerk hochgeladen wird. Man könnte auch ein privates IPFS-Netzwerk innerhalb der Unternehmen beziehungsweise der Endkunden aufbauen.
E: Da muss man halt auch einen Spagat machen zwischen Konsortium-Lösung und private Blockchain oder IPFS. Da gehen halt die Vorteile dieser öffentlichen verteilten Datenstrukturen verloren, vor allem im Hinblick auf Manipulationssicherheit, was voll und ganz berechtigt sein mag, wenn die Teilnehmer unter sich nochmals die Daten replizieren. Dann ist da gegenseitig sichergestellt ist, dass die Manipulation nicht passiert oder teuer ist oder eben mit Vertragsstrafen belegt ist und einfach erkannt werden kann. Man muss da einfach irgendwie den trade-off finden für die richtige Lösung. Zu IPFS: man kann da schon auch incentives online schaffen, damit die verfügbar bleiben, zum Beispiel über einen Smart Contract. Da können Leute aktiv dafür bezahlt werden, dass sie entweder auf ihre IPFS node hosten oder aktiv pollen. Dann hätte man weiterhin diese verteilte Instanz. Da muss man sich definitiv auch noch Gedanken machen. Synchrone

Verschlüsselung anhand vom Preimage: Wenn klar ist, wer die Teilnehmer in dem Netzwerk sind (gerade nicht im Endkundengeschäft, sondern Zulieferer und Manufacturer, wo es wenige große bis mittelständische sind), dann könnte man auch über asymmetrische Kryptographie nachdenken, weil die Logistik für das Key-Management ist nicht so groß. Dann ließe sich dieses off-chain-Verteilen dieser Preimages vielleicht noch durch Einmalschlüssel irgendwie lösen. Da bin ich auch nicht Kryptoexperte genug, aber da gibt es sicherlich auch noch Möglichkeiten.

A: Wie schätzt du die Integration von so einem Konzept in bestehende Prozesse ein?

E: Das aktuelle Problem, weswegen man so allübergreifende Lösungen auch nicht hat, ist ja, dass die Teilnehmer in der Lieferkette nicht am Endprodukt interessiert sind, weil sie den Vertrag mit dem jeweils Nächsten in der Lieferkette haben. Deswegen ist es für die nicht notwendig und macht deshalb preislich keinen Sinn, sich an so einem großen System zu beteiligen. Es ist halt auch ein gesundes Misstrauen vorhanden. Sich irgendwie darauf zu verlassen, dass jemand die Informationen in Step 1 richtig einträgt und ich die in 13 noch richtig lese, wo 12 davor waren, ohne eigene Validation, wird in Zukunft nicht passieren. Grund ist, weil auch da wieder Qualitätsstandards (in der Software Service Level Agreements) einzuhalten sind. Deswegen macht es auch Sinn, dass man in der Warenannahme zumindest stichprobenartig kontrolliert. Was ich schon sehe, ist, dass man das zusätzlich zu den aktuellen Konzepten irgendwie etablieren kann. Aber vor allem, indem der jeweils Nächste in der Lieferkette dem Vorherigen einen Anreiz schafft, daran teilzunehmen. Was ich mir vorstellen kann: Der Lieferant davor nimmt daran teil und lädt seine Tracking-Daten und bekommt dann im Austausch dafür vom Kunden etwas zurückgeliefert. Vom Endkunden wäre das das Geld, ansonsten zum Beispiel statistische Daten, Analysedaten (wie gut war das Produkt, ...), damit die auch intern den Anreiz haben, diesen Prozess zu verbessern und sich besser zu machen. Das wäre dann auch wieder ein Wettbewerbsvorteil. Das kommt immer darauf an, ob ein Teilnehmer (auch ohne große Marktmacht) diesen ganzen Prozess kontrolliert oder ob er die Leute zwingen kann, daran teilzunehmen. Müsste man auch auf die use cases schauen.

A: Ja.

E: Im Endkundengeschäft ist es primär Aufwand für die Teilnehmer. Wieso soll Amazon plötzlich an einem Trackingsystem für den Endkunden teilnehmen, das kostet die nur Geld und ist für den Endkunden eine schöne Spielerei. Was aber in die andere Richtung ganz interessant sein kann für Amazon, weil sie eben Zeit und Ressourcen minimieren, wenn gewissen Qualitätsstandard vorangestellt sind oder wenn ein Produkt von einem Lieferanten eine Option nicht stimmt. Dann kann schon gesagt werden, dass man das gar nicht anschaut.

Oder was man sich auch schon vorstellen könnte (wenn Amazon ein Endprodukt verkauft und in vielen Schritten davor Zugriff auf den Status des Rohmaterials hat), dass er dann auch Lieferverspätungen oder -ausfälle viel früher erkennen könnte, indem er halt merkt, dass etwas schiefläuft oder die vertragliche Vereinbarungen von früheren Gliedern dieser Lieferkette schon nicht erfüllt werden. Das wäre glaub ich ganz interessant. Das steht und fällt damit, dass eben die einzelnen Teilnehmer einen Mehrwert davon haben und einen Mehrwert davon haben, daran aktiv teilzunehmen. Der muss halt irgendwie geschaffen werden.

A: Das sehe ich auch so. Das ist hier tatsächlich ein Drittanbietersystem, das zwischen den Parteien steht. Wie siehst du diese Modellierung?

E: Letztendlich sehe ich das nicht kritisch. Was bei sowas immer wichtig ist, dass auch wieder Transparenz da ist, damit als Teilnehmer die Prozesse nachvollziehen kann. Du hast irgendwelche Datenstrukturen, wo du das selbst machen kannst aber keine Kapazitäten hast das zu machen. Deswegen hast du gerne mal jemanden dazwischen, mit dem du den Vertrag schließt und auch einen Kopf kürzer machen kannst, wenn etwas nicht funktioniert. Das ist erstmal das Angenehme an einer Zwischenpartei. Da wäre das Interessante, das trotzdem nachvollziehbar ist, was passiert. Wenn der finanzielle Aufwand, sowas anzubinden, vertretbar ist und ein Mehrwert da ist, dann ist es meiner Meinung nach absolut in Ordnung, wenn da jemand als vertraglicher Ansprechpartner dazwischensteht. Das war auch lange Zeit das Problem bei Linux zum Beispiel. Es war an sich ein super System, es gab aber keine Vertragsparteien. Das ist halt in der Business-Welt schlecht, weil man immer jemanden haben möchte, auf den man bei Problemen zugehen kann. Ich glaube da gilt es auch einen tradeoff zu finden zwischen der Nachvollziehbarkeit der Funktionsweise und es klar ist, dass diese Drittpartei die schönen Merkmale Transparenz und Fälschungssicherheit nicht aussetzen kann, wenn sie will. Dass aber durch die Drittpartei ein schönes Interface, eine schöne API und eine smoothe Anbindung gewährleistet ist.

A: Du hast es eigentlich vorher schon gesagt. Abschließend hast du schon den Eindruck, dass so ein Konzept letztendliche die Transparenz aber auch das Vertrauen zwischen den Parteien in der Lieferkette erhöhen kann?

E: Ja, definitiv. Wenn definiert ist, was für Informationen hinterlegt sind und was die genauen Richtlinien und Rahmenbedingungen sind für die Durchführung der einzelnen Trackingschritte. Und dass die Sachen, die drin stehen auch autorativ sind, also dass es trotzdem eine Verbindlichkeit unter den Parteien hat. Dann aber definitiv. Gerade vorzeitig Ausfälle zu erkennen, ohne dass 13 Parteien miteinander telefonier müssen, kann interessant werden. Da ist auch wieder der Zugangsschutz (berechtigte Parteien können lesen, andere nicht) essentiell. Was hier dargestellt ist, sind Lieferant und Endkunde. Bei einer echten Lieferkette hast du genau diese Verbindung mehrere

Male hintereinander. Da ist jeder Vorgänger in der Lieferkette Lieferant und jeder Nachfolger gewissermaßen auch Kunde, auch wenn er im nächsten Schritt wieder Lieferant sein kann. Das wäre sehr interessant, wenn auch weiter hinten stehende Endkunden gewissermaßen Zugriff haben und mit den Daten frühzeitig was anfangen können und sehen können, was aktuell passiert. Ein großer Fehlerfaktor ist letztendlich der Mensch. Ganz stupide gesagt sitzen da Leute, die scannen Barcodes und mappen die dann zu eigenen Barcodes. Die packen was von einem Lieferanten eigentlich nochmal um in ihr internes Zeug. Das ist einfach ein riesiger Fehlerfaktor, weil jetzt die Leute auch mal nicht bei der Sache sind. Wenn man das automatisieren kann und beschleunigen, dann sind sicherlich viele Leute bereit, daran teilzunehmen.

B.3.5 *Expert Interview 5*

A: Kurz zu meiner Person: Ich schreibe gerade meine Bachelorarbeit und habe in meinem Bachelorprojekt einen Prototyp entwickelt, der die Blockchain-Technologie in Lieferketten-Prozesse einbindet. Für die Evaluation von diesem Prototyp führe ich unter anderem noch Experteninterviews durch. Dabei freue ich mich sehr und bedanke mich bei Ihnen an dieser Stelle, dass sie sich für das Interview bereiterklärt haben. Das Interview ist so aufgebaut, dass ich zuerst ein paar einleitende Fragen hätte, die sehr allgemeint gestellt sind. Danach würde ich kurz den Prototyp vorstellen und daraufhin hätte ich noch Fragen zum Prototyp, beziehungsweise Ihre Meinung zum Prototyp. Dann fange ich jetzt mit den einleitenden Fragen an. Wie würden Sie Produktverfolgung gestalten (beziehungsweise wie ist das bei Ihnen gestaltet)? Und welche Technologien Sie bevorzugt einsetzen würden oder welche eingesetzt werden.
E1: Und was meinen Sie mit Produktverfolgung?
A: Wenn zum Beispiel ein Produkt hergestellt wird dessen gesamter Lieferkettenprozess. Wie da die Daten, die da aufkommen, verwaltet oder erstmal erfasst werden.
E1: Reden Sie über Traceability oder über die normalen Liefer- und Auftragsdaten?
A: Über Traceability.
E1: Okay. Traceability ist generell ein recht neues Thema. Das heißt, wir haben Ansätze zum Thema Chargenverfolgung und es gibt Roadmaps und Traceability-Ansätze auch auf Einzelprodukten, auf Behältern und auch Chargen durch die ganzen Ketten durch zu installieren. Wir haben erste use cases, normalerweise ist Traceability auf A- und B-Teile an einem konkreten Produkt schon realisiert in Einzelfällen. Das wird weiter ausgedehnt werden, und in die anderen zwei Felder werden wir vermehrt reingehen.
A: Wenn Sie das Tracking gestalten würden: Hätten Sie irgendwelche Tech-

nologien (QR codes, RFID tags, . . .) die Sie bevorzugt einsetzen würden?
E1: Alles von dem.
A: Nichts bevorzugt in dem Sinn?
E1: Nein. Es gibt verschiedene Varianten und es sind auch verschiedene Varianten im Einsatz. Es wird an weiteren technischen Lösungen geforscht.
A: Okay. Dann würde ich mal zur nächsten Frage übergehen. Überprüfen Sie zugekaufte oder Produkte, die zu Ihnen kommen, oder deren Status vom Hersteller abfragen? Müssen Ihre Produkte selber oder die, die Sie kaufen, Transportstandards oder Bedingungen erfüllen? Unabhängig davon: Wie könnte die Transportbedingung und deren Einhaltung überprüfen?
E1: Wir überprüfen Menge und Termin. Wir haben keine Notwendigkeit, bestimmte Transportstandards einzuhalten wie in der Pharmaindustrie (Temperatur, Feuchtigkeit, . . .). Wir haben natürlich auf dem Seeweg zum Beispiel entsprechende Exportverpackung, dass die Materialen anders verpackt werden für andere Transportbedingungen. Wir haben einen use case, wo wir teilweise Seefrachten oder längere Strecken tracken und evaluieren (ob es Schäden gibt auf den Transporten). Sowas wird teilweise gemacht.
A: Jetzt unabhängig, wie es in einem speziellen use case gemacht wird: Hätten Sie da einen Vorschlag, wie man solche Bedingungen überprüfen könnte (generell)?
E1: Sie sagen jetzt NFC oder RFIC. Wir haben neuere Technologien, die ein Stück weitergehen und die dann eben Temperatur und andere Themen erfassen können. Die sind dann entsprechend auswertbar.
A: Welche Anforderungen generell stellen Sie an Lieferkettenprozesse? Also was muss ein Lieferkettenprozess für Sie erfüllen?
E2: Wir müssen kurz unterbrechen.
E2: Okay, wir können wieder weitermachen.
A: Soll ich die Frage nochmal wiederholen?
E2: Ja.
A: Welche Anforderungen stellen Sie an Lieferkettenprozesse? Also was muss ein Lieferkettenprozess für Sie erfüllen?
E1: Wie gesagt, normalerweise ist die Relevanz, welche zeitlichen Bedingungen da dahinterstecken und dass diese Zeiten auch eingehalten werden. Wir haben eine starke Diskussion um das Thema Vorlaufszeiten im Transport und Einhaltung der Vorlaufszeiten, wie wir wirklich entsprechend Planungssicherheit in den Ketten haben. Man kann es so allgemein beantworten: termintreu, liefertreu und natürlich qualitativ dürfen die Produkte nicht beeinträchtigt werden.
A: Okay. Die nächste Frage greift da teilweise rein. Welchen Stellenwert hat dann Transparenz und Vertrauen gegenüber Kunden in Lieferkettenprozessen? Ich kann die Frage noch spezifizieren. Bezüglich Transparenz zum Beispiel: Es fallen zum Beispiel bei einer Lieferung die zeitlichen Daten an. Wie transparent sollen die dann mitgeteilt werden? Wollen Sie die haben?
E1: Die hat man ja im Allgemeinen. Wir verstehen die Frage nicht

wirklich.
E2: Meinen Sie ein Online-Tracking, wo sich die Ware befindet zum Beispiel?
A: Ja zum Beispiel. Wie kommuniziere ich Sachen, die jetzt auf dem Lieferweg passieren? Wenn wir auf den use case der Pharmaindustrie (Temperaturdaten) gehen. Wie kommunizieren Sie diese Daten? Wie würden Sie die preisgeben gegenüber dem Kunden? Würden Sie die überhaupt preisgeben?
E1: Wir haben vorhin gesagt, dass bei uns Termin und Menge [wichtig sind]. Natürlich, wenn was was schief läuft im Transport, muss man kommunizieren. Das passiert aber heute auch sofort.
A: Okay. Dann lassen wir das mal so stehen. Die nächste Frage haben Sie eigentlich schon beantwortet. Welchen Stellenwert haben Lieferketten für Sie speziell im Unternehmen, auch für interne Prozessoptimierungen?
E1: Ich habe ja vorhin schon gesagt, dass Liefertreue, Terminabkürzungen, Zuverlässigkeit, Einhaltung dieser Laufzeiten entsprechend wichtig sind.
A: Ja. Viele Unternehmen benutzen auch externe System für das Tracking zum Beispiel. Werden Lieferkettenprozesse bei Ihnen selbst entwickelt oder haben Sie das auch ausgelagert?
E1: Das ist immer recht schwierig, weil „Lieferkettenprozess“ kein gängiger Begriff ist, der bei uns verwendet wird. Wir haben eine normale Lieferbeziehung mit entsprechenden Aufträgen, Terminen, Lieferplänen, Eintrefftermine, zugesagten Terminen und so weiter. Das wird natürlich alles im System nachbehalten und getrackt.
A: Bei Ihnen selber?
E2: Bei uns selber.
E1: Dann gibt es natürlich mit Spedition entsprechende Prozesse. Sowohl zur Spedition, wie zu Kunden, werden die Daten über EDI direkt online übermittelt, sodass jeder das gleiche Bild hat. Und es gibt natürlich auch für Kunden oder Lieferanten, die nicht so eingebunden sind, entsprechende Internetanwendungen, über die das Gleiche passiert: Man teilt dem Partner Daten mit und preisgibt. Von daher gibt es entsprechende Prozessdesigns. Vieles ist in-house entwickelt, es ist aber auch Fremdsoftware eingebunden in diese Prozesse. Wir reden über Big Data Lakes und Cloud Solutions und natürlich dort auch weitere Lösungen zu implementieren und die Prozesskette weiter transparent zu machen. Sie reden immer von Traceability. Es gibt zwei Themen. Das Eine ist über Massenauswertung diese Daten zu analysieren und für Optimierungen zu verwenden. Das wäre eher eine nach hinten in die Vergangenheit gerichtete Sichtweise mit Optimierungspotential für die Zukunft. Das Andere ist das was sie Traceability und Online-Verfügbarkeit von Daten nennen in den Prozessketten, um das Tagesgeschäft zu steuern. Ich glaube heute liegt der Fokus auf der Steuerung vom Tagesgeschäft. Zukünftig wird der Fokus darauf liegen, mehr Transparenz zu schaffen und die Prozessketten weiter zu optimieren.

A: Sehr interessant. Jetzt haben wir sozusagen den generellen Teil der Lieferketten abgeschlossen. Sind Sie durch Ihre Arbeit oder privat mit der Blockchain-Technologie in Berührung gekommen?
E1: Nein.
E2: Nein.
A: Noch nicht okay. Ist Ihr Unternehmen an der Entwicklung für Blockchain-Technologie interessiert?
E1: Ich habe es gehört in dem Kontext. Die Frage ist natürlich immer: Was verbirgt sich dahinter und ist es wirklich was Neues? Oder ist es nur ein Begriff für Themen, die sowieso kommen? Also von daher, ja, ich habe Planer, die sich daran interessieren; ja, wir haben diskutiert, ob wir das für unsere Prozesse anschauen wollen und werden; nein, wir haben noch nicht konkret gestartet. Wir haben ja den Kollegen von der IT in der Leitung. Kamen bei euch schon Anfragen an?
E3: Ja gut, Blockchain ist momentan ein riesen Hype-Thema und geht natürlich momentan in die Richtung, dass es halt bisschen kritisch gesehen wird. Wir gehen in das Tal der Tränen hinein im Gartner Hype Cycle. Zum Thema Blockchain generell: Es muss halt die Lösung aus meiner Sicht passen. Ob ich da drunter eine Blockchain oder eine verteilte Datenbank habe, hängt vom Business-Modell ab und nicht von der Technologie. Wir haben uns in Richtung Blockchain aufgestellt. Wir haben beispielsweise mit dem Car eWallet eine der ersten Payment-Lösungen für autonome Fahrzeuge am Markt beziehungsweise als Startup und sind grundsätzliche an der Technologie interessiert. Aber nicht aus einer technologischen Perspektive, sondern der Mehrwert muss klar werden. Die nächste Frage ist dann auch immer die, wenn wir über Blockchain sprechen: Blockchain ist jetzt erstmal eine Technologie. Wie wird die dann auch organisational aufgebaut? Das heißt, sprechen wir von public Blockchains mit den allfälligen Problematiken, die es momentan an vielen Stellen noch gibt oder sprechen wir von Konsortien. Dann ist immer die Frage: Sind wir reiner Nutzer einer Konsortium-Blockchain oder werden wir founding member von dieser Konsortium-Blockchain.
A: Gut, wunderbar. Jetzt würde ich ganz kurz meinen Prototyp vorstellen, den ich entwickelt habe. Dieser Prototyp ist ein sehr genereller Ansatz. Es wird vieles stark heruntergebrochen, was die Prozesse angeht. Aber nichtsdestotrotz geht es vor allem darum, wie man die Blockchain-Technologie in Lieferkettenprozesse einbinden kann.
E3: Was ist denn der problem solution den sie anbieten?
A: Was der Prototyp versucht zu lösen, ist, dass die Transparenz in Lieferkettenprozessen erhöht wird. Vor allen Dingen, wenn man sich kritischere use cases wie in der Pharmaindustrie anschaut. Das ist das Eine. Auf der anderen Seite möchten wir natürlich durch die Blockchain-Technologie eine Dezentralisierung der Daten noch erreichen, ohne irgendwelche sensible Daten preiszugeben. Das war der hauptsächliche Ansporn.
Erstmal habe ich den Prototyp in drei Teile unterteilt: Bestellung, das Tracking

an sich und der Bezahlvorgang. Hier muss man natürlich noch dazusagen, dass der Bezahlvorgang an sich auch dezentralisiert gestaltet wurde. Wie erläutere ich nachher noch. Generell zur Struktur, wie der Prototyp in Verbindung mit den verschiedenen Parteien steht: Es wurde ein Fall mit zwei Parteien letztendlich entwickelt, Kunde und Verkäufer. Die Kommunikation zwischen den Parteien wird hauptsächlich über den Prototyp abgewickelt. Zwischen Kunde und Verkäufer werden nur zum Beispiel Passwörter ausgetauscht oder der Produktpreis. Der Prototyp ist im Prinzip ein Drittanbietersystem. Jetzt würde ich ganz kurz auf die verwendeten Technologien eingehen und müsste kurz fragen, ob Blockchains und Smart Contracts bekannt sind.

E2: Nein.

E1: Nein.

A: Okay, dann erläutere ich das einfach ganz kurz. Die Technologie hinter der Blockchain ist eigentlich eine Art der Datenspeicherung. Dabei werden Datenblöcke aneinandergereiht und die Blöcke wiederum miteinander verkettet. Die Verkettung folgt über kryptographische Verfahren. Bekanntestes Beispiel, wo die Blockchain-Technologie auch ihren Ursprung hat, ist in der Kryptowährung Bitcoin. Also die zugrundeliegende Technologie von Bitcoin ist die Blockchain. Dann gibt es noch sogenannte Smart Contracts. Smart Contracts kann sich vorstellen wie kleine Programme, die über die Blockchain ausgeführt werden. Wir haben folgende Vorteile der Blockchain-Technologie: Die Blockchain-Technologie ist verteilt gestaltet. Das heißt, wir haben zum Beispiel bei einer öffentlichen Blockchain die Datenblöcke auf tausenden Rechnern und Servern repliziert. Das erhöht die Sicherheit der Daten so, dass die Blöcke von Transaktionen nicht verändert werden können. Theoretisch ist das natürlich immer möglich, aber je größer das dahinterstehende Netzwerk ist, desto sicherer wird die Technologie. Dann habe ich noch IPFS eingesetzt. IPFS ist ein verteiltes Dateisystem, um Medien zu speichern und zu verteilen. Jedes Medium (Datei, ...) bekommt einen eindeutigen Hash-Wert zugewiesen und über diesen kann auf die Datei zugegriffen werden.

E3: Darf ich kurz die Frage stellen, ob das vielleicht technisch bisschen zu tief geht auch?

A: Ich würde kurz was zu OriginStamp sagen, der nachfolgende Teil ist nicht mehr so technisch.

E3: Für mich ist das in Ordnung, ich komme aus der IT und kenne die ganzen Begrifflichkeiten und könnte auch tiefer rein. Die Frage ist, ob das zum Ziel beiträgt. Deshalb mein Input, ob wir jetzt wirklich so tief gehen müssen oder ob es nicht darum geht, den Mehrwert an den verschiedenen Stellen zu erläutern. Es geht vielmehr darum zu sagen: Ist das überhaupt ein Problem, das es für uns wert wäre zu lösen an der Stelle?

E1: Wichtig ist eben, auf den Prozess zu schauen. Wir müssen verstehen, was im Prozess passieren soll. Die ganze Technologie, auch wenn wir nicht im Detail drin sind, kann ich jetzt nachvollziehen, was das bedeuten wird. Zumindest habe ich ein Bild dazu, ob es stimmt oder

nicht sei mal dahingestellt. Für den Prozess ist es auch völlig egal. Sie sollten darstellen, was da zwischen Kunde und Lieferant passieren soll und dann können wir auch dazulegen, ob das ein Mehrwert hat oder nicht.

A: Okay, dann versuche ich jetzt die Prozesse zu erklären. Wie ich vorher schon gesagt habe, habe ich die Unterteilung in Bestellvorgang, Tracking und Bezahlvorgang gemacht. Wir haben beim Bestellvorgang einen Vertragsschluss zwischen Verkäufer und Käufer, der über den Prototyp abgewickelt wird. Das Ganze ist blockchain-basiert, das heißt, dass die Sicherheit gilt und der Vertrag beispielsweise tausendfach repliziert wird. Dadurch haben wir den Vorteil, dass das Ganze nachvollziehbar und sicher wird. Zusätzlich haben wir bei der Abwicklung über die Blockchain den Vorteil, dass der Verkäufer sich sicher sein kann, dass der Käufer auch das Geld bereitstellen kann. Der Käufer wiederum muss noch nichts bezahlen, solange die Ware sozusagen noch nicht bei ihm im Haus ist. Der Vertrag enthält also ein Passwort und ein Zeitlimit und das Passwort hat nur der Käufer. Dieses Passwort kann er, wenn die Ware angekommen ist, dem Verkäufer übermitteln und dann erfolgt letztendliche die Bezahlung.

E1: Das heißt, das kann man auch beliebig zeitlich verzögern? Weil eins der heutigen Kriterien in heutigen Zahlungswelten sind ja weitreichende Zahlungs-Deale über mehrere Wochen und Monate. Ich bringe jetzt mal wieder das Aldi-Beispiel, wo ein Lieferant nach einem Jahr das Geld bekommt. Ganz so schlimm ist es hoffentlich nicht. Aber der typische Warenfluss und die Bezahlung gehen ja nicht zum selben Zeitpunkt einher.

E3: Das wäre auch mein Input, zu dem was sie gerade anbieten. Wenn man das auf eine abstrakte Ebene hebt, ist ja das, was Ethereum und Smart Contracts zugrunde liegt, ein escrow base, also ein Treuhandkonto, auf das das Geld überwiesen wird. Das hat aber wirklich zur Folge (ich weiß nicht, wie Sie es gestaltet haben) in der Standard Ethereum-Implementation, dass sie zum Zeitpunkt der Transaktion wirklich das Geld haben müssen und die Liquidität. Sie zahlen quasi das Geld, bevor die Ware eintrifft, an ein Treuhandkonto. Damit ist Liquidität abgeflossen, was ja genau entgegen dem Zahlungsziel von 60 Tage ist, um dann zwischendrein mit dem Geld arbeiten zu können. Das liegt dann beim Treuhänder und erst, wenn Sie sagen, dass Sie die Ware erhalten haben, dann würde der Treuhänder das Geld releasen und an den Verkäufer auszahlen. Aber der Punkt ist: Aus Käufersicht ist Ihnen das Geld abgeflossen, bevor die Ware da ist, also komplett invers.

E1: Genau, das ist ja nicht die gängige Praxis.

E3: Nicht die gängige Praxis bei uns, aber die Blockchain ist momentan halt so aufgebaut. Ich meine nur, dass es ein Konflikt ist und es wäre interessant zu sehen, ob Sie das auch so gelöst haben.

A: Letztendliche wurde es so gelöst. Man könnte es auch abändern.

E1: Das heißt, Sie haben es so gelöst, wie es heute im Internet üblich

ist im gängigen Umgang mit Kryptowährungen zwischen Käufer und Verkäufer. Sie haben sich jetzt aber nicht überlegt, ob es eine Speziallösung gibt für den normalen Warenverkehr im ganzen Business-Bezug. Kaufen und bezahlen ist ja nicht gängige Geschäftspraxis in der Industrie.

A: Ja, genau. Da haben Sie recht. Letztendliche läuft es schon so, dass das Geld überwiesen wird und die Ware folgt. Aber natürlich der Kunde hat trotzdem noch die vollständige Kontrolle über sein Geld, ohne auf einen Drittanbieter angewiesen zu sein.

E3: Wir hatten ähnliche Situationen im eWallet und ich kann Ihnen aus Erfahrung sagen, dass das ein Thema ist, dass Sie dann noch das Thema Volatilität haben, das Sie beachten müssen. Wenn Sie jetzt zum Beispiel in Ether tauschen, oder was auch immer Ihr coin letztendlich ist, müssen Sie überlegen, ob Sie eine Bankenlizenz brauchen oder nicht und der der das macht und die Fiat-to-Cryptocurrency conversion macht und wie Sie das vertraglich gestalten ist nicht ganz ohne. Und dann auch wie Sie mit dem Volatilitätsrisiko umgehen, dass eben die Kryptowährung sehr stark, je nachdem in was Sie sie halten, dann im Wert sich ändert. Wenn Sie dann den Schritt gehen und Sie das komplett aus Krypto rausnehmen und machen nur Verrechnungspunkte, die Sie in einem anderen System abgleichen, ist der Mehrwert geringer. Also da gibt es schon substantielle Punkte, die momentan schwierig zu handhaben sind.

A: Das stimmt natürlich, aber das hätte den Umfang des Projektes bisschen gesprengt. Es ging vor allem darum, die Sicherheit von dem Kunden zu haben, dass er erst nach Erhalt und Verifikation der Ware bezahlt, ohne Drittanbieter dazwischen.

E1: Die Frage ist: Wo ist der Mehrwert zu den heutigen Prozessen? Ich mein, das passiert heute ja auch. Unsere Kunden zahlen auch erst dann, wenn sie die Ware haben.

E3: Im B2B ist es halt schwierig, im B2C ist es ersichtlich. Wenn ich im B2C wäre, dann wäre da das Thema, dass ich sicher bin, dass da beim Treuhänder Geld liegt. Die Schwierigkeit tritt immer dann auf, wenn ich Konfliktresolution machen muss. Also in dem Moment, wo wir uns alle einig sind und der Verkäufer brav sagt, dass er die Ware erhalten hat oder man sich vorher einigt, dass wenn DHL-Tracking sag, dass es zugestellt ist, dann wird vom Treuhänder das Geld überwiesen. Dann ist natürlich das Kreditorenrisiko weg und ich habe kein Ausfallrisiko mehr bezüglich der Schuld vom Kunden. Im B2B-Umfeld spielt das aber aus meiner Sicht eine untergeordnete Rolle, weil insbesondere in hierarchisch aufgestellten Lieferketten wie zum Beispiel Automobilindustrie sieht die Lieferbeziehung bisschen anders aus. Wir rechnen ja nicht damit, dass die großen OEMs in Deutschland morgen hops gehen.

E1: Genau. Der Insolvenzfall ist der einzig kritische Fall, alle anderen Fälle sind vertraglich komplett abgesichert.

E3: Konfliktresolution ist auch nicht einfach. Auch das Thema Smart Contracts ist ein Thema, das schwierig in der rechtlichen Dimension ist. Ich mein technisch funktioniert das, das sind Ausführungsbestimmungen (kleines Script), wie der Vertrag abgearbeitet wird. Aber es gibt hochgradige Differenzen momentan, ob wirklich ein Vertragsschluss/Willenserklärung dem dann zugrunde liegt und so weiter. Da haben wir auch noch das Ein oder Andere. Und Konfliktresolution da rein zu programmieren, ist alles andere als trivial. Die Frage ist, ob Sie die richtigen Konditionen finden, auf die man sich einigt. Und am Ende des Tages kann es Ihnen passieren, und das ist die nächste Frage dann, wenn Sie dann automatisch eine Konfliktresolution vornehmen, dann kommt ein Gericht und sagt, dass es aber anders ist. Dann sind Sie dran, die Blockchain zu ändern.
E1: Wir konzentrieren uns jetzt massiv auf das Thema Zahlungsverkehr. Wir haben jetzt noch ein paar Minuten. Es ist die Frage, ob wir das Thema jetzt verlassen. Wir sehen da jetzt nicht den Mehrwert. Wir sehen eher Risiken und Konfliktpotentiale aber keinen erkennbaren Mehrwert zu heute. Eher einen finanziellen Nachteil, indem man praktisch die Werte hinterlegen muss und dann sollten wir uns eher auf den Abwicklungsprozess beziehen und den noch kurz anschauen.
E3: Agreed.
A: Sehe ich auch so. Jetzt geht's einfach um die Tracking-Daten, die anfallen und wie auch immer (Sensoren) automatisiert getrackt werden. Das erfolgt so, dass von den Rohdaten, die zum Beispiel ein Sensor produziert, ein Zeitstempel gemacht wird über OriginStamp. Danach folgt der Upload der verschlüsselten Daten und werden so abgelegt, dass sie von außen zugreifbar sind. Allerdings braucht man natürlich diesen Zugangshashwert und das Verschlüsselungspasswort, ansonsten kann man die Daten nicht mehr entschlüsseln. Die einzelnen Tracking-Daten an sich sind so miteinander verknüpft, dass der zweite Track zum Beispiel den IPFS-Hash und das Verschlüsselungspasswort vom vorherigen Track beinhaltet. So haben wir dann eine Folge von Tracking-Daten. Wenn wir nochmal auf das einfache Beispiel zurückkommen, dass etwas verschickt wird und beim Kunden landet, dann kann der Kunde diese Tracking-Daten dann verifizieren, wenn er vom Hersteller den letzten Tracking-Datensatz bekommt, weil er dann alles rückverfolgbar abrufen kann.
E2: Aber heißt dann auch: Er kann nicht sagen, ob er an Track 2 oder Track 1 ist. Erst am Schluss kann er das Ganze auswerten.
A: Der Hersteller könnte jetzt auch sagen, dass er dem Kunden schon Track 2 mitten im Prozess zur Verfügung stellt. Dann kann der Kunde Track 2 und Track 1 schon anschauen. Er kann auch sagen, dass er dem Kunden jeden Track zur Verfügung stellt, sobald ein neuer erfasst wird. Dann könnte er theoretisch immer wieder diese gesamte Kette abrufen.
E1: Beispiel dafür wie sowas aussieht? Haben Sie mal einen Screenshot?

A: Nicht zur Hand.
E1: Ich frage deswegen, weil letztendlich, wenn wir über ein IT-Design reden, muss ich mich ja in die Rolle des Kunden oder des Lieferanten reinversetzen und fragen: Was sieht er zu welchem Zeitpunkt? Wenn ich Kunde bin aber auch als Lieferant will ich mir keine Gedanken machen, ob ich Track 1, 2 oder 3 bin. Ich will nicht zugreifen können auf Track 1, 2 oder 3. Es ist nicht so, wie man sich das daheim vorstellt, wenn man irgendwo bestellt. Dann kriegt man eine Mail mit einem Link und dann kann man schauen, wo seine Sendung sich gerade befindet. Die Zeit hat in der Industrie keiner. Das heißt, es muss ein System sein, das das Tracking im Hintergrund vollautomatisch durchführt und das einzige, was Kunden und Lieferanten sehen wollen, sind Alerts und Ausnahmemeldungen. Und die dann so zielgerichtet, dass dazu alles gesehen wird. Da will man sich auch nicht durch Track 1, Track 2 oder Track 3 durchkämpfen, sondern ich will sehen, dass es einen Alert für die Materialnummer oder Sendung in dieser Kette gibt und das ist bisher übergreifend passiert. Ich beschleunige jetzt ein bisschen aufgrund von der Zeit. Das ist das, wo wir einen Zusatznutzen hätten.
A: Mit dem aktuellen Prototyp komme ich da natürlich hin. Ich sehe aber durchaus Möglichkeiten und wenig Problem den so auszubauen, dass man da hinkommt, weil wir die Möglichkeit haben, das alles vollautomatisiert zu gestalten. Und auch die Überprüfung (wenn zum Beispiel eine Warnmeldung kommt), dass dann eine extra Meldung an die jeweilige Stelle erfolgt.
E1: Im Prinzip müssen Sie sich das so vorstellen: Wir sind ein Unternehmen mit über 230 Standorten weltweit, mit Millionen Tonnen von Waren, die täglich versendet werden, egal ob im Inbound- oder im Outbound-Bereich. Das heißt, die meisten dieser Lieferungen erfolgen vollautomatisch und auf die Daten schaut niemand. Es ist eine Menge an Informationen. Die werden irgendwann in großen Datenbanken landen und die Hauptfrage, die man sich jetzt stellen muss, ist: Welche Person benötigt zu welchem Zeitraum oder in Eintritt welches Ereignisses Zugriff auf diese Informationen? Und vor allen Dingen: Welche Anspruchhaltung hat man? Das Eine ist wirklich das was ich gesagt habe: im akuten Fall eine Alert-Meldung oder ein Eingriff in die Lieferkette. Das Andere sind diverse Auswert- und Darstellungsmöglichkeiten. Und ich frage eben deswegen, weil das Eine ist technisch, so wie Sie es dargestellt haben, so zu realisieren, dass erst diese Daten erfasst werden und in dieser Datenbank liegen. Das Andere ist, wenn wir über einen Zusatznutzen für uns reden. Dann müssen wir uns natürlich fragen: Was machen wir mit diesem Datengrab? Weil viele Daten zu haben bringt uns in der Anwendung draußen gar nichts. Wir müssen genau überlegen: Was ist der Nutzen dieser Daten? Wie wollen wir zugreifen? Zu welchem Zweck verwenden wir diese? Die IT muss uns dann die entsprechenden Tools an die Hand geben, um diese Daten für uns nutzbar zu machen.

A: Die Auswertung der Daten wäre ja ohne Probleme möglich.
E3: Wenn ich da mal unterbrechen darf. Es wird immer noch nicht ersichtlich, wie der Ansatz für das Thema Lieferketten einen benefit bringt. Weil momentan höre ich raus, wenn ich das richtig verstanden hab von der fachlichen Seite, dass wir aus unserer Sicht keinen need dazu sehen, dass diese Daten in einem System außerhalb unseres Unternehmens gehalten werden, weil wir das alles bilateral intern verwalten und das eigentlich gut funktioniert. Die Frage ist, gibt es durch Ihr System, das sie anbieten, einen Mehrwert über die komplette Lieferbeziehung hinweg. Also von den Zulieferern unserer Zulieferer über uns bis zum OEM sämtliche Tracking-Daten für einen Liefervorgang dann und das daraus entstehende Aggregat (wir bauen ja aus einzelnen Komponenten unsere Komponente, die dann wieder in das Auto gebaut etc. pp.), dass die in dieser Blockchain für alle sichtbar, teils verschlüsselt oder auch nicht, dann existiert. Und die Frage ist: Ist der Zusatzaufwand durch einen Mehrwert gerechtfertigt? Das wäre ja die grundsätzliche Frage.
E1: Anders herum. Wir werden bei uns auch solche Datenbanken aufbauen. Wir werden genau das machen, genau das ist konzipiert. Aber wir werden die in irgendeinen Data Lake schmeißen. Da reden wir nicht über Blockchain, da reden wir über irgendwelche Big Data Technologien.
E3: Die wesentlicher günstiger sind.
E1: Die Frage ist natürlich: Welchen Vorteil hätte eine Blockchain-Technologie im Vergleich zu einer konventionellen Technologie, wo wir einfach im Wareneingang/ -ausgang von den Spediteuren unsere Meldepunkte nehmen und praktisch diese Trigger-Punkte und Buchungsdaten, die weltweit generiert werden, in diese Datenbank schreiben und diese Datenbank auswerten (auch mit Heuristiken, KI und mit allem, was da dazugehört). Ich habe immer noch nicht den Link zur Blockchain.
E3: Ich auch nicht. Und was ich sagen wollte, ist: Wenn man es an der abstrakten Ebene packt, ist Blockchain auch eine Art der Datenhaltung, genauso wie es eine Datenbank ist, nur dass diese Datenhaltung eben außerhalb der Einflusssphäre von unserem Unternehmen in der Blockchain ist. Wenn ich in die Ethereum-Blockchain was reinschreibe ist es einfach bei der Ethereum-Foundation und allen Rechnern auf der Welt, die daran teilnehmen, vorhanden. Ich kann es noch verschlüsseln, aber faktisch sind es Daten, die außerhalb in einer Datenhaltung gehalten werden. Und die Frage ist es eben für uns: Was ist der konkrete Mehrwert davon? Denn es ist auch deutlich teurer. Ich kann Ihren Ansatz total verstehen in der Pharma, wo es, nicht für Lieferketten aber für auditibility, für den Fall, dass einer hops geht, enorm wichtig ist, dass ich nachvollziehen kann, dass in der Lieferkette da und da die Temperatur nicht gepasst hat und dass jeder Hersteller das nachweisen kann. Dann haben wir noch nicht

Cyber-Physical Threshold diskutiert, das heißt, wenn Sie quasi vom Sensor garbage kriegen oder jemand in der Kette das manipuliert, bevor es in die Blockchain geht, dann haben Sie garbage gestempelt. Aber für uns scheint das momentan jetzt schwierig zu sein diesen Schritt zu gehen, wo der Mehrwert für uns liegt. Das sind jetzt sehr abstrakte Geschichten.
A: Ich kann das nachvollziehen und verstehen, was Sie damit meinen. Wenn man sowas anfängt zu designen hatte ich immer das Bild von sensibleren Daten im Hinterkopf und im speziellen Fall bei Ihnen: Es kommt immer drauf an, was man nachweisen muss und was man nachweisen möchte in Lieferketten. Was mit den Tracking-Daten geschieht und was nicht geschieht. In Ihrem Fall sehe ich das natürlich auch, dass es da keinen Nutzen gibt, wenn Sie zum Beispiel den Bezahlvorgang über eine Blockchain abwickeln. Ganz zu schweigen von den Problemen, die das mit sich bringt.
E3: Ein Risiko, das ich Ihnen noch mitgeben wollte für Ihr weiteres Denken, ist natürlich auch: Können Sie sicher ausschließen, dass durch eine Metaanalyse Geschäftsmuster nach außen dringen? Ich mein, da sind ja Metadaten drin. Man würde zum Beispiel sehr transparent in Ethereum erkennen können mit wem wir Lieferbeziehungen haben, wie viel wir darüber machen (hängt von Verschlüsselung der Daten ab) aber Sie könnten aus der Frequenz und anderen Sachen schon Schlüsse ziehen, wie wir unser Geschäftsmodell aufbauen. Das ist durchaus möglich.
A: Das ist natürlich ein allgemeines Problem, wenn man auf öffentlichen Blockchains operiert. Das Problem hat man immer. Auf der anderen Seite sehe ich keinen Nutzen, wenn man letztendliche eine private Blockchain benutzt, weil da hat man keine benefits in dem Sinn.
E3: Nö. Aber die Frage ist: Muss ich Blockchains überhaupt benutzen?

B.3.6 *Expert Interview 6*

A: Ich habe das Interview so gegliedert, dass es drei Teile gibt: anfangs einleitende Fragen, dann stelle ich mein entwickeltes Konzept kurz vor und danach im dritten Teil Fragen dazu. Erstmal eine einleitende Frage: Wie werden Produkte bei euch verfolgt beziehungsweise welche Technologien setzt ihr da ein? Auf was wird eventuell besonders wert gelegt wird?
E: Mir ist der Kontext unklar. Was meinst du denn? Bei uns direkt? Was genau meinst du? Denn ein Auto ist ziemlich komplex. Meinst du einzelne Bauteile, meinst du die Telematik oder das Gesamte? Da gibt es so viel Einsatzgebiete und das ist so unterschiedlich, deswegen verstehe ich das nicht, in welchem Kontext du das siehst.
A: Dann ist die Frage eventuell missverständlich. Es sollte eher generell auf die Produktverfolgung abzielen. Alternativ könnte man die Frage auch so formulieren, dass sie allgemein gestellt bleibt. Wie würdest du Produktver-

folgung gestalten (du selbst) und welche Technologien würdest du einsetzen und auf was würdest du besonders achten?
E: Was ist es jetzt? Ist es industriegetrieben oder meine allgemeine Einstellung?
A: Grundsätzliche deine Einstellung.
E: Okay, das heißt, wie ich Produkte tracken würde beispielsweise?
A: Genau.
E: Okay. Also ich verbinde das einfach, weil es nicht mein Fokus ist tatsächlich Produkte zu tracken. Aber in der Industrie werden ganz normale Barcodes, die standardisiert sind, verwendet. Das sind Seriennummern, sogenannte vehicle identification numbers, die einfach von Zulieferer bis hin zum Produkt ziemlich transparent sind in der Automobilbranche. Getrackt werden sie durch optische Scanner. Es gibt zentrale Tools mit Datenbanken, die sich gegenseitig synchronisieren. Das ist dann immer ein Etikett auf einzelnen Komponenten drauf und werden so getrackt. Da ist auch ständig die Bemühung da, das automatisiert machen zu können. Aber aufgrund der Situation der Zulieferer und dass da noch kein Standard etabliert ist, dass die sich daran halten müssten (es gibt viele, die standardisiert und zertifiziert sind), bekommt man das noch nicht richtig hin. Deswegen bleibt es immer noch bei diesen Etiketten mit Barcodes und den Scannern. Die sind auch in den Maschinen drin beim Zusammenbauen von dem Fahrzeug selbst. In dem Moment, wo ich quasi zwei Bauteile zusammensetze, dann wird das Eine mit dem Anderen gescannt. Das kannst du auch dann nur scannen in dem Moment, wo du es zusammenklippst. So ist auch der Nachweis gegeben, dass es geklippst wurde beispielsweise. Aber das sind alles optische Scanner, die Etiketten abscannen. In der Automobilbranche ist die Gefahr nicht so da, dass da Fake-Produkte drin sind. Das ist nicht so wie bei anderen Produkten.
A: Der Barcode beziehungsweise die ID bleibt über die verschiedenen Stationen hinweg gleich oder wird die durchaus auch mal geändert?
E: Du meinst die Stationen von einem Bauteil?
A: Ja. Wenn man jetzt ein Bauteil hat und ihr bekommt das über Zulieferer oder wie auch immer. Ändert sich die ID oder wird die ID übergreifend genutzt?
E: Der Aufbau der ID wechselt natürlich, aber nicht bei jeder Station.
A: Weißt du zufällig, welche Kosten ungefähr durchschnittlich bei einem Produkt nur für dessen Nachverfolgbarkeit im Verhältnis zu dessen Wert anfallen?
E: Kann ich dir leider nicht beantworten. Ich befinde mich ja nicht in der Abteilung, die jetzt diese Nachverfolgbarkeit überhaupt forciert, vor allem nicht bei physischen Produkten.
A: Welche Anforderungen stellst du an Lieferkettenprozesse im Allgemeinen? Was muss ein Lieferkettenprozess erfüllen?
E: Grundsätzlich ist für mich wichtig, dass ich keine Brüche habe und

dass ich die komplette Transparenz habe und dass ich in real-time on demand jederzeit den Status erfragen kann. Also dass ich keinen Zeitpunkt im Idealfall in der Kette habe, der quasi leer ist, der nicht nachvollziehbar ist. Dann kommt es natürlich darauf an, welches Objekt ich da tracke. Dann kommen natürlich die Metainformationen, die relevant sein könnten, zum Beispiel Kühlkette oder bei irgendwelchen Komponenten, zum Beispiel bei Ledersitzen, dass da keine kleinen Kinder das Leder gegerbt haben (in einem Land, was keine Regelungen dazu hat). Im Endeffekt geht es mir um die Transparenz und dass zu jedem Zeitpunkt der Status abgleichbar wäre.

A: In diesem Fall hat Transparenz für dich den höchsten Stellenwert in der Lieferkette. Wie würdest du es einschätzen, welchen Stellenwert eine Lieferkette letztendlich hat (auch bezogen auf die Automobilbranche)? Generell für das Unternehmen selbst aber auch für die Kunden?

E: Man bezieht sich nicht darauf, dass man irgendwie minder oder schlecht produzierte Bauteile im Premium-Segment bezieht. Und dadurch ist eben gesichert, dass es keine Produkte aus dem Hinterhof aus irgendeinem Land hat, sodass eben die Wichtigkeit ist natürlich da und steigen, weil die Gesellschaft Transparenz verlangt. Das wird auch Marketing-Aspekte sein. Der Konzern stellt sich auch in die Richtung ein, dass man nachhaltige Produkte vertreibt, das wird immer mehr. Da gibt es auch genug Initiativen, die das nach außen kommunizieren. Aber für den Kunde ist das im Premium-Segment das Mindeste. Der Kunde erwartet, dass ein Premium-Fahrzeuge dafür garantiert, dass jedes Bauteil mit einer entsprechenden Qualität hergestellt wurde und auch verbaut wurde. Das ist immer wichtiger und das ist die Aussage, die ich treffen kann. Man merkt, dass ziemlich viele Initiativen gebildet werden, die da eben die Transparenz als Vertriebs- oder Marketingzweck hinzuziehen. Aber eigentlich wäre es nicht wichtig im Premium-Segment, weil beim Kunden das setting sowieso da ist. Der braucht beim Premium-Segment kein extra Bioaufkleber beispielsweise, weil dieser schon impliziert ist.

A: Sehr interessant. Jetzt noch die letzte allgemeine Frage bezogen auf die Blockchain-Technologie. Bist du schon mal mit der Blockchain-Technologie in Berührung gekommen? Wenn ja, wie und wann?

E: Bei mir ist es so, dass ich durch den Master an der Universität Konstanz mit der Blockchain-Technologie in Berührung gekommen bin. In dem Konzern war ich ziemlich schnell aufgrund meiner Vorbildung in dem inneren Kreis dieser Technologie. Die Technologie wurde natürlich auch untersucht im Konzern für sämtliche use cases. Da gibt es Austausch-Workshops, wo man sich mit unterschiedlichen Bereichen zusammensetzt. Proof-of-concept (Prototypen) werden gemeinsam entwickelt oder zumindest mal an den Start bringt. Also erster Kontakt an der Universität Konstanz durch den Master durch die Betreuung von Bela Gipp und im Konzern durch die sämtlichen Bereiche, die ihre eigenen Anforderungen haben.

A: Wunderbar. Jetzt komme ich zur Präsentation von meinem Prototyp. OriginStamp kennst du nehme ich an?
E: Klar.
A: IPFS auch, oder?
E: Ja.
A: Gut, dann geht es nur noch um HTLC, die ich verwendet hab. Kennst du die?
E: Ja. Ich habe selber noch keinen definiert, habe aber davon gelesen.
A: Dir ist das Prinzip mit dem Hashlock und dem Timelock bekannt wie es funktioniert?
E: Ja.
A: Dann stelle ich dir den Prototypen gleich mal vor. Ich habe folgende Unterteilung vorgenommen: Bestellvorgang, Tracking und den eigentlichen Bezahlvorgang. Der Bestellvorgang funktioniert folgendermaßen: Ich habe das Ganze mit zwei Parteien modelliert, Kunde und Verkäufer. Der Prototyp steht zwischen Kunde und Verkäufer, ist also ein Drittanbieter. Der Kunde beginnt damit, dass er natürlich ein Produkt beim Verkäufer bestellt. Sobald das Produkt bestellt ist, überweist der Kunde dann an den Prototyp den gewissen Betrag vom Verkäufer und inkludiert in die Transaktion (über Kryptowährung) einen Hash-Wert, der sich wiederum aus einem selbstgesetzten Passwort und der Mail vom Kunden zusammensetzt. Das dient zur Absicherung, dass der Verkäufer die Transaktion erst dann nutzen kann, wenn er die E-Mail vom Kunden weiß und das Passwort ebenfalls. Sobald die Transaktion durch ist, schickt er Kunde das Passwort aus der Transaktion dem Verkäufer, damit dieser das verwenden kann. Der Verkäufer initiiert dann das neue item/Bestellung beim Prototyp dadurch, dass er Transaktionshash, Passwort und Mail vom Kunden angibt. Wenn diese Informationen stimmen, dann kreiert Bloctrack (Prototyp) einen HTLC zwischen dem Kunden und dem Verkäufer und schickt dann an den Kunden wiederum diese ganzen Informationen aus dem HTLC, damit der Kunde die volle Kontrolle über sein Geld behält. War das verständlich?
E: Ja, ich kann dir folgen.
A: Okay. Dann ist das item erstellt und als nächster Schritt folgt die Trackingphase. Zum Beispiel wird ein Paket versendet und währenddessen fallen irgendwelche Tracking-Daten an, zum Beispiel gibt es einen Temperatursensor, der automatisch die Daten trackt. Das Tracking läuft aktuell über den Prototyp und da werden die Tracking-Daten erstmal unverschlüsselt getimestamped über OriginStamp und dann werden die Daten verschlüsselt über IPFS hochgeladen. Das läuft dann so weiter und zusätzlich wird noch im aktuellen Track der IPFS hash und das encryption password vom vorherigen Track mit reingenommen. Letztendlich haben wir eine Blockchain von Tracking-Daten. Wenn das item dann verschickt wird und ankommt, dann braucht der Kunde vor der Warenannahme die Tracking-Daten mit Hilfe des letzten Tracks verifizieren. Wenn er die verifizieren kann, dann gilt „Ware gegen Preimage" (Passwort aus dem Hashlock). Sobald der Kunde die Ware annimmt, muss er das Preimage an den Verkäufer schicken/geben. Dann

kann der Verkäufer direkt den contract vervollständigen und bekommt sein Geld und der Kunde hat seine Ware. Was zusätzlich noch gemacht wurde, ist, dass die gesamten abgebildeten Prozesse ohne den Prototyp verifizierbar sind. Die Tracking-Daten sind ohne den Prototyp erreichbar und verifizierbar, die ganzen Timestamps sowieso. Eine Sache, was für die Verifikation noch wichtig ist, ist, wenn der HTLC erstellt wird, dann wird auch wieder ein Zeitstempel aus dem Transaktionshash, aus der contract ID vom HTLC und von der internen item ID von Bloctrack zusammen. Das hat den Grund, dass der Kunde nachweisen kann, dass seine Transaktion zum Beispiel schon verwendet wurde und der Verkäufer keine Transaktion zweimal verwenden kann. Das Tracking an sich habe ich über einen QR code und eine App realisiert, die wiederum den Prototyp über die API anspricht. Das ist das umgesetzte Konzept. Hast du dazu noch Fragen?

E: Vielleicht hast du es gesagt und ich habs nur nicht verstanden. Könnte ich rein theoretisch mitten in einem Trackingprozess (Produkt bei 60% des Lieferweges) als Kunde auf die Daten zugreifen? Soweit ich es verstanden hab erfolgt der Zugriff auf die Daten erst am Ende.

A: Der Verkäufer kann den letzten Track jederzeit dem Kunden zur Verfügung stellen und der Kunde kann jederzeit die gesamte (bis hierhin vorhandene) Blockchain von Tracking-Daten anschauen. Das ist durchaus möglich.

E: Rein rechtlich ist es ja so: In dem Moment, wo ich es kaufe und mir zusenden lasse, ab wann ist denn der Eigentumswechsel? Wann gehört mir das?

A: Habe ich mich nicht weiter damit beschäftigt.

E: Das wäre in meinen Augen ein interessanter Aspekt, weil die Daten des Trackings zu welchem Zeitpunkt wem gehören würde mich interessieren. Wir haben gerade gesagt, dass der Verkäufer die Daten der Position des Produkts, welches eigentlich schon bezahlt ist, hat. Es ist ja eigentlich schon abgezogen vom Käufer und der hat sein Geld schon los, hat aber noch nicht mal die Daten von dem Status. Da stellt sich halt für mich die Frage, ob die Daten nicht dem Verkäufer gehören, sondern irgendwie so schon zugänglich wären. Das war der einzige Punkt, alles andere hab ich soweit verstanden.

A: Das ist tatsächlich ein interessanter Punkt. Effektiv hat der Verkäufer ja noch kein Geld vom Kunden bekommen. Das bekommt er ja erst, wenn er das Preimage aus dem HTLC bekommt. Das bekommt er ja erst bei der Übergabe („Ware gegen Preimage").

E: Der ist also das Risiko eingegangen und hat es einfach weggeschickt.

A: Ja, wobei er schon weiß, dass das Geld da ist, weil der Kunde es ja sozusagen an den contract an sich da ist. Aber klar, wenn der Kunde das Preimage nicht rausrückt, kann es ein Problem geben. Allerdings haben wir da jetzt den Vorteil, dass der Prototyp ein Drittanbieter ist, weil da könnte man durchaus in das System eingreifen. Die Daten sind zumindest teilweise beim Prototyp hinterlegt und dass man dann die Daten über den Prototyp ausliest und es außerhalb regelt. Diese Möglichkeit gäbe es schon.

E: Gut, dann habe ich das soweit verstanden.
A: Dann wäre es super, einen ersten Eindruck von dir zu hören.
E: Feedback zum Prototyp?
A: Genau.
E: Okay, also dadurch, dass ich mir das alles im Kopf rekonstruieren muss, ist das bisschen schwierig. Ich habe mich ja schon selber mit den Architekturen auseinandergesetzt. Zwar nicht coding-technisch, aber von dem Aufbau der Architektur. Ja, ich find das gut. Ich find auch diesen zeitlichen Aspekt der contracts ganz gut. Bis auf diese Rückfrage mit der Abbildung des Prozesses... Es ist auf jeden Fall ein guter Einstieg, man müsste auf jeden Fall die juristischen Seiten und rechtlichen Aspekte bei einem Kauf übereinstimmen und ich weiß nicht, ob das da so eingehalten werden kann. Ansonsten vom Aufbau finde ich es gut. Von dem Prototyp, von dem du sprichst: Wie kann ich mir den vorstellen? Es ist ein Konsortium von Drittanbietern? Oder ist es eine zentrale Stelle, die das verwaltet?
A: Es ist aktuell so, dass es eine zentrale Stelle ist. Es läuft so, dass es users gibt (Verkäufer), die darüber verwaltet werden. Das ist auch ein großes Problem natürlich, weil da verlieren wir einige Aspekte von den Vorteilen von der Dezentralisierung durch diese Zentralisierung.
E: Wie argumentiert ihr, dass man das braucht? Warum hast du dich beim Design dazu entschieden, das so zu machen? Warum hast du ihn als zentrale Instanz entworfen? Dein Fokus war wahrscheinlich auch nicht darauf.
A: Der Fokus war bei dem Prototyp die Technologien und die verschiedenen Ansätze, die ich integriert habe (IPFS, HTLC und OriginStamp), sinnvoll zu integrieren und letztendlich eine Vertrauensoptimierung zwischen den Parteien zu bekommen und zu dezentralisieren. Die Verifikation ohne jegliche Drittanbieter soll letztendlich unter anderem die Transparenz erhöhen. Das war der Hauptfokus. Das Problem, dass es ein Drittanbietersystem ist, war uns schon bewusst. Es gibt die Möglichkeit, ein Netzwerk aus diesem Prototyp herzustellen, sodass jeder Verkäufer und jeder Käufer wie eine node unterhält. Diese nodes können untereinander kommunizieren und die HTLC werden abgewickelt. So war es aber für Demonstrations- und Evaluationszwecke erstmal auch am Praktikabelsten und Einfachsten.
E: Okay. Es ist echt ein gutes Konzept. Und das ist auch funktionsfähig?
A: Ja klar, das ist so implementiert. Das war ja mein Bachelorprojekt. In der Bachelorarbeit habe ich das weitergesponnen. Siehst du spontan Schwächen oder Limitierungen, abgesehen von der Modellierung als Drittanbieter?
E: Von dem Konzept an sich nicht, aber man müsste einfach damit spielen und ausprobieren (Performance testen, ...). Ansonsten nein. Im Endeffekt sind es ja diese Konzepte, die als Proof-of-concept gemacht werden in der Industrie.
A: Wie schätzt du die Bedenken von Unternehmen ein, auf einer öffentlichen Blockchain zu operieren? Wie ist da die Bereitschaft?

E: Die ist eigentlich gar nicht da, weil da kein Vertrauen ist. Meine persönliche Meinung ist, dass ich es nicht verstehe. Man kann sehr wohl die Daten öffentlich zur Verfügung stellen, weil man eine gewissen Glaubwürdigkeit damit erlangt. Aber die Positionen, die das entscheiden, sind überhaupt nicht offen dafür, Daten freizugeben. Das höchste aller Gefühle ist, dass sich Konsortien bilden. In public blockchains wird höchstwahrscheinlich nichts gespeichert. Das ist so meine Wahrnehmung.

A: In diesem Fall siehst du es schon so, dass der Prototyp Transparenz und aber auch Vertrauen zwischen den Parteien optimiert oder zumindest verbessert?

E: Die Transparenz auf jeden Fall, aber die ursprünglich abgefragten wichtigsten Aspekte wären ja, dass ich zu jedem Zeitpunkt einen Status abfrage. Und der ist halt ziemlich einseitig gelöst in diesem Konzept, weil ich abhängig von dem Willen dieser einen Partei bin. Die Daten sind also nicht in der Luft und man kann darauf zugreifen, sondern die gehören immer noch der einen Partei, die die Freiheit hat, ob sie die zur Verfügung stellt oder nicht. Aber wahrscheinlich ist es nur eine Implementationsfrage, hätte man wahrscheinlich auch anders lösen können. Aber ansonsten ja, kann ich so zustimmen.

BIBLIOGRAPHY

[1] Saveen A. Abeyratne. "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger." In: *International Journal of Research in Engineering and Technology* 05.09 (2016), pp. 1–10. ISSN: 23217308. DOI: 10.15623/ijret.2016.0509001. URL: http://esatjournals.net/ijret/2016v05/i09/IJRET20160509001.pdf.

[2] Naif Alzahrani and Nirupama Bulusu. "Block-Supply Chain: A New Anti-Counterfeiting Supply Chain Using NFC and Blockchain." In: (2018), pp. 30–35. DOI: 10.1145/3211933.3211939. URL: https://doi.acm.org/10.1145/3211933.3211939.

[3] M. Antonopoulos Andreas. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies - Andreas M. Antonopoulos - Google Books*. 2014. ISBN: 978-1-449-37404-4. URL: https://books.google.de/books?hl=en&lr=&id=IXmrBQAAQBAJ&oi=fnd&pg=PR4&dq=+A.M.+Antonopoulos&ots=9BaVqtHnNZ&sig=CKNtb7QKUD-DH3As6i7V3zRgcVY&redir_esc=y#v=onepage&q=A.M.Antonopoulos&f=false.

[4] L. M (Rochester Institute of Technology) Bach, B. (Rochester Institute of Technology) Mihaljevic, and M. (Rochester Institute of Technology) Zagar. "Comparative Analysis of Blockchain Consensus Algorithms." In: *MIPRO* (2018), pp. 1545–1550.

[5] Juan Benet and Juan@benet Ai. "IPFS -Content Addressed, Versioned, P2P File System (DRAFT 3)." In: *Proceedings - International Conference on Distributed Computing Systems* 45.July 2017 (2017), pp. 1–6. ISSN: 1063-6927. DOI: 10.1145/2980137.2980141. URL: http://dl.acm.org/citation.cfm?doid=2831347.2831354%0Ahttp://arxiv.org/abs/1805.06411%0Ahttp://dl.acm.org/citation.cfm?doid=2980137.2980141.

[6] Rafael Bettín-Díaz, Alix E. Rojas, and Camilo Mejía-Moncayo. "Methodological approach to the definition of a blockchain system for the food industry supply chain traceability." In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 10961 LNCS (2018), pp. 19–33. ISSN: 16113349. DOI: 10.1007/978-3-319-95165-2{_}2. URL: http://link.springer.com/10.1007/978-3-319-95165-2_2.

[7] BitFury Group. "Proof of Stake versus Proof of Work." In: 2015 (2015), pp. 1–26. URL: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf.

[8] BitInfoCharts. *Bitcoin Avg. Transaction Fee historical chart*. 2018. URL: https://bitinfocharts.com/comparison/bitcoin-transactionfees.html.

[9] Thomas Bocek, Bruno B. Rodrigues, Tim Strasser, and Burkhard Stiller. "Blockchains everywhere - A use-case of blockchains in the pharma supply-chain." In: *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management* (2017), pp. 772–777. DOI: 10.23919/INM.2017.7987376.

[10] AA Boschi, R Borin, JC Raimundo, and A Batocchio. "An exploration of blockchain technology in supply chain management." In: October (2018), pp. 0–12. URL: https://www.repository.cam.ac.uk/bitstream/handle/1810/284353/8_-_an_exploration_of_blockchain_technology_in_supply_chain_management.pdf?sequence=1.

[11] Vitalik Buterin and others. "A next-generation smart contract and decentralized application platform." In: *white paper* (2014).

[12] Miguel Pincheira Caro, Muhammad Salek Ali, Massimo Vecchio, and Raffaele Giaffreda. "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation." In: *2018 IoT Vertical and Topical Summit on Agriculture - Tuscany, IOT Tuscany 2018* (2018), pp. 1–4. ISSN: 23146141 23146133. DOI: 10.1109/IOT-TUSCANY.2018.8373021.

[13] Roberto Casado-Vara, Javier Prieto, Fernando De La Prieta, and Juan M. Corchado. "How blockchain improves the supply chain: Case study alimentary supply chain." In: *Procedia Computer Science* 134 (2018), pp. 393–398. ISSN: 18770509. DOI: 10.1016/j.procs.2018.07.193. URL: https://doi.org/10.1016/j.procs.2018.07.193.

[14] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: current status, classification and open issues." In: *Telematics and Informatics* (2018). ISSN: 07365853. DOI: 10.1016/j.tele.2018.11.006. URL: https://linkinghub.elsevier.com/retrieve/pii/S0736585318306324.

[15] Jasmine Aichih Chang, Michael N Katehakis, Benjamin Melamed, and Jim Shi. "Blockchain Design for Supply Chain Management." In: *Ssrn* January 2019 (2018), pp. 1–35. ISSN: 1556-5068. DOI: 10.2139/ssrn.3295440. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3295440.

[16] Konstantinos Christidis and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." In: *IEEE Access* 4 (2016), pp. 2292–2303. ISSN: 21693536. DOI: 10.1109/ACCESS.2016.2566339.

[17] Gabriela B. Christmann. "Expert Interviews on the Telephone: A Difficult Undertaking." In: *Interviewing Experts* (2009), pp. 157–183. ISSN: 1098-6596. DOI: 10.1057/9780230244276{_}8. URL: http://link.springer.com/10.1057/9780230244276_8.

[18] Martin Christopher, Helen Peck, and Denis Towill. "A Taxonomy for selecting global supply chain strategies." In: *International Journal of Logistics Management* (2006), pp. 277–287.

[19] Corrado Costa, Francesca Antonucci, Federico Pallottino, Jacopo Aguzzi, David Sarriá, and Paolo Menesatti. "A Review on Agri-food Supply Chain Traceability by Means of RFID Technology." In: *Food and Bioprocess Technology* 6.2 (2013), pp. 353–366. ISSN: 19355130. DOI: 10.1007/s11947-012-0958-7.

[20] Kyle Croman et al. "On Scaling Decentralized Blockchains." In: *Physics Letters, Section B: Nuclear, Elementary Particle and High-Energy Physics* 773 (2017), pp. 106–125. ISSN: 03702693. DOI: 10.1016/j.physletb.2017.08.011.

[21] Yao Cui, Ming Hu, and Jingchen Liu. "Values of Traceability in Supply Chains." In: November (2018).

[22] Hongyan Dai, Ling Ge, and Weihua Zhou. "A design method for supply chain traceability systems with aligned interests." In: *International Journal of Production Economics* 170 (2015), pp. 14–24. ISSN: 09255273. DOI: 10.1016/j.ijpe.2015.08.010. URL: http://dx.doi.org/10.1016/j.ijpe.2015.08.010.

[23] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, E. Riva Sanseverinc, G. Sciume, and G. Zizzo. "An Energy Blockchain, a Use Case on Tendermint." In: *Proceedings - 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe, EEEIC/I and CPS Europe 2018* (2018). DOI: 10.1109/EEEIC.2018.8493919.

[24] Davor Dujak and Domagoj Sajter.
Blockchain Applications in Supply Chain.
Springer International Publishing, 2019, pp. 21–46.
ISBN: 978-3-319-91667-5. DOI: 10.1007/978-3-319-91668-2.
URL:
http://link.springer.com/10.1007/978-3-319-91668-2.

[25] Magdi ElMessiry and Adel ElMessiry. "Blockchain
Framework for Textile Supply Chain Management."
In: 10974 (2018), pp. 213–227. ISSN: 09608524.
DOI: 10.1007/978-3-319-94478-4. URL:
http://link.springer.com/10.1007/978-3-319-94478-4.

[26] Ittay Eyal, Adem Efe Gencer, Emin Gun Sirer, and
Robbert van Renesse.
"Bitcoin-NG: A Scalable Blockchain Protocol." In: (2015).
URL: http://arxiv.org/abs/1510.02037.

[27] Simone Figorilli et al. "A blockchain implementation
prototype for the electronic open source traceability of wood
along the whole supply chain."
In: *Sensors (Switzerland)* 18.9 (2018), pp. 1–12. ISSN: 14248220.
DOI: 10.3390/s18093133.

[28] Kristoffer Francisco and David Swanson.
"The Supply Chain Has No Clothes: Technology Adoption of
Blockchain for Supply Chain Transparency."
In: *Logistics* 2.1 (2018), p. 2. ISSN: 2305-6290.
DOI: 10.3390/logistics2010002.
URL: http://www.mdpi.com/2305-6290/2/1/2.

[29] Vincent Fremont and Gideon Mekonnen Jonathan.
"Can blockchain technology solve trust issues in industrial
networks?"
In: *CEUR Workshop Proceedings* 2218 (2018), pp. 399–404.
ISSN: 16130073.

[30] Gilbert Fridgen, Florian Guggenmos, Jannik Lockl,
Alexander Rieger, André Schweizer, and Nils Urbach.
"Developing an Evaluation Framework for Blockchain in the
Public Sector: The Example of the German Asylum Process."
In: *Proceedings of the 1st ERCIM Blockchain Workshop 2018,
Reports of the European Society for Socially Embedded Technologies*
10 (2018), pp. 1–8. ISSN: 2510-2591.
DOI: 10.18420/blockchain2018.
URL: https://dl.eusset.eu/bitstream/20.500.12015/3157/
1/blockchain2018_10.pdf%0Ahttps://www.fim-
rc.de/Paperbibliothek/Veroeffentlicht/756/wi-756.pdf.

[31] Bela Gipp, Norman Meuschke, and André Gernandt. "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin." In: February (2015). URL: http://arxiv.org/abs/1502.04015.

[32] Bigchaindb Gmbh. "A BigchainDB Primer." In: May (2017), pp. 1–9. URL: https://www.bigchaindb.com/whitepaper/bigchaindb-primer.pdf.

[33] Laura Sánchez González, Félix García Rubio, Francisco Ruiz González, and Mario Piattini Velthuis. "Performance improvement of manufacturing supply chain using back-up supply strategy." In: *Journal of Service Management* 26.2 (2015), pp. 182–205. ISSN: 0957-4093. DOI: 10.1108/MBE-09-2016-0047. URL: http://dx.doi.org/10.1108/JOSM-12-2014-0323.

[34] Ian Gorton, John Klein, and Albert Nurgaliev. "Architecture Knowledge for Evaluating Scalable Databases." In: *Proceedings - 12th Working IEEE/IFIP Conference on Software Architecture, WICSA 2015* (2015), pp. 95–104. DOI: 10.1109/WICSA.2015.26.

[35] Dominique Guegan. "Public Blockchain versus Private blockhain Centre d ' Economie de la Sorbonne Documents de Travail du Public Blockchain versus Private blockhain." In: (2017).

[36] N. Hackius and M. Petersen. "Blockchain in Logistics and Supply Chain: Trick or Treat?" In: *Proceedings of the Hamburg International Conference of Logistics* October (2017), p. 23. ISSN: 2365-5070. DOI: 10.15480/882.1444. URL: https://tubdok.tub.tuhh.de/bitstream/11420/1447/1/petersen_hackius_blockchain_in_scm_and_logistics_hicl_2017.pdf.

[37] Mohamad Ghozali Hasan, Kamal Imran Sharif, and Mahadi Hasan Miraz. "Supply Chain Management for Garments Industries Using Blockchain in Bangladesh." In: *Journal of Business Management and Economic Research* 2.8 (2018), pp. 13–20. ISSN: 2602-3385. DOI: 10.29226/TR1001.2018.54. URL: http://jobmer.org/2018/vol2_issue8_article2_fulltext.pdf.

[38] Vaibhav Hatiskar and Archana G Pai. "Blockchain and it's Integration with Supply Chain." In: *International Journal of Computer Applications* 179.52 (2018), pp. 20–24.

[39] Thomas Hepp, Matthew Sharinghousen, Philip Ehret, Alexander Schoenhals, and Bela Gipp. "On-chain vs. off-chain storage for supply- and blockchain integration."

In: *it - Information Technology* 60.5-6 (2018), pp. 283–291. ISSN: 2196-7032. DOI: 10.1515/itit-2018-0019. URL: http://www.degruyter.com/view/j/itit.2018.60.issue-5-6/itit-2018-0019/itit-2018-0019.xml.

[40] Thomas Hepp, Alexander Schoenhals, Christopher Gondek, and Bela Gipp. "OriginStamp : A blockchain-backed system for decentralized trusted timestamping." In: (2018).

[41] Thomas Hepp, Patrick Wortner, Alexander Schönhals, and Bela Gipp. "Securing Physical Assets on the Blockchain Linking a novel Object Identification Concept with Distributed Ledgers." In: *Proceedings of 1st CryBlock* (2018), pp. 60–65. DOI: 10.1145/3211933.3211944.

[42] Thomas Hepp, Gordana Marmulla, Alexander Schoenhals, Philip Ehret, and Bela Gipp. "Towards Scalability of Distributed Ledgers using Directed Acyclic Graphs." unpublished. 2018.

[43] Charles Herder, Meng Day Yu, Farinaz Koushanfar, and Srinivas Devadas. "Physical unclonable functions and applications: A tutorial." In: *Proceedings of the IEEE* 102.8 (2014), pp. 1126–1141. ISSN: 00189219. DOI: 10.1109/JPROC.2014.2320516.

[44] Charles Herder, Meng Day Yu, Farinaz Koushanfar, and Srinivas Devadas. "Physical unclonable functions and applications: A tutorial." In: *Proceedings of the IEEE* 102.8 (2014), pp. 1126–1141. ISSN: 00189219. DOI: 10.1109/JPROC.2014.2320516.

[45] Erik Hofmann, Urs Magnus Strewe, and Nicola Bosia. "Supply Chain Finance and Blockchain Technology." In: (2018). DOI: 10.1007/978-3-319-62371-9. URL: http://link.springer.com/10.1007/978-3-319-62371-9.

[46] Jinyou Hu, Xu Zhang, Liliana Mihaela Moga, and Mihaela Neculita. "Modeling and implementation of the vegetable supply chain traceability system." In: *Food Control* 30.1 (2013), pp. 341–353. ISSN: 09567135. DOI: 10.1016/j.foodcont.2012.06.037. URL: http://dx.doi.org/10.1016/j.foodcont.2012.06.037.

[47] Lijuan Huang, Qiaoqiao Luo, Peng Yu, and Guoping Yu. "Designing and planning agricultural supply chain traceability system based on modern RFID technology." In: *Proceedings 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, MEC 2011* (2011), pp. 2112–2118. DOI: 10.1109/MEC.2011.6025908.

[48] IBM.
"The Benefits of Blockchain to Supply Chain Networks."
In: (2017), pp. 1–4. URL: https://www-01.ibm.com/software/commerce/offers/pdfs/Blockchain_3-15-2017.pdf.

[49] Arman Jabbari and Philip Kaminsky.
"Blockchain and Supply Chain Management."
In: January (2018). URL: http://www.mhi.org/downloads/learning/cicmhe/blockchain-and-supply-chain-management.pdf.

[50] André Jeppsson and Oskar Olsson.
"Blockchains as a solution for traceability and transparency."
In: (2017). URL: https://lup.lub.lu.se/student-papers/search/publication/8919957.

[51] Lukáš KUBÁČ.
"RFID Technology and Blockchain in Supply Chain."
In: LXIV.1 (2018), pp. 35–44.
URL: http://shodhganga.inflibnet.ac.in/bitstream/10603/3353/10/10_chapter2.pdf.

[52] Wolfgang Kersten, Thorsten Blecker, Christian M Ringle, Niels Hackius, and Moritz Petersen. "Published in: Digitalization in Supply Chain Management and Logistics Blockchain in Logistics and Supply Chain: Trick or Treat?"
In: 9783745043 (2017). URL: https://tubdok.tub.tuhh.de/bitstream/11420/1447/1/petersen_hackius_blockchain_in_scm_and_logistics_hicl_2017.pdf.

[53] Henry M. Kim and Marek Laskowski.
"Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance." In: *SSRN Electronic Journal* (2016).
ISSN: 1556-5068. DOI: 10.2139/ssrn.2828369.
URL: http://www.ssrn.com/abstract=2828369.

[54] Donald E. Knuth. "Computer Programming As an Art."
In: *Commun. ACM* 17.12 (Dec. 1974), pp. 667–673.
ISSN: 0001-0782. DOI: 10.1145/361604.361612.
URL: http://doi.acm.org/10.1145/361604.361612.

[55] Kari Korpela, Jukka Hallikas, and Tomi Dahlberg.
"Digital Supply Chain Transformation toward Blockchain Integration." In: (2017), pp. 4182–4191.
DOI: 10.24251/HICSS.2017.506.
URL: http://hdl.handle.net/10125/41666.

[56] Mahtab Kouhizadeh and Joseph Sarkis. "Blockchain practices, potentials, and perspectives in greening supply chains."
In: *Sustainability (Switzerland)* 10.10 (2018). ISSN: 20711050.
DOI: 10.3390/su10103652.

[57] Daniel Kraft.
"Difficulty control for blockchain-based consensus systems."
In: *Peer-to-Peer Networking and Applications* 9.2 (2016),
pp. 397–413. ISSN: 19366450.
DOI: 10.1007/s12083-015-0347-x.

[58] Nir Kshetri. "1 Blockchain's roles in meeting key supply chain management objectives." In: *International Journal of Information Management* 39.December 2017 (2018), pp. 80–89. ISSN: 02684012. DOI: 10.1016/j.ijinfomgt.2017.12.005. URL: https://doi.org/10.1016/j.ijinfomgt.2017.12.005.

[59] Jani Kurki. "Benefits and guidelines for utilizing blockchain technology in pharmaceutical supply chains." In: (2016).

[60] Olga Labazova, Tobias Dehling, and Ali Sunyaev. "From Hype to Reality : A Taxonomy of Blockchain Applications." In: *Hawaii International Conference on System Sciences* September 2018 (2019).

[61] Kaijun Leng, Ya Bi, Linbo Jing, Han Chi Fu, and Inneke Van Nieuwenhuyse.
"Research on agricultural supply chain system with double chain architecture based on blockchain technology."
In: *Future Generation Computer Systems* 86 (2018), pp. 641–649.
ISSN: 0167739X. DOI: 10.1016/j.future.2018.04.061.

[62] Xu Li and Pin Chao Liu. "Based on RFID Food Supply Chain Traceability System Framework Design."
In: *Key Engineering Materials* 474-476 (2011), pp. 2150–2154.
ISSN: 1662-9795.
DOI: 10.4028/www.scientific.net/KEM.474-476.2150.
URL: http://www.scientific.net/KEM.474-476.2150.

[63] Antonios Litke, Dimosthenis Anagnostopoulos, and Theodora Varvarigou. "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment."
In: *Logistics* 3.1 (2019), p. 5. ISSN: 2305-6290.
DOI: 10.3390/logistics3010005.
URL: http://www.mdpi.com/2305-6290/3/1/5.

[64] Dianhui Mao, Fan Wang, Zhihao Hao, and Haisheng Li. "Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain." In: *International Journal of Environmental Research and Public Health* 15.8 (2018). ISSN: 16604601. DOI: 10.3390/ijerph15081627.

[65] Juri Mattila, Timo Seppälä, and Jan Holmström. "Information Management: A Case Study of a Shared Platform with Blockchain Technology." In: (2016). URL: http://escholarship.org/content/qt65s5s4b2/qt65s5s4b2.pdf.

[66] Trent Mcconaghy, Rodolphe Marques, Andreas Müller, Dimitri De Jonghe, Troy Mcconaghy, Greg Mcmullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto. "BigchainDB: A Scalable Blockchain Database (DRAFT)." In: *BigchainDB* (2016), pp. 1–65.

[67] Alexander Mittermeier. *Kryptowährungen: Was sind Proof of Work und Proof of Stake*. 2017. URL: https://bit.ly/2LUa22Z.

[68] Navonil Mustafee, Simon J.E. Taylor, Korina Katsaliaki, and Sally Brailsford. "Facilitating the Analysis of a UK National Blood Service Supply Chain Using Distributed Simulation." In: *Simulation* 85.2 (2009), pp. 113–128. ISSN: 0037-5497. DOI: 10.1177/0037549708100530. URL: http://journals.sagepub.com/doi/10.1177/0037549708100530.

[69] Vallipuram Muthukkumarasamy, Kamanashis Biswas, and Wee Lum Tan. "Blockchain Based Wine Supply Chain Traceability System." In: *Future Technologies Conference (FTC) 2017* November (2017), p. 7. URL: https://www.researchgate.net/publication/321474197%0Ahttps://www.researchgate.net/profile/Kamanashis_Biswas/publication/321474197_Blockchain_Based_Wine_Supply_Chain_Traceability_System/links/5a22ac140f7e9b71dd0508ea/Blockchain-Based-Wine-Supply-Chain-Trac.

[70] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." In: *Www.Bitcoin.Org* (2008), p. 9. ISSN: 09254560. DOI: 10.1007/s10838-008-9062-0. URL: https://bitcoin.org/bitcoin.pdf.

[71] Mitsuaki Nakasumi. "Information sharing for supply chain management based on block chain technology." In: *Proceedings - 2017 IEEE 19th Conference on Business Informatics, CBI 2017* 1 (2017), pp. 140–149. DOI: 10.1109/CBI.2017.56.

[72] Christopher Natoli and Vincent Gramoli. "The Blockchain Anomaly." In: *Proceedings - 2016 IEEE 15th International Symposium on Network Computing and Applications, NCA 2016* January (2016), pp. 310–317. ISSN: 1098-6596. DOI: 10.1109/NCA.2016.7778635.

[73] Tatsushi Nishi, Masami Konishi, and Shinji Hasebe. "An autonomous decentralized supply chain planning system for multi-stage production processes." In: i (2005), pp. 259–275.

[74] Daniel E. O'Leary. "Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems." In: *Intelligent Systems in Accounting, Finance and Management* 24.4 (2017), pp. 138–147. ISSN: 21600074. DOI: 10.1002/isaf.1417.

[75] Kelly Olson, Mic Bowman, James Mitchell, Shawn Amundson, Dan Middleton, and Cian Montgomery. "Sawtooth: An Introduction." In: January (2018), pp. 1–7. URL: https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf.

[76] Kristoffer Just Petersen. "Blockchain in Supply Chain." In: *Cio* June (2017), pp. 0–13. URL: https://blockchain-technology.cioreviewindia.com/cioviewpoint/blockchain-in-supply-chain-nid-4275-cid-1.html.

[77] Moritz Petersen, Niels Hackius, and Birgit von See. "Mapping the sea of opportunities: Blockchain in supply chain and logistics." In: *it - Information Technology* 0.0 (2018). ISSN: 2196-7032. DOI: 10.1515/itit-2017-0031. URL: http://www.degruyter.com/view/j/itit.ahead-of-print/itit-2017-0031/itit-2017-0031.xml.

[78] Oskar Petersen and Fredrik Jansson. "Blockchain Technology in Supply Chain Traceability Systems." In: (2017). URL: https://lup.lub.lu.se/student-papers/search/publication/8918347.

[79] Joseph Poon and Thaddeus Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." In: *Technical Report (draft)* (2016), p. 59. URL: https://lightning.network/lightning-network-paper.pdf.

[80] Joseph Poon and Thaddeus Dryja. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." In: *Technical Report (draft)* (2016), p. 59. URL: https://lightning.network/lightning-network-paper.pdf.

[81] Narayan Prusty. *Building Blockchain Projects*. Packt Publishing Ltd, 2017.

[82] Danny Ryan. *Costs of a Real World Ethereum Contract*. 2017. URL: https://hackernoon.com/costs-of-a-real-world-ethereum-contract-2033511b3214.

[83] Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, and Lejia Shen. "Blockchain technology and its relationships to sustainable supply chain management." In: *International Journal of Production Research* 0.0 (2018), pp. 1–19. ISSN: 0020-7543. DOI: 10.1080/00207543.2018.1533261.

URL: https://www.tandfonline.com/doi/full/10.1080/00207543.2018.1533261.

[84] Alexander Schönhals, Thomas Hepp, and Bela Gipp. "Design Thinking Using the Blockchain: Enable Traceability of Intellectual Property in Problem-Solving Processes for Open Innovation." In: *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (2018), pp. 105–110. ISSN: 0738-1360. DOI: 10.5950/0738-1360-25.2.155. URL: http://doi.acm.org/10.1145/3211933.3211952.

[85] Stefan Seuring, Joseph Sarkis, Martin Müller, and Purba Rao. "Sustainability and supply chain management - An introduction to the special issue." In: *Journal of Cleaner Production* 16.15 (2008), pp. 1545–1551. ISSN: 09596526. DOI: 10.1016/j.jclepro.2008.02.002.

[86] Henrik Sternberg and Giulia Baruffaldi. "Chains in Chains – Logic and Challenges of Blockchains in Supply Chains." In: *51th Hawaii International Conference on System Sciences (HICSS-51)* (2018), pp. 3936–3943. URL: https://scholarspace.manoa.hawaii.edu/handle/10125/50382%0Ahttps://scholarspace.manoa.hawaii.edu/bitstream/10125/50382/1/paper0495.pdf.

[87] Ferri Andrianto Susilo and Yaya Sudarya Triana. "Digital supply chain development in blockchain technology using Rijndael algorithm 256." In: *IOP Conference Series: Materials Science and Engineering* 453 (2018), p. 012075. ISSN: 1757-899X. DOI: 10.1088/1757-899X/453/1/012075. URL: http://stacks.iop.org/1757-899X/453/i=1/a=012075?key=crossref.04c87d3e163b810ad1fb2817024f9f7a.

[88] Melanie Swan. *Blockchain - Blueprint for a New Economy*. ISBN: 9781491920497.

[89] Tim Swanson. "Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems." In: *Whitepaper* (2015), p. 66. ISSN: 1098-6596. DOI: 10.1017/CBO9781107415324.004. URL: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

[90] Feng Tian. "An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain Technology." In: *2016 13th International Conference on Service Systems and Service Management (ICSSSM)* (2016), pp. 1–6. ISSN: 2161-1890. DOI: 10.1109/ICSSSM.2016.7538424. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7538424.

[91] Feng Tian. "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things." In: *14th International Conference on Services Systems and Services Management, ICSSSM 2017 - Proceedings* (2017). DOI: 10.1109/ICSSSM.2017.7996119.

[92] Kentaroh Toyoda, P. Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki. "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain." In: *IEEE Access* XXX.XXX (2017), pp. 1–13. ISSN: 21693536. DOI: 10.1109/ACCESS.2017.2720760.

[93] Horst Treiblmaier. "The impact of the blockchain on the supply chain: a theory-based research framework and a call for action." In: *Supply Chain Management* 23.6 (2018), pp. 545–559. ISSN: 13598546. DOI: 10.1108/SCM-01-2018-0029.

[94] Horst Treiblmaier. "Working Paper : Case Studies for Blockchain Use Cases : A Bottom-Up Research Working Paper Case Studies for Blockchain Use Cases : A Bottom-Up Research Agenda." In: October (2018).

[95] Youness Tribis, Abdelali El Bouchti, and Houssine Bouayad. "Supply Chain Management based on Blockchain: A Systematic Mapping Study." In: *MATEC Web of Conferences* 200 (2018), p. 00020. ISSN: 2261-236X. DOI: 10.1051/matecconf/201820000020. URL: https://www.matec-conferences.org/10.1051/matecconf/201820000020.

[96] Florian Tschorsch and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." In: *IEEE Communications Surveys and Tutorials* 18.3 (2016), pp. 2084–2123. ISSN: 1553877X. DOI: 10.1109/COMST.2016.2535718.

[97] Jen Hung Tseng, Yen Chih Liao, Bin Chong, and Shih Wei Liao. "Governance on the drug supply chain via gcoin blockchain." In: *International Journal of Environmental Research and Public Health* 15.6 (2018). ISSN: 16604601. DOI: 10.3390/ijerph15061055.

[98] H. Ping Tserng, Samuel Y. L. Yin, and Sherman Li. "Developing a Resource Supply Chain Planning System for Construction Projects." In: *Journal of Construction Engineering and Management* 132.4 (2006), pp. 393–407. ISSN: 0733-9364. DOI: 10.1061/(ASCE)0733-9364(2006)132:4(393). URL:

http://ascelibrary.org/doi/10.1061/%28ASCE%290733-9364%282006%29132%3A4%28393%29.

[99] Virbahu Nandishwar Jain and Devesh Mishra. "Blockchain for Supply Chain and Manufacturing Industries and Future It Holds!" In: *International Journal of Engineering and Technical Research* V7.09 (2018). ISSN: 2278-0181. DOI: 10.17577/IJERTV7IS090020. URL: http://www.ijert.org/browse/volume-7-2018/september-2018-edition?download=24706:blockchain-for-supply-chain-and-manufacturing-industries-and-future-it-holds.

[100] Mark Walport. "Distributed ledger technology: Beyond block chain." In: *Government Office for Science* (2015), pp. 1–88.

[101] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, and Jay Junichi Kishigami. "Blockchain contract: A complete consensus using blockchain." In: *2015 IEEE 4th Global Conference on Consumer Electronics, GCCE 2015* (2016), pp. 577–578. ISSN: 9781479987511. DOI: 10.1109/GCCE.2015.7398721.

[102] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. "Storj a peer-to-peer cloud storage network." In: (2014).

[103] Lei Xu, Lin Chen, Zhimin Gao, Yang Lu, and Weidong Shi. "CoC: Secure Supply Chain Management System Based on Public Ledger." In: *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (2017), pp. 1–6. DOI: 10.1109/ICCCN.2017.8038514. URL: http://ieeexplore.ieee.org/document/8038514/.

[104] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. "A Taxonomy of Blockchain-Based Systems for Architecture Design." In: *Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017* (2017), pp. 243–252. DOI: 10.1109/ICSA.2017.33.

[105] Yury Yanovich, Igor Shiyanov, Timur Myaldzin, Ivan Prokhorov, Darya Korepanova, and Sergey Vorobyov. "Blockchain-Based Supply Chain for Postage Stamps." In: *Informatics* 5.4 (2018), p. 42. ISSN: 2227-9709. DOI: 10.3390/informatics5040042.

[106] Minjae Yoo and Yoojae Won. "A Study on the Transparent Price Tracing System in Supply Chain Management Based on Blockchain."

In: *Sustainability* 10.11 (2018), p. 4037. ISSN: 2071-1050.
DOI: 10.3390/su10114037.
URL: http://www.mdpi.com/2071-1050/10/11/4037.

STATUTORY DECLARATION

Ich versichere hiermit, dass ich die anliegende Bachelorarbeit mit dem Thema:

Enhancing Trust in Supply Chain Processes using Blockchain Technology
(Vertrauensoptimierung in Lieferkettenprozessen durch Blockchain-Technologie)

selbstständig verfasst und keine anderen Hilfsmittel und Quellen als die angegebenen benutzt habe.

Die Stellen, die anderen Werken (einschließlich des Internets und anderer elektronischer Text- und Datensammlungen) dem Wortlaut oder dem Sinn nach entnommen sind, habe ich in jedem einzelnen Fall durch Angabe der Quelle bzw. der Sekundärliteratur als Entlehnung kenntlich gemacht.
Weiterhin versichere ich hiermit, dass die o.g. Arbeit noch nicht anderweitig als Abschlussarbeit einer Bachelor- bzw. Masterprüfung eingereicht wurde. Mir ist ferner bekannt, dass ich bis zum Abschluss des Prüfungsverfahrens die Materialien verfügbar zu halten habe, welche die eigenständige Abfassung der Arbeit belegen können.
Die Arbeit wird nach Abschluss des Prüfungsverfahrens der Bibliothek der Universität Konstanz übergeben und katalogisiert. Damit ist sie durch Einsicht und Ausleihe öffentlich zugänglich. Die erfassten beschreibenden Daten wie z. B. Autor, Titel usw. stehen öffentlich zur Verfügung und können durch Dritte (z. B. Suchmaschinenanbieter oder Datenbankbetreiber) weiterverwendet werden.
Als Urheber der anliegenden Arbeit stimme ich diesem Verfahren zu.

Eine aktuelle Immatrikulationsbescheinigung habe ich beigefügt.

(Unterschrift)

Konstanz, 06.03.2019

(Ort, Datum)