Exploring the Role of Blockchain in the Future of Car Sharing:

A Designed Artifact of a Car Sharing Platform on the Foundation of Blockchain and IoT Integration

Master Thesis
for the Attainment of the Degree

Master of Science in Business Administration and E-Business

Submitted By:	Sophia Anna Katharina Auer, 124198 Sophia Luise Berta Nagler, 124431
Supervisor:	Raghava Rao Mukkamala
Pages:	117
Characters:	265,564
Hand-in Date:	May 13, 2020

CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Abstract

Notably, there is a growing interest of OEMs in car sharing representing an environment-friendly alternative to the traditional owned vehicle. At the same time, blockchain is seen as the digital universal weapon that is deemed to transform the automotive industry. Motivated by these two trends, this thesis aims to explore how blockchain can drive the advancement of car sharing. Along these lines, based on key design principles, an artifact is designed, comprising a conceptual design and high-level architecture of a platform combining car sharing and leasing on the foundation of a blockchain and IoT integration.

While the domain blockchain for car sharing has attracted some research interest, so far, most publications have focused on either the technical implementation or the socio-behavioral aspects of blockchain in car sharing without assessing the greater impact on the industry. In addition, the domains of car sharing and leasing, in combination with blockchain, are researched mainly separately. The study aims to fill this gap by following the Design Science Research strategy for the development of a blockchain-based platform streamlining car sharing and leasing processes while demonstrating the applicability of an IoT and blockchain integration. Thus, both, the technical implementation and the business impact, are evaluated from the perspective of OEMs, a P2P car sharing provider, and municipality.

This thesis can confirm that blockchain, as one possible technology, can advance car sharing by facilitating inter-company collaboration and eliminating the need for trust to some extent. Nevertheless, the design of the respective platform depends on the right balance between the key design principles - security & privacy, authenticity, traceability & reliability, scalability, and interoperability.

Keywords: *Blockchain; Internet of Things; Car Sharing; Car Leasing; Automotive Industry; Prototyping; Hyperledger Fabric; Design Science Research*

Table of Contents

List of Abbreviation VII

List of Figures VIII

List of Tables VIII

1. Introduction 1

2. Methodology 4

2.1. Research Philosophy 4

2.2. Research Approach 5

2.3. Research Design 6

2.4. Research Strategy: Design Science Research 6

2.4.1. Problem Identification 8

2.4.2. Define objectives for a solution 9

2.4.3. Design and Development 10

2.4.4. Demonstration 10

2.4.5. Evaluation 11

2.4.6. Communication 15

3. Literature Review 16

3.1. Car Sharing 16

3.1.1. Ownership versus Access 18

3.1.2. P2P Car Sharing 19

3.2. Car Leasing 20

3.3. Blockchain 21

3.3.1. Characteristics of Blockchain Technology 21

3.3.2. Types of Blockchain Technology 27

3.4. Blockchain & IoT 29

3.4.1. Challenges in IoT addressed by Blockchain 29

3.4.2. Communication between IoT Network and Blockchain 31

3.5. Blockchain Platform for IoT 35

3.5.1. Comparison of different Blockchain Platforms 35

3.5.2. Hyperledger Fabric 38

3.6. Blockchain & Car Sharing 41

3.6.1. Blockchain for P2P Car Sharing 41

3.6.2. Blockchain for Car Leasing 42

4. Design & Development 44

4.1. Problem Identification 44

4.2. Key Design Principles 46

4.3. Assumptions 48

4.4. Designed Artifact 49

4.4.1. Conceptual Design 49

4.4.2. High-level Architecture 53

4.4.3. Overview of Use cases 56

5. Demonstration of Keyless Vehicle Access Control 57

5.1. Transaction Process of Use Case 57

5.2. Implementation of Prototype 60

5.2.1. Development Environment 60

5.2.2. Deployment of Prototype 63

5.2.3. Results 69

5.3. Technical Evaluation of Prototype 71

5.3.1. IoT Physical Domain 71

5.3.2. Connectivity Domain 72

5.3.3. IoT Blockchain Service Domain 73

5.3.4. Application Domain 74

6. Business Evaluation of Artifact 76

6.1. Car Sharing as a Business Model 76

6.2. Security & Privacy 79

6.3. Authenticity 80

6.4. Traceability & Reliability 82

6.5. Scalability 83
6.6. Interoperability 85
7. Discussion 89
7.1. Security & Privacy 89
7.1.1. Decentralization 90
7.1.2. Immutable Chains 91
7.2. Authenticity 92
7.3. Traceability & Reliability 93
7.4. Scalability 95
7.5. Interoperability 97
7.5.1. Smart Contracts 97
7.5.2. Shared Database 98
7.5.3. Possible types of consortiums 99
7.6. Summary of Discussion 101
8. Limitations & Future Outlook 103
9. Conclusion 105
Bibliography 107
Appendix 120

List of Abbreviation

Abbreviation	Description
API	Application Programming Interface
AV	Autonomous Vehicle
B2B	Business to Business
B2C	Business to Customer
BFT	Byzantine fault tolerant
CA	Certificate Authority
CFT	Crash fault tolerant
DAV	Decentralized Autonomous Vehicles
DB	Database
DLT	Distributed Ledger Technology
EVM	Ethereum Virtual Machine
GDPR	General Data Protection Regulation
HF	Hyperledger Fabric
HL	Hyperledger
HTTP	HyperText Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IS	Information Systems
JSON	JavaScript Object Notation
KYC	Know Your Customer
MaaS	Mobility as a Service
MOBI	Mobility Open Blockchain Initiative
MQTT	Message Queuing Telemetry Transport
NFC	Near Field Communication
NPM	Node package manager
OEM	Original Equipment Manufacturer
P2P	Peer-to-Peer
PoW	Proof of Work
PSP	Payment Service Provider
REST	Representational State Transfer
RFID	Radio Frequency Identification
RPi	Raspberry Pi
SDK	Software Development Kit
SSI	Self-Sovereign Identity
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Person
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VM	Virtual Machine
VW	Volkswagen
WSN	Wireless Sensors Networks

List of Figures

Figure 1: Adoption of DSR iteration process based on the context of this thesis 8
Figure 2: Overview of problems and derived key design principles of our artifact 9
Figure 3: Types of car sharing 17
Figure 4: Simplified transaction process 22
Figure 5: Example of a Block Structure 26
Figure 6: Generic IoT Blockchain Architecture 33
Figure 7: Exemplary MQTT Architecture 34
Figure 8: Hyperledger Fabric network with one channel 39
Figure 9: Conceptual design of a blockchain-based car sharing platform integrating leasing 51
Figure 10: High-level architecture for the conceptual design 53
Figure 11: Overview of use cases enabled by the conceptual design 56
Figure 12: Transaction flow of Keyless Vehicle Access Control 59
Figure 13: IoT Device Setup 60
Figure 14: Infrastructure setup of First Network 62
Figure 15: Workflow of transaction deployment 64
Figure 16: Pseudocode of Invoke Node.js Program 65
Figure 17: Pseudocode of Reading and Publishing Program on RPi 66
Figure 18: Pseudocode of our main transaction function openCar() 67
Figure 19: Received JSON object and success notification 67
Figure 20: Schematic visualization of transaction verification process 68
Figure 21: Snippet of the block in regard to endorsement 70
Figure 22: Snippets of the block in regard to event submission & ledger update 70
Figure 23: Summary of possible interconnections between key design principles 102

List of Tables

Table 1: Documentation of our major literature 13
Table 2: Overview of Interviewees 15
Table 3: Types of Blockchains 28
Table 4: Comparison of IOTA, Ethereum and Hyperledger Fabric 37
Table 5: Comparison of consensus mechanisms in HF 41
Table 6: Overview of needed attributes of class car 58
Table 7: Development Environment for the Raspberry Pi-based IoT server 61
Table 8: Development Environment for IoT Blockchain Network 62
Table 9: Docker images of nodes 63
Table 10: Output of query and blockchain info before and after the submitted transaction 69

1. Introduction

The dominance of road transportation has reached alarming levels for society due to its negative environmental impacts as well as economic and societal costs. In particular, passenger cars are a significant polluter accounting for 60.7% of total CO2 emissions from road transportation in Europe (EU Parliament News, 2019). To reverse this trend, the modes of transportation have evolved from the classic owned vehicle to alternative modes. As one of its kind, car sharing has gained powerful traction with its promise to satisfy individualized transportation demand more sustainably by decreasing the demand for passenger cars leading to a potential reduction of emissions (Chen & Kockelman, 2016; Shaheen & Cohen, 2013). Since private vehicles are standing idle on average 95% of the time, new business models in the area of car sharing are aiming to exploit these underutilized cars by substituting ownership with on-demand access to a fleet of shared or privately-owned cars (Fraiberger & Sundararajan, 2017).

As an employee at Volkswagen (VW) summarizes the relevance of car sharing suitably, it is about time to give back the city to the citizens (Y. Zuehlke, personal communication, March 06, 2020). This example demonstrates the growing awareness of original equipment manufacturers (OEM) to set an example to reduce the carbon footprint within cities. In fact, besides new innovative businesses (e.g., Zipcar), also established OEMs such as Daimler with Car2Go, BMW with DriveNow, and VW with WeShare have started to float with the current.[1] Naturally, future mobility concepts such as car sharing have drawn the interest of the automotive industry, being able to incorporate consumer trends with technology while maintaining to provide users the unique feeling of driving a car. Nevertheless, OEMs have to ensure the further development of innovative concepts to take car sharing to the next level (Schiller, Scheidl, & Pottebaum, 2017).

As one possible technical advancement and the reputed digital universal weapon, blockchain is deemed to move forward various mobility services in the automotive industry. With more secure, traceable transactions, and better transparency of information, blockchain is promised to strengthen trust and collaboration among businesses, consumers, and even vehicles (Gösele & Sandner, 2019). The growing interest of OEMs in both car sharing and blockchain serves us as a motivation to explore more in-depth how blockchain may be able to advance the development of car sharing in the future by designing a blockchain-based car sharing platform.

[1] Since 2019 Daimler and BMW have merged DriveNow and Car2Go to ShareNow (see more here).

Not only in the industry but also academic research, the cross-sectional domain car sharing and blockchain has been of rising interest. An increasing amount of publications cover blockchain for the automotive industry (Dorri, Steger, Kanhere, & Jurdak, 2019; Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019; Guhathakurta, 2018) as well as general sharing economy (Hawlitschek, Notheisen, & Teubner, 2020). Moreover, scholars address blockchain in the shared mobility (Shivers et al., 2019; Yuan & Wang, 2016) as well as specifically car sharing (Bossauer, Neifer, Pakusch, & Staskiewicz, 2019; Madhusudan, Symeonidis, Mustafa, Zhang, & Preneel, 2019; Valastin, Kost'al, Bencel, & Kotuliak, 2019). However, the focus of existing research lies mainly on the sole technical implementation or socio-behavioral aspects of blockchain without considering the interconnection between business and technical implications as well as the more significant impact on the car sharing and automotive industry.

During the research within the intersection of blockchain and car sharing, Toyota and Oaken Innovation's project of a car sharing and leasing platform, combining secure Internet of Things (IoT) with blockchain technology (Toyota Research Institute, 2017), has sparked the interest to extend the idea of a blockchain-based car sharing platform with car leasing. Indeed, car leasing gains importance due to supporting the movement away from car ownership (Pfeifle, Tauschek, & Enderle, 2017) while being able to give the customer still the feeling of owning (i.e., psychological ownership) (Paundra, Rook, van Dalen, & Ketter, 2017; Peck & Shu, 2018). In academic research, only a few scholars mention the combination of leasing and blockchain as one example application of blockchain within the automotive industry (Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019). In contrast, despite the industrial case of Toyota and Oaken Innovation, academic research about blockchain for car sharing with leasing is nowhere to be found, making this thesis an exploratory study "creating new reality" by designing a novel artifact (Iivari & Venable, 2009, p. 8).

The lack of research as well as the growing hype of applying blockchain for both the automotive and car sharing industry serves as motivation to investigate more in-depth whether blockchain brings actual value and impact for the industry, leading to the overarching research question:

How can blockchain drive the advancement of car sharing?

Parallelly to the growing interest in car sharing, OEMs are turning today's shared vehicles into much more than a mode of transport. The 21st-century cars are moving data centers with on-board IoT sensors and computers that gather information about the vehicle (Dorri et al., 2019). Blockchain is considered to be beneficial for IoT applications due to its ability to improve fault tolerance, secure data storage, and trusted authentication (Pavithran, Shaalan, Al-Karaki, & Gawanmeh, 2020; Reyna, Martín, Chen, Soler, & Díaz, 2018). However, its integration per se is deemed to be challenging because of scalability and high-resource constraints (Dedeoglu et al., 2020). This discord serves as motivation to investigate the integration more in-depth besides studying the combination of blockchain and car sharing. Various scholars have researched different IoT blockchain architectures and implementations (Hang & Kim, 2019; Liu, Han, & Li, 2020; Yuan & Wang, 2016). However, bringing the technical requirements of an IoT blockchain integration in connection with its industrial-specific business implications is yet missing, especially in the context of car sharing. This leads us to the more technical research sub-question addressing only a part of the artifact:

How does blockchain interoperate with IoT based on the example of a keyless vehicle access control system?

To answer the two research questions, this thesis follows the Design Science Research strategy with an abductive approach where the literature review is part of the process of reasoning in the form of an ex ante evaluation. Along these lines, we first outline the methodology of the thesis, followed by examining the theoretical underpinnings, concepts, and problems within car sharing, blockchain, and IoT together with its cross-sectional domains. On this basis, five key design principles (security & privacy, authenticity, traceability & reliability, scalability, and interoperability) are derived. These serve as the foundation to design an artifact comprising a conceptual design of a blockchain-based car sharing platform integrating car leasing and a high-level IoT and blockchain architecture. To both get an understanding of the technology behind that architecture as well as evaluate the technical implication of the blockchain-based platform, this thesis incorporates the development of a prototype for a keyless vehicle access control demonstrated with a Raspberry Pi and Radio Frequency Identification (RFID) sensor together with Hyperledger Fabric. In addition, interviews with experts from OEMs (BMW, VW & Bosch), a peer-to-peer car sharing provider (GoMore) and municipality (Frederiksberg Kommune) complement the technical understanding with the business implications and impact on the car sharing industry of the designed artifact. Finally, the findings from the literature review, prototype, and interviews are discussed, followed by outlining the limitations and future outlook of this thesis. In general, the thesis and findings are limited in its scope target-wise to the business side disregarding the insights of end-users and geographically to Europe due to the selection of the interviewed experts. Besides, due to the focus on car sharing, car leasing is examined in a rather superficial manner and serves mainly as a bridge to enable our blockchain-based car sharing platform.

In conclusion, this thesis contributes to research the major finding that blockchain, as one possible technology, can take part in advancing car sharing by facilitating inter-company collaboration and eliminating the need for trust to some extent. However, the design of the respective platform depends on the right balance between security & privacy, authenticity, traceability & reliability, scalability and interoperability.

2. Methodology

To discover in what way blockchain can drive the future of car sharing, an exploratory multi-method qualitative research study is conducted following the Design Science Research (DSR) strategy and using an abductive research approach. First, the choice of pragmatism as our research philosophy is described, followed by explaining the decision to take an abductive research approach. Next, our exploratory multi-method research design is outlined. Finally, the steps of a DSR strategy that determines the structure of the overall thesis is presented in detail.

2.1. Research Philosophy

Based on believing in the practical meaning of knowledge (epistemology) and seeing the reality as the practical consequence of ideas (ontology), the research philosophy underpinning this thesis is **pragmatism**. Along these lines, the purpose of our thesis is not to attain a single universal truth that will solve all of the problems in car sharing, but rather to gain a deeper understanding on how blockchain may be one possible technology to support the future progress of car sharing. Thus, we conciliate both objectivism and subjectivism while our most important determinant in the overall research design is to address our research problem (Saunders, Lewis, & Thornhill, 2016; Tashakkori & Teddlie, 2003). This goes in line with taking into consideration different types of knowledge and methods, leading to our multi-method qualitative study with prototyping and expert interviews (Saunders et al., 2016). Since knowledge should come from experience (i.e. *making*), the goal of pragmatists is to create a workable and tentative solution to problems that give practical value (Goldkuhl, 2012). Our tentative solution is the conceptual design for a blockchain-based car sharing platform that aims to address the problems of lacking the commercial scale of car sharing initiated by OEMs as well as the current challenges of integrating IoT and blockchain. Whether the solution is workable is tested by the process of implementing a technical prototype as well as interviewing relevant experts giving insights to business implications, thereby creating a final knowledge based on experience. This results in insightful findings that provide practical value.

Along these lines, our chosen research strategy, DSR, can be seen as essentially pragmatic in nature due to its emphasis on relevance (Hevner, 2007). Thus, DSR goes alongside the philosophy of pragmatism where “the truth (justified theory) and utility (artifacts that are effective) are two sides of the same coin” leading to the conclusion that “scientific research should be evaluated in the light of its practical implications” (Hevner, March, Park, & Ram, 2004, p. 4). All in all, since for both pragmatists and design researchers the research starts commonly with a problem and aims to contribute solutions informing future practice, it goes in conjunction with our overall abductive approach of reasoning (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007; Saunders et al., 2016).

2.2. Research Approach

While deductive and inductive approaches are beneficial reasoning tools for theory development, theorizing in design science requires the adoption of a line of reasoning that is fundamental for problem-solving resulting in our **abductive** approach of reasoning. By theorizing abductively, we can have a disciplined imagination involving an intuitive and creative thinking process to address the design problem through the conceptualization of a design artifact (Lee, Pries-Heje, & Baskerville, 2011). The abductive activity of creating a theory is based on both real-world observations (inductive) as well as theoretical viewpoints (deductive). By comparing the observed and the known, we can detect irregularities and start originating a new theory (Gregory & Muntermann, 2011). We first gained an understanding of the problem and explored the concepts and theories within car sharing, blockchain, and IoT, as well as the interface of these three domains. At the same time, we started building our prototype, which helped us to understand the underlying technology. Based on that, we deductively inferred design principles for an idea (i.e., *guess*) of a blockchain-based car sharing platform. By assessing the technical implementation of our scaled-down prototype as well as evaluating the business implications in the form of expert interviews, our tentative idea is tested inductively in a single cycle but lacks subsequent cycles that need to be conducted in further research. As the focus is on a holistic assessment of both the technical and business implications, a subsequent modification of our idea based on the findings is omitted. Nevertheless, we can conclude impactful findings that can be used to further elaborate our idea in the form of additional design cycles. In this sense, our inference may seem weaker than deduction or induction, but given the exploratory setting, the gained understanding should be highlighted more than an explicit confirmation.

2.3. Research Design

In the course of following the DSR strategy, we explore the problems, its possible solution, and implications while pursuing open questions. Since the main aim of our thesis is to discover problems in car sharing and IoT as well as gain insights into how blockchain may address those problems, we are following an **exploratory research design** (Saunders et al., 2016). Furthermore, we follow a **multi-method qualitative study** with prototyping as one qualitative data collection and expert interviews as another while following the DSR strategy itself is already qualitative by nature (Peffers, Rothenberger, & Chatterjee. 2018). Prototyping, or also called Testing, is sometimes seen as rather quantitative research because of commonly conducting performance tests comparing different settings (Ellis & Levy, 2009). Nevertheless, as a prototype often represents just one possible solution, it results in a more subjective and small data sample. Overall, due to our priority to include expert interviews, we omitted to conduct performance tests and instead follow an observational approach relying on the relatively subjective and hence qualitative evaluation of the prototype based on our observations during the implementation and along with the defined design principles (UNISDR, 2015).

2.4. Research Strategy: Design Science Research

The research strategy stipulates how the research is conducted to answer the research question. Hence, the research strategy is used as the methodological link between the philosophy and subsequent methods of data collection (Denzin & Lincoln, 2011). In line with the philosophy of pragmatism to create knowledge by “making”, **DSR**, as the chosen research strategy, focuses on creating and evaluating a designed object (i.e., artifact) with an embedded solution to an identified and understood research problem in the intersection of information systems (IS) and organizations (Hevner et al., 2004; Peffers et al., 2007).

As the originator of DSR, Hevner et al. (2004) define some general guidelines to carry out purposeful research. In this way, the artifact needs to address an unsolved and essential problem and be evaluated rigorously about its utility, quality, and efficacy. The developed artifact needs to base on a search process deriving existing theories and knowledge to come up with a solution to the defined problem (Hevner et al., 2004; Müller & Thoring, 2011). As we aim to get a hands-on understanding of the intersection of blockchain and IoT by building a prototype, our artifact is an instantiation located in the physical level of design knowledge but also contributes to the symbolic level through the conceptual design of our overall idea (Hevner et al., 2004). Ever since Hevner et al. (2004) started the movement of design research, various alterations and resulting genres have been developed. As one of its kind, Pfeffers et al. (2007) are the first to create an actual methodology representing a framework for carrying out research based on DSR principles. Along these lines, a design science process model is introduced that is aimed to be flexible and least concerned with design rigor. Nevertheless, by complementing Pfeffers et al. (2007) methodology with an additional ex-ante formative evaluation besides the existing ex-post summative evaluation, we aim to achieve a more disciplined and *informed* way of knowledge, thus, following a more rigorous approach to knowledge creation in the DSR process (Sonnenberg & vom Brocke, 2012; Venable, Pries-Heje, & Baskerville, 2016).

Many DSR genres require kernel theories from natural, social or behavioral science to justify the proposition of hypothesis making DSR more theory-driven (Baskerville & Pries-Heje, 2010; Gregor & Jones, 2007; Niehaves & Ortbach, 2016). In contrast, in Pfeffers et al. (2007) DSR methodology, the focus lies on the applicable artifact development where theory has the role of a reasoned argument that an artifact might work and, at the same time serves the purpose of generalizability (Peffers et al., 2018). Thus, we decide to omit the use of a kernel theory and instead rely on the identified concepts and background knowledge in our literature review, leading to our design principles. The evaluation is aimed to be rather outcome-oriented and practical instead of conceptual and iterative. Nevertheless, several cycles of development are desired to reach better rigor but can also be left for subsequent projects or research (Peffers et al., 2007).

One cycle in Pfeffers et al. (2007) DSR process consists of the six activities *Problem Identification and Motivation*, *Defined Objectives for a solution*, *Design & Development, Demonstration, Evaluation,* and *Communication*. Figure 1 provides an overview of the steps for each activity and the expected outcome based on Pfeffers et al. (2007) iteration process, which forms the structure of our entire thesis. Each of the activities is explained more in detail in the upcoming sub-sections. While in Pfeffers et al. (2007) process it is not expected to proceed in sequential order and researchers may actually start at almost any step, we still take a rather problem-centered approach having *Problem Identification and Motivation* as our entry point (Peffers et al., 2007).

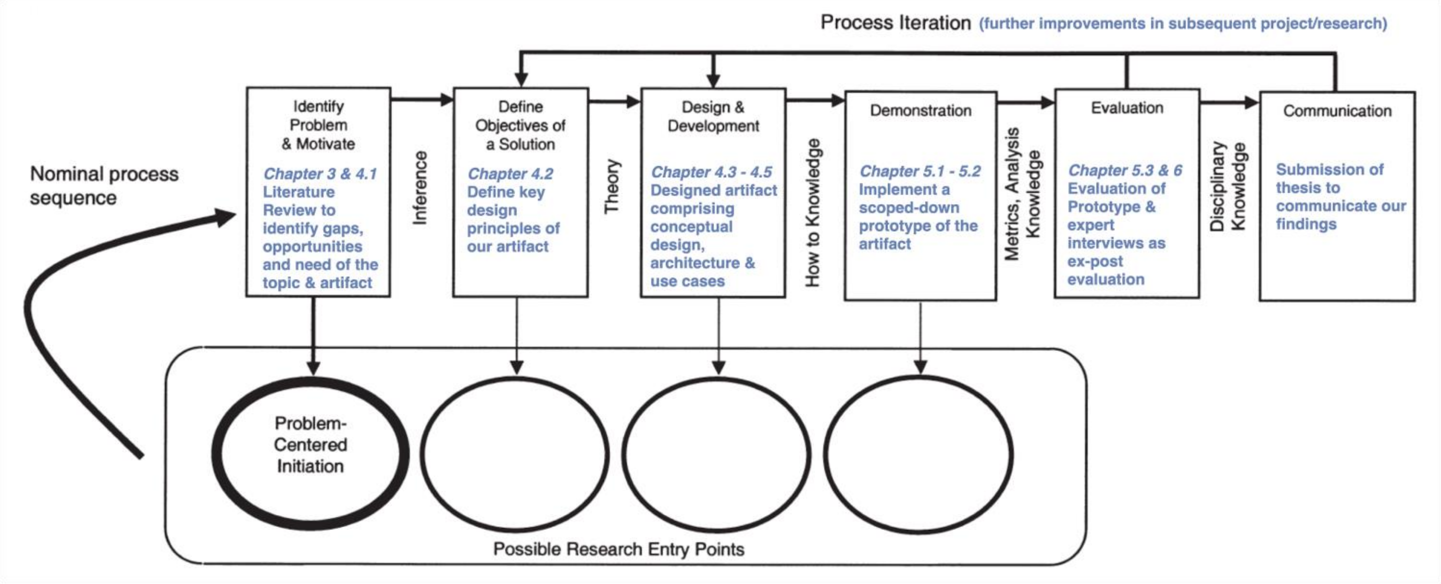

Process Iteration (further improvements in subsequent project/research)
Nominal process sequence
Identify Problem & Motivate
Chapter 3 & 4.1 Literature Review to identify gaps, opportunities and need of the topic & artifact
Inference
Define Objectives of a Solution
Chapter 4.2 Define key design principles of our artifact
Theory
Design & Development
Chapter 4.3 - 4.5 Designed artifact comprising conceptual design, architecture & use cases
How to Knowledge
Demonstration
Chapter 5.1 - 5.2 Implement a scoped-down prototype of the artifact
Metrics, Analysis Knowledge
Evaluation
Chapter 5.3 & 6 Evaluation of Prototype & expert interviews as ex-post evaluation
Disciplinary Knowledge
Communication
Submission of thesis to communicate our findings
Problem-Centered Initiation
Possible Research Entry Points

Figure 1: Adoption of DSR iteration process based on the context of this thesis

2.4.1. Problem Identification

In line with our research strategy, the specific research problem needs to be identified and defined to justify the proposed solution. The development of our artifact requires a well-considered **problem definition** to derive an effective solution (Peffers et al., 2007). As part of the ex-ante evaluation, the existing literature is reviewed, gaps in research are found, and the problem is derived.

Due to the peer-to-peer (P2P) distributed nature of blockchain, it is decided to focus on P2P car sharing. The challenge for OEMs occurs to find the right deployment of car sharing at a commercial scale. Thus, the high growth potential of P2P car sharing due to its network effects and the increasing interest of OEMs in car sharing (Phillips, 2019; Schiller et al., 2017) leads to the idea of a P2P car sharing initiated by OEMs. At the same time, leasing, as another alternative of owning, is getting more attractive compared to financing a car, leading to our idea to use car leasing as the bridge for such a P2P car sharing platform (cf. 4.1 Problem Identification). Besides the possible capabilities of such a combination, the respective platform requires a sharing of data and resources across many stakeholders in a secure way leading to the extended idea of using blockchain to facilitate the entire platform.

Especially the sharing of IoT data generated by vehicles is of significant relevance for all involved stakeholders to facilitate actual streamlining of processes and features (Dorri et al., 2019; Gösele & Sandner, 2019). However, this leads to the challenge of a needed robust and scalable IoT infrastructure and network (Dedeoglu et al., 2020; Reyna et al., 2018). According to various research, blockchain can address some of these IoT challenges (Dedeoglu et al., 2020; Hang & Kim, 2019; Pavithran et al., 2020; Reyna et al., 2018). Nevertheless, there is a lack of a detailed and hands-on demonstration integrating IoT with blockchain, which we aim to address. Moreover, although there is a growing interest in using Hyperledger Fabric (HF) in an industrial context, there is a lack of research implementing IoT applications with HF. Especially in the context of shared mobility, we could only find one publication implementing a ride-hailing application using HF (Shivers et al., 2019).

2.4.2. Define objectives for a solution

Based on the aforementioned identified problem specifications and comparison with current solutions, objectives for a solution should be rationally inferred which can be quantitative or qualitative (Peffers et al., 2007). Along these lines, we derive **key design principles** for the artifact qualitatively from the defined problems and gained knowledge within the concepts of P2P car sharing, leasing, blockchain, and IoT. In the end, these design principles are compared to the actual results "observed" from the interviews and the implemented prototype to test its fulfillment. Thereby, an informed knowledge as a contribution of this thesis is created. In this way, our defined key design principles are the primary thread followed in this thesis. In Figure 2, an overview of the derived key design principle (right) opposed to its identified problem in car sharing and leasing (left), as well as current technical problems (middle), is shown. A more in-depth elaboration is found in chapter 4.2 Key Design Principles.

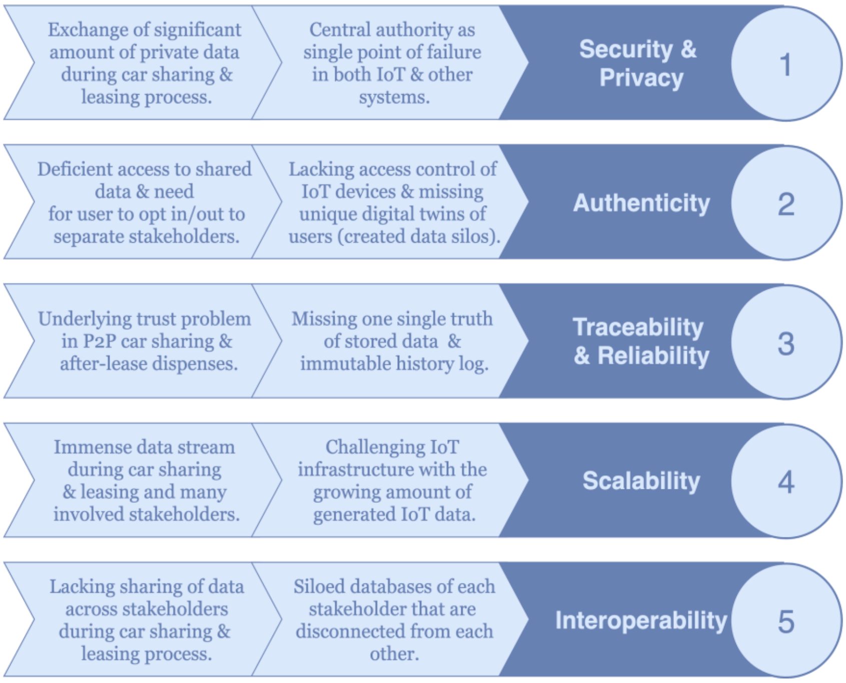

Exchange of significant amount of private data during car sharing & leasing process.
Central authority as single point of failure in both IoT & other systems.
Security & Privacy
1
Deficient access to shared data & need for user to opt in/out to separate stakeholders.
Lacking access control of IoT devices & missing unique digital twins of users (created data silos).
Authenticity
2
Underlying trust problem in P2P car sharing & after-lease dispenses.
Missing one single truth of stored data & immutable history log.
Traceability & Reliability
3
Immense data stream during car sharing & leasing and many involved stakeholders.
Challenging IoT infrastructure with the growing amount of generated IoT data.
Scalability
4
Lacking sharing of data across stakeholders during car sharing & leasing process.
Siloed databases of each stakeholder that are disconnected from each other.
Interoperability
5

Figure 2: Overview of problems and derived key design principles of our artifact

2.4.3. Design and Development

According to Pfeffers et al. (2007), any designed object can be utilized as the design research artifact, provided the design incorporates the research contribution. The design and development entail the determination of the functionalities and architecture of the artifact and the actual creation, described in-depth in chapter 4 Design & Development. Contributing to the symbolic level of design knowledge (Müller & Thoring, 2011), the artifact consists of the conceptual design and high-level architecture, enabling a variety of use cases. The **conceptual design** is derived from our literature review, determining the key design principles. Our conceptual design aims to bring together different stakeholders on one platform enabled by blockchain, showcasing the ability to streamline the entire leasing and car sharing process. Furthermore, a possible **high-level architecture** serving as the foundation of the conceptual design is developed to provide insights to one potential IoT and blockchain integration needed for an actual industry implementation. Six main enabling use cases are described to dive deeper into the applicability of our artifact and the possible business impacts.

2.4.4. Demonstration

Within one of the six use cases, **keyless vehicle access control**, one transaction is developed as the prototype in our demonstration, contributing additionally to the physical level of design knowledge as an instantiation (Hevner et al., 2004; Müller & Thoring, 2011). As the design of a blockchain-based car sharing platform is complex and extensive, the demonstration is scoped down to enable a feasible implementation. The required knowledge of how to develop and use the artifact to solve the instance, keyless vehicle access control, is gained through the literature review (Peffers et al., 2007). As the goal is to understand the blockchain technology in-depth, it is decided to implement one transaction to give the feasibility evaluation of the artifact a sound footing (cf. 5 Demonstration of Keyless Vehicle Access Control). In particular, one specific use case (keyless vehicle access control) with possible transactions is described. Then, it is scoped down to one transaction (unlock a car), which is eventually implemented with a Raspberry Pi (representing a car) and RFID sensor (representing the door) based on the high-level architecture involving HF. In this way, the overall development environment, the actual deployment (incl. a demo video), and the results are outlined. The technical evaluation of the implementation is based on observations of working with the HF network setup and extensive literature research on how best to implement such a transaction (UNISDR, 2015).

2.4.5. Evaluation

The evaluation of the artifact is one of the key activities within DSR, contributing to the advancement of the artifact development and assuring research rigor (Venable et al., 2016, p. 81). The applied evaluation method must be chosen carefully and executed thoughtfully to demonstrate the utility, quality, and efficacy of the artifact (Hevner et al., 2004). Such evaluation methods may involve logical proof or empirical evidence (Peffers et al., 2007). After the evaluation, it is possible to either iterate back to the *Design and Development* activity, improving the effectiveness of the artifact, or communicate the current state to initiate subsequent projects improving the artifact. The feasibility of such iterations is dependent on the research scope (Peffers et al., 2007). To successfully choose a strategy for the evaluation of our artifact, we follow the Framework for Evaluation in Design Science Research (FEDS) designed by Venable et al. (2016). After analyzing the possible strategies, it is decided to follow the so-called Quick & Simple approach. This approach "[...] conducts relatively little formative evaluation and progresses quickly to summative and more naturalistic evaluations." (Venable et al., 2016, p. 81). The strategy is fitting to the research of this thesis since it includes relatively few evaluation episodes and takes into account the rather restricted time frame leading to quick project conclusions, i.e., the design is more of a small and simple nature (Venable et al., 2016).

In line with this strategy, we conduct an **ex ante evaluation** (formative nature) to decide whether the development of a blockchain-based car sharing platform is based on a sound footing and which platform should be adopted for the prototype (Venable et al., 2016). Along these lines, a literature review is conducted, leading to an informed problem and concept understanding of the business and technical aspects. Additionally, the implementation of the prototype amplifies the technical understanding of blockchain technology and IoT through hands-on experience. In summary, an informed knowledge base is gained by combining the practical experience and theoretical aspects of our subsequently designed blockchain-based car sharing platform.

In general, an **ex post evaluation** assesses the choice and development of the system after the design process and implementation. An ex post evaluation (summative nature) is conducted for both the prototype within the demonstration and the whole artifact within the (business) evaluation (Venable et al., 2016). The technical evaluation of the prototype is conducted based on the gathered knowledge and observation, leading to a well-informed assessment of the feasibility of the artifact. The business evaluation of the artifact incorporates the conducted expert interviews (cf. 6 Business Evaluation of Artifact).

2.4.5.1. Ex Ante: Literature Review

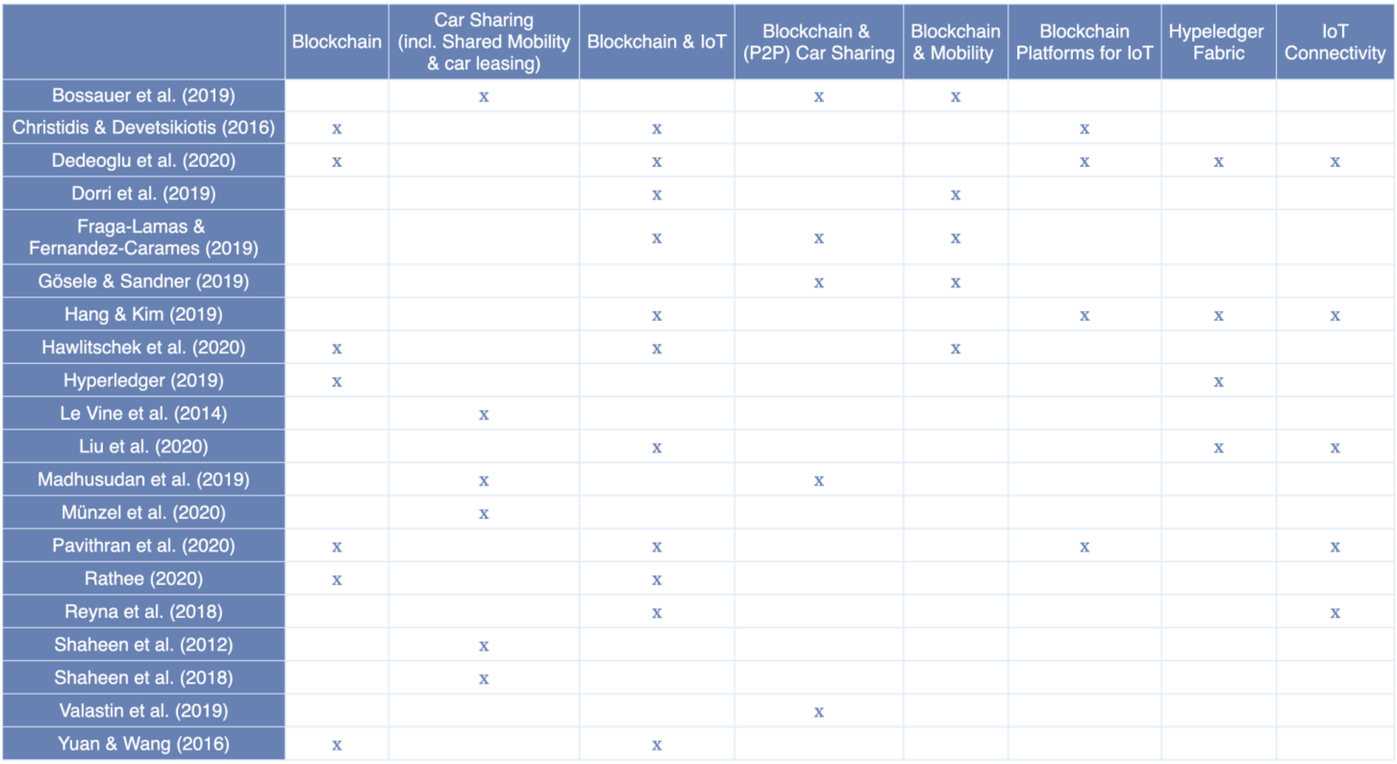
To obtain a clear overview of the topic, reviewed literature, and corresponding research areas, we constructed literature documentation that classifies the literature in research areas. The respective literature documentation, shown in Table 1, lists the major research domains and respective literature.

Google Scholar, CrossRef, and PubMed are used as exemplary tools to find the most suitable literature and the focus lies on papers published in respected journals. To find relevant technical applications and insights, we concentrated on documentations and whitepapers published by adequate organizations. As a first step, the abstract, introduction, and conclusion are examined to assess the suitability of the paper at hand. In case the paper is assessed as suitable for one of the research areas, a useful contribution, and extension of the knowledge base, the entire paper was read thoroughly.

Throughout the research process, we extended and specified the research areas from the separate domains blockchain and car sharing (incl. shared mobility and car leasing) to the combined domains blockchain and IoT as well as blockchain and car sharing, while trying to keep the focus on P2P car sharing. The extension of the research area car sharing with shared mobility was needed to place the research domain into a greater context. As we were not able to find suitable literature for the combination of blockchain with car leasing, the search was extended to the joint domain blockchain and mobility. This expanded research supported us in deriving the described *use cases* in chapter 4.4.3 Overview of Use cases.

The literature related to blockchain and IoT led to a more in-depth analysis of existing blockchain platforms for IoT and the technical integration of both. Within the analysis of the aforementioned research areas, we realized that IoT connectivity needs to be included in the research areas. As a result, we can construct a high-level architecture and gain valuable insights into the implementation of our prototype. In addition, during the assessment of blockchain platforms for IoT, we decided to extend the literature review to Hyperledger and subsequent Hyperledger Fabric leading to the well-informed implementation of our prototype.

The entire literature research serves as the basis to subsequently derive the key design principles and develop the conceptual design.



	Blockchain	Car Sharing (incl. Shared Mobility & car leasing)	Blockchain & IoT	Blockchain & (P2P) Car Sharing	Blockchain & Mobility	Blockchain Platforms for IoT	Hypeledger Fabric	IoT Connectivity
Bossauer et al. (2019)		x		x	x			
Christidis & Devetsikiotis (2016)	x		x			x		
Dedeoglu et al. (2020)	x		x			x	x	x
Dorri et al. (2019)			x		x			
Fraga-Lamas & Fernandez-Carames (2019)			x	x	x			
Gösele & Sandner (2019)				x	x			
Hang & Kim (2019)			x			x	x	x
Hawlitschek et al. (2020)	x		x		x			
Hyperledger (2019)	x						x	
Le Vine et al. (2014)		x						
Liu et al. (2020)			x				x	x
Madhusudan et al. (2019)		x		x				
Münzel et al. (2020)		x						
Pavithran et al. (2020)	x		x			x		x
Rathee (2020)	x		x					
Reyna et al. (2018)			x					x
Shaheen et al. (2012)		x						
Shaheen et al. (2018)		x						
Valastin et al. (2019)				x				
Yuan & Wang (2016)	x		x					

Table 1: Documentation of our major literature

2.4.5.2. Ex Ante & Post: Prototype

Hevner et al. (2004) describe the insufficiency of the existing knowledge base during the design and development phase as a common challenge within DSR. Hence, the researchers have to rely on their intuition and experience as well as to conduct the design and development in a trial-and-error manner. Based on the relatively new and still emerging state of blockchain applications in the industrial context, one can argue that the implementation of the prototype is mostly experimental. Its implementation results in learnings about the problem's nature and possible solution as well as the related environmental aspects leading to the extension of our knowledge base (Hevner et al., 2004). The artificial evaluation (formative) commonly involves a reduction from the natural setting in the way that it relates to a more abstract and unrealistic environment of the developed prototype. Thus, the evaluation results are restricted and may not relate to real-world implementation (Venable et al., 2016).

The implementation of the prototype itself relates to an **ex ante evaluation** (formative) to gain in-depth technical understanding, contributing to the basis for the design of the artifact in regard to feasibility and high-level architecture. The technical evaluation of the implementation is used as an **ex post evaluation** to oppose the gained technical understanding (ex ante) to some of the key design principles of the artifact. In particular, the implementation is evaluated based on observations along with the domains of the high-level architecture (IoT Physical, Connectivity, IoT Blockchain Service and Application Domain, cf. Figure 10 in 4.4.2 High-level Architecture, p. 53).

2.4.5.3. Ex Post: Qualitative Data Collection

The ex post evaluation of the artifact is needed to observe how well the constructed artifact supports the derived solution to the problem. Hence, the comparison of the objectives of the solution to actual observed results is needed (Peffers et al., 2007). According to Pfeffers et al. (2007), the artifact can be evaluated by comparing its functionalities with the solution objectives and client feedback, in our case, key design principles and stakeholders. Besides a sole technical and observational evaluation of the prototype, the primary ex post evaluation of the artifact is based on **expert interviews**. In general, we aimed to find experts relevant to the topics of blockchain and car sharing as well as mobility. More in-depth, we decided to conduct interviews with new mobility experts at BMW and VW as those are actively involved in car sharing. Additionally, we interviewed a distributed ledger technology (DLT) expert at Bosch as another OEM since the company works closely with automotive manufacturers to design and manufacture parts of vehicles themselves. Moreover, Bosch is a major player in the automotive aftermarket leading to the extensive expertise of the whole lifecycle of a car. We interviewed an expert within the P2P car sharing company GoMore due to its experience in P2P car sharing in combination with leasing. As we assume that the government is a significant part of any initiative striving shared mobility, we interviewed Frederiksberg Kommune to support this choice. Nevertheless, we excluded the government from our platform based on focusing on the business impacts, but still, see their expert opinion as an added value to the evaluation. A more detailed description of the interviewees, including the organization, role, and a short introduction is summarized in Table 2.

The interviews are **semi-structured** by asking questions within a list of key topics (Car sharing, Blockchain, IoT & Blockchain Integration, Designed Artifact, Mobility Outlook) and adjusting them to the different stakeholder groups (cf. attached interview guides)[2]. The topics and questions were left relatively open and unrelated to the key design principles to encourage interviewees to express their opinions freely without leading the interview too much towards our direction. Afterward, the interviews were coded and analyzed along with the five key design principles as well as the concept of car sharing. Finally, the coded interviews are used to evaluate the business

[2] The interviews with BMW, VW and Bosch are conducted in German and translated to English, otherwise the interviews with GoMore and Frederiksberg Kommune are conducted in English, as seen in the interview guides. The original recordings are attached as well.

implications of the artifact (cf. 6 Business Evaluation of Artifact) and discuss the findings together with the literature review and technical evaluation (cf. 7 Discussion).

Interviewee	Organization	Role	Short Introduction
Yannik Zuehlke	Volkswagen	New Business Models & Technology Research	• Focus on Blockchain & DLT research with its respective business models within mobility • Entire department: use of new technologies in Germany as well as its legal perspectives
Benjamin Ottensten	GoMore	Product Designer & Head of *Keyless* Product	• Product Designer of the app • Keyless responsibilities: ○ Partnerships ○ UX ○ Feedback from support team
Peter Busch	Bosch	Product Owner DLT Mobility	• Focus on technical evaluation and subsequent impact on business model • Technical strategy development for the automotive sector • Evaluation of new and potentially important future technologies • Technologies: Connectivity, car to car communication, IoT, AI, DLT
Dominik Pietsch	BMW	Manager Product Strategy Mobility Services	• Strategies for mobility services • Taking into account all services related to mobility: car sharing, ride-hailing, charging, parking
Camilla Mortensen	Frederiksberg Kommune	Smart City & Digitalization	• Support of other departments within technology (especially IoT), mainly strategy for smart city and how to use technology • Entire department: Maintenance & Infrastructure

Table 2: Overview of Interviewees

2.4.6. Communication

As proposed by Hevner et al. (2004), there is a need for communication to spread the resulting knowledge gained throughout the DSR process. The described steps lead to our research results accumulated from our business evaluation of the artifact and subsequent discussion. These compiled together with the limitations & future outlook and conclusion lead to a holistic assessment and comprehension of the studied subject and related research questions. The research at hand provides comprehensive information for both technical and business audiences. The chapters of the current research represent the outcome of the aforementioned research process. The overall **master thesis serves as a communication** of the created knowledge in the form of understanding and findings that can be used for further research.

3. Literature Review

As the ex-ante evaluation aims to understand the problem and achieve an informed knowledge base, the concepts and challenges of car sharing as well as car leasing are introduced, followed by the theoretical underpinnings of blockchain, the specific blockchain platform Hyperledger Fabric and the integration with IoT. Finally, the cross-sectional domain blockchain and car sharing is examined. Based on this gained knowledge, the key design principles are derived as the foundation for designing the artifact.

3.1. Car Sharing

The concept of sharing as such exists already for quite some time and has its foundation in a sharing or collaborative consumption of resources, which results in its common naming of *sharing* or *collaborative economy* (Shaheen, Cohen, Chan, & Bansal, 2020). In the transportation sector, it is called *shared mobility*. Its transportation modes evolved from traditional busses, rails, owned bicycles, and taxis to models of ride-hailing (e.g., Uber), carpooling (e.g., Blablacar), car-, bike- or e-scooter sharing (e.g., GoMore, Donkey Republic, Voi) and private shuttles on a crowd-sourced route (e.g., Berlkönig in cooperation with ViaVan in Berlin) (Burghard & Dütschke, 2019).

In a nutshell, shared mobility is defined as transportation services and resources that are shared among users enabling short-term access to transport modes on an on-demand basis. As a result, the multimodality increases, reducing vehicle ownership as well as providing new ways to access goods and services. In recent years, shared mobility gained traction due to the advancement in technology (primarily smartphones, mobile payment, GPS positioning, and IoT sensors), economic changes as well as social and environmental concerns related to vehicle ownership and urban living (Machado, de Salles Hue, Berssaneti, & Quintanilha, 2018).

As one of the most established modalities in shared mobility, car sharing evolved significantly from the traditional car rental, where consumers access operator-owned vehicles at a fixed location for at least a day (round-trip), towards pay-as-you-go models charging per kilometer with flexible drop-off locations (Burghard & Dütschke, 2019). Car sharing aims to reduce the economic inefficiency of personal vehicle ownership while distributing fixed costs and responsibility of ownership over many users (Shaheen et al., 2020).

The common understanding of car sharing is **short-term access to cars on an as-needed basis**. According to Chen & Kockelman (2016), car sharing can satisfy personalized transportation demands more sustainably by decreasing the demand for cars and parking, consequently leading to reduced emissions and freed-up space for the society. Besides, supporters of collaborative consumption in a sharing economy argue that the accompanied community interactions have a positive social impact (McLaren & Agyeman, 2015).

Overall, car sharing allows consumers to use locally available cars at any time and for any duration in exchange for monetary compensation. It differs from taxis, ride-hailing services (e.g., Uber), or carpooling (e.g., Blablacar) in the way that the renters themselves drive the shared car. Additionally, it also differs from the traditional car rental (e.g., Europcar) since cars are available nearby, and the rent is more flexible regarding the duration and pick-up/drop-off location (Münzel, Boon, Frenken, Blomme, & van der Linden, 2020).

As depicted in Figure 3, car sharing can be split broadly into Business-to-Customer (B2C) and Peer-to-Peer (P2P) models (Münzel et al., 2020). Within **B2C car sharing**, the earliest established model is round-trip (Le Vine, Zolfaghari, & Polak, 2014). More recently, one-way models including free-floating and station-based emerged, addressing especially young adults who seem to be less interested in owning cars (Klein & Smart, 2017). Besides, the **P2P model** has been the most recent addition to the overall car sharing concept (cf. more in-depth in the below sub-section). In a one-way system, the cars do not have to be returned to the initial pick-up location but can be dropped off either anywhere in a designated area (free-floating) or at a different station determined by the provider (station-based) (Münzel et al., 2020).

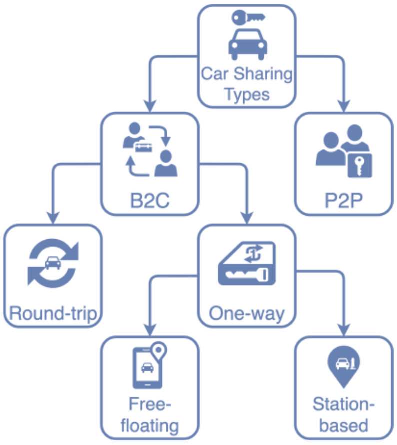


Figure 3: Types of car sharing

In particular, the fleets for **free-floating car sharing** are centrally owned by the car sharing provider, usually an OEM, and allows the user to drop-off the car anywhere in a designated geographic zone (Le Vine et al., 2014). While this increases flexibility for the users, free-floating car sharing providers often struggle with policy decisions by the municipality in regard to managing street space for parking. This challenge depends on the respective municipality in any country, which makes the growth and scale of companies more challenging and contributes to the fragmentation of the overall car sharing market (Le Vine & Polak, 2019).

Paundra et al. (2017) point out the challenge of attracting users for whom it is essential to own a car (i.e., psychological ownership). Those who value ownership are more willing to pay for a car, even if cheaper alternatives are available (Paundra et al., 2017). On the other side, those who are using public transportation regularly and do not rely as much on personal car use are often more interested in joining car sharing (Hinkeldein, Schoenduwe, Graff, & Hoffmann, 2015; Wang, Yan, Zhou, Xue, & Sun, 2017).

As the key in shared mobility is to overcome ownership and ensure social equality by offering consumers access instead of ownership, it is relevant first to explain the differences between ownership, sharing, and access in the next subsection. Next, P2P car sharing, as the focused car sharing model in this thesis, is described more in-depth.

3.1.1. Ownership versus Access

Historically, ownership used to be the dominant way of consumption expressing the special relationship between a person and an object, in this case, a car, where the object is called *personal property* or *possession* (Bardhi & Eckhardt, 2012). While **ownership** characterizes a long-term interaction with the car, access, as an emerging alternative of ownership, is a temporary and circumstantial consumption (Chen, 2009). Since sole ownership enables freedom and responsibility toward the car with clear boundaries between the owner and others, it is still a challenge to overcome this psychological ownership (Paundra et al., 2017). This is especially addressed by car leasing, giving long-term and exclusive access (Peck & Shu, 2018).

While car sharing has the word "sharing" embedded, it does not accurately describe the actual behavior of it - getting "**access**" to a car owned by another person or entity (Bardhi & Eckhardt, 2012; Paundra et al., 2017). The essential difference between sharing and access is the perceived or shared sense of ownership. In sharing, that commonly occurs within family and friends, ownership and possession are joint so that the car is free for all to use, does not require monetary compensation, and its responsibilities (e.g., car maintenance) are shared (Belk, 2010). In contrast to sharing, in access, there is no transfer of ownership or joint ownership, but the user simply gains access to use the car (Bardhi & Eckhardt, 2012).

3.1.2. P2P Car Sharing

As our designed artifact is addressing P2P car sharing due to its blockchain applicability, the respective car sharing model is elaborated more in-depth.

In general, P2P car sharing enables **privately owned vehicles to be made temporarily available** for shared use, representing a decentralized car sharing fleet (Le Vine et al., 2014). In this way, the car owner or lessee (host) can cover the high fixed costs or monthly leasing payment by profiting from transactions with the renters (guests) (Shaheen, Martin, & Bansal, 2018). Commonly, a car sharing provider operates this two-sided platform connecting the car host with the renter and keeps a percentage of the usage fees while additionally providing a tailored insurance product (Münzel et al., 2020). The P2P car sharing provider often aims to build a community around the platform to exploit the two-sided network effects. Consequently, the primary target market of P2P car sharing is in dense urban centers (Shaheen et al., 2018).

As the network is determined by the location of vehicle hosts and **not centrally-managed**, P2P car sharing offers potentially a greater selection of pick-up and drop-off locations, vehicle types, and daily/hourly usage prices than B2C car sharing (Ballús-Armet, Shaheen, Clonts, & Weinzimmer, 2014). Unlike one-way car sharing that is dependent on a company-maintained vehicle fleet, P2P car sharing is seen as the **paramount example of collaborative consumption** as it promotes the sharing of underutilized cars (Shaheen, Martin, & Hoffman-Stapleton, 2019). In addition, a P2P driven system can significantly reduce operating costs as the platform provider does not have to invest in the car fleet, which usually accounts for 70% of the total operating expenses for one-way and round-trip car sharing companies (Shaheen, Mallery, & Kingsley, 2012).

Nonetheless, P2P car sharing is facing considerable **challenges** concerning liability in regard to insurance, fear of sharing and **lack of trust**, the expense of smooth technological solutions, assurance of vehicle reliability as well as vehicle availability (Shaheen et al., 2012). Besides the difficulty of country-specific regulations concerning insurances, personal vehicle insurances are commonly not valid while a vehicle is rented out to others so that a P2P car sharing company has to provide secondary car insurance (Shaheen et al., 2012). However, a vehicle owner or lessee may still be exposed to some financial liability, especially concerning their own personal insurance premium spikes (Lieber, 2012). Moreover, insurances often charge a car sharing provider three to four times more than a comparable private car owner would pay (Le Vine et al., 2014).

Regardless, technological developments in the area of in-vehicle **telematics**[3] can be used to assess better risk as well as usage of the vehicle by tracking mileage, repairs, and more (Le Vine et al., 2014). To address the lack of trust when sharing a valuable asset such as the car, user rating, thorough screening and selection of users as well as integration with social networks are some key mechanisms for a P2P car sharing provider to implement (Shaheen et al., 2012).

3.2. Car Leasing

This paper aims to explore blockchain for car sharing that integrates car leasing. Thus, it is essential to shortly introduce car leasing besides car sharing as an alternative to car ownership.

Car dealerships and fleet management firms that offer leasing of vehicles to private consumers or other firms have been the **forerunner of the sharing economy**, providing the benefits of car ownership without its responsibility (Johnson, Herrmann, & Huber, 1998). Essentially, leasing gives the consumer (i.e., lessee) **exclusive access** to a car for a certain period (usually six months and up to four years) by paying a fixed monthly rate while not obtaining the ownership of the car (Liao, Molin, Timmermans, & van Wee, 2019). Nevertheless, by acquiring the permanent exclusive use of a car over that **long period**, lessees usually perceive the car as their property satisfying the psychological ownership (Peck & Shu, 2018). Conclusively, leasing provides the benefits of car ownership without its burdens, including high upfront purchase price, maintenance, and resale worries. In some countries, the monthly leasing rate covers insurance cost, road tax, and possible maintenance, warranty, and repair costs (Liao et al., 2019).

After all, according to Guyader & Piscicelli (2019), the primary motivation to promote leasing is the fact that consumers are more stimulated towards the movement away from ownership, which may lead to greater P2P car sharing adoption where leasing costs can be shared.

[3] Telematics represents the use of smartphones for data collection referring to services where telecommunications are employed to transmit information provided by sensors in, e.g., vehicles (vehicle telematics). Some of the resulting features include fuel monitoring, eco-driving, vehicle tracking, geo-fencing, entertainment, and broadcasting. Moreover, remote diagnostics and insurance telematics are other upcoming areas being worked on (Wahlstrom, Skog, & Handel, 2017).

3.3. Blockchain

A common challenge posed by information systems is the lack of trust and a single point of failure in centralized systems due to the mutability of traditional databases (CRUD operations[4]) that often leads to security breaches (Gatteschi, Lamberti, & Demartini, 2020). To establish trust in information systems, the implementation of a verification or audit mechanism is needed (Nakamoto, 2008; Reyna et al., 2018). Satoshi Nakamoto first resolved this challenge by introducing the mainstream blockchain system, cryptocurrency Bitcoin, allowing payments between its users in a **P2P manner independent of a central authority** (trusted intermediary), e.g., central banks. (Dedeoglu et al., 2020; Hawlitschek et al., 2020; Nakamoto, 2008). This implementation showed the ability of blockchain to enable trustless networks, leading to the evolution from a sole verification mechanism for cryptocurrencies to a wide range of economic and commercial applications in different industries (Christidis & Devetsikiotis, 2016; Hawlitschek et al., 2020; Wörner, Von Bomhard, Schreier, & Bilgeri, 2016).

The concept of a "**trustless**" system means the guarantee that the rules of interaction are known and agreed upon by the participants in the system, leading to a canonical truth. In this way, the power and trust are distributed among the participants eliminating the need for a trusted intermediary (Klems et al., 2017). As there are no real trustless systems in the sharing economy (Hawlitschek et al., 2020), a more accurate description could be "distributed trust" that can be seen as more trustful than a "central trust" (Klems et al., 2017).

Within this chapter, on the one hand, the characteristics of blockchain technology (distributed ledger technology, decentralized consensus mechanism, cryptographic algorithms, blockchain structure, and smart contract) are outlined more in detail. On the other hand, the two broad types of blockchain technology, permissionless and permissioned, are opposed to each other.

3.3.1. Characteristics of Blockchain Technology

Overall, the architecture of blockchain technology is commonly referred to as distributed ledger technology (DLT) (Rathee, 2020). The technology of blockchain is composed of a **distributed** database or **ledger**, a **decentralized consensus mechanism**, and **cryptographic algorithms**. **Smart contracts** serve as a tool to rely on this technical setup allowing the implementation of decentralized applications (Hawlitschek et al., 2020). Before describing these four characteristics together with a more in-depth elaboration on the **blockchain structure**

[4] CRUD operations enable anybody in traditional databases to edit, copy, remove, delete, or update the documents and hence the security is often breached too easily (Gatteschi et al., 2020).

within this chapter, a simplified transaction process of an asset within the blockchain, based on Christidis & Devetsikiotis (2016), is demonstrated in Figure 4 and explained referring to the corresponding steps with its blue highlighted numbers.

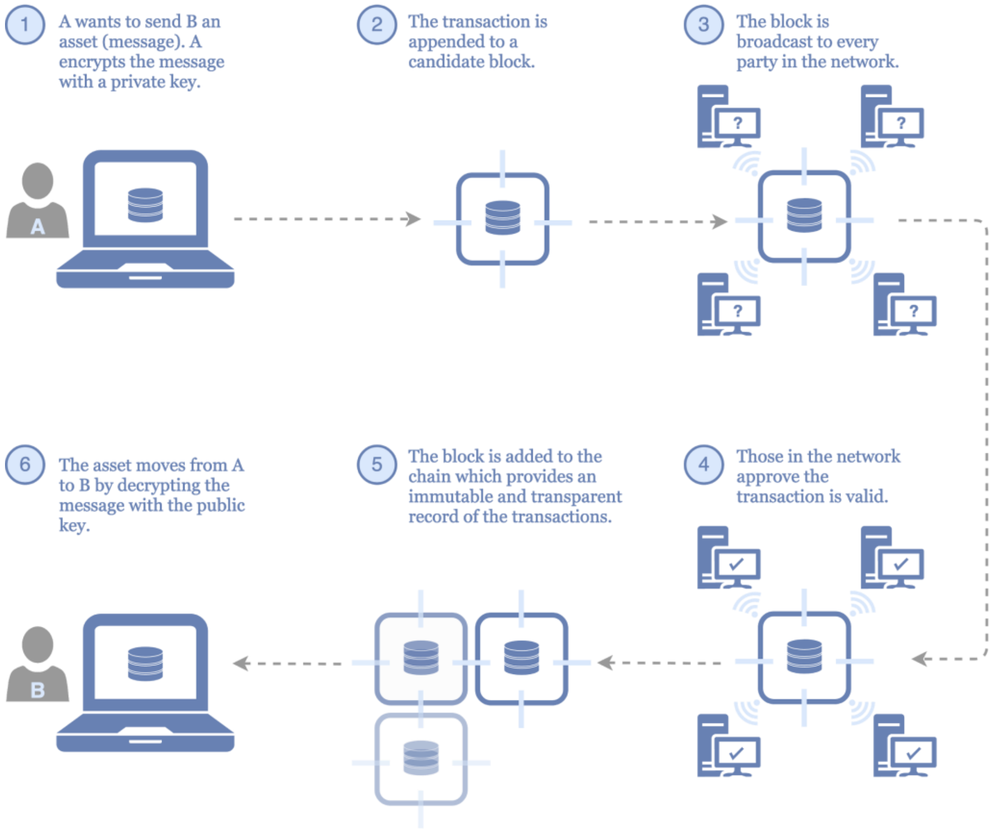

1 A wants to send B an asset (message). A encrypts the message with a private key.
2 The transaction is appended to a candidate block.
3 The block is broadcast to every party in the network.
A
?
6 The asset moves from A to B by decrypting the message with the public key.
5 The block is added to the chain which provides an immutable and transparent record of the transactions.
4 Those in the network approve the transaction is valid.
B

Figure 4: Simplified transaction process

The interaction of the users with the blockchain is enabled by a pair of private and public keys (cf. 3.3.1.3 Cryptographic Algorithms). The **public key** enables each user (6) in the network to be addressable by other users. The **private key** is used to sign the transaction of the respective user (1). Each transaction is stored in a data block, which is initially called a **candidate block** (2). Once a transaction is signed, the created candidate block is **broadcasted** by the user's node to all nodes in the network (3) (Christidis & Devetsikiotis, 2016). To ensure the validity of the block, each node has to **verify** the genuineness of the block. Once the block is validated, each node will add the recently created candidate block to their copy of the chain (4). This verification process includes the revision of whether the candidate block contains a valid transaction, and the hash references the correct previous block on the corresponding copy of the chain (Christidis & Devetsikiotis, 2016). Then, all nodes in the network have to agree on the validity of the block with the aid of a **consensus mechanism**. In case the block is found to be valid, it will be **added** to the cryptographically interconnected data **blocks** (i.e., chain of blocks) (5). If the consensus deems the block has been manipulated, it will be rejected by all nodes (Christidis & Devetsikiotis, 2016; Rathee, 2020). A detailed description of a concrete transaction use case will be elaborated within the demonstration in chapter 5.1 Transaction Process of Use Case.

After all, the ledger is distributed and accessible by every entity, which is part of the network. As soon as data is recorded into the ledger, the data cannot be mutated (Puthal, Malik, Mohanty, Kougianos & Das, 2018). This enables the interaction of the users of the blockchain without depending on a central authority to resolve the conflicting order of transactions (Hawlitschek et al., 2020).

3.3.1.1. Distributed Ledger Technology

The blockchain network is made up of a set of nodes, so-called clients, acting as the entry point into the network for several users. The access of each user to the network is based on permissions (Christidis & Devetsikiotis, 2016). Each node within the network incorporates a copy of the ledger, which consists of the world state and the blockchain. The **world state** represents a database that holds a cache of the current values of a set of ledger states. This enables a program to directly access the current value of a state rather than having to go through the entire transaction log. The **blockchain** represents the transaction log recording all the changes that have resulted in the current world state (Mikula & Jacobsen, 2018) (cf. 3.3.1.4 Blockchain structure). This mechanism of distributing the ledger on different nodes results in the characteristic of a **distributed network**, ensuring that not a single node holds control over the blockchain. The communication and coordination of the various nodes are enabled by passing messages between each other (Rathee, 2020).

The distribution of the network leads to the elimination of a single point of (potential) failure of the network since it is not reliant on centralized storage of the ledger compared to traditional central cloud architecture. While this distribution is an advantage of blockchain technology, it leads to the challenge of synchronizing all the copies of the ledgers in the network so that they all share the same world state (Rathee, 2020). To address this challenge, a consensus mechanism needs to be implemented (Christidis & Devetsikiotis, 2016).

3.3.1.2. Decentralized Consensus Mechanism

To maintain the world state, the various nodes need to reach an agreement on the transactions and the way they are ordered on the new block. Without such a consensus mechanism, the divergence of the blockchain cannot be prevented, resulting in forks of the blockchain and different world states of the various nodes. Consequently, the unique, authoritative chronology is no longer maintained by the network (Christidis & Devetsikiotis, 2016).

The ideal consensus scenario would entail the voting of all validating nodes on the order of transactions per block. However, this can lead to a harmful outcome in an open network that can be joined by anyone as a minority could take control of the network (Christidis & Devetsikiotis, 2016). Hence, each system needs to tailor the utilized consensus mechanism to its need. Depending on the type of blockchain, there are different kinds of consensus mechanisms that consider the used architecture, the hardware requirements, and the attack vector that is intended to be mitigated (Dedeoglu et al., 2020). In the following, the most popular consensus mechanism will be shortly explained.

To control the generation of new blocks, the **Proof-of-Work** (PoW) consensus mechanism utilizes the solving of a cryptographic puzzle (mining), as validation work, which usually is resource-intensive. PoW is mainly used as a reward-based consensus by many popular blockchain applications that involve cryptocurrencies, such as Bitcoin and IOTA (Dedeoglu et al., 2020).

In case there is no need for an economic incentive for mining, a wider range of consensus mechanisms can be utilized. In distributed systems, a system can suffer a **crash failure** in case it is stopping abruptly and does not resume its activity. However, a **Byzantine failure** is much severer as the process can appear normal, although it is acting arbitrarily. In this case, contradicting messages are sent by faulty or malicious nodes in the hope of sabotaging the consensus (Xiao, Zhang, Lou, & Hou, 2020).

Crash fault tolerant (CFT) consensus can be established by utilizing a leader-follower model. A leader is dynamically elected among the nodes responsible for the ordering of the transactions and then replicates messages to the follower nodes. A system is rated as CFT if it can sustain the loss of nodes, including leader nodes, as long as there is a majority of ordering nodes remaining (Xiao et al., 2020). A **Byzantine fault tolerant** (BFT) consensus protocol is naturally CFT based on the inclusive relationship between those two failures (Xiao et al., 2020). A node might be behaving strangely and sends a different response about the decision to the nodes in the network. The idea is that a higher amount of honest nodes will agree on a correct decision than faulty nodes agreeing on an incorrect decision, leading to the rejection of false information by the majority (Christidis & Devetsikiotis, 2016; Dedeoglu et al., 2020).

The choice of the consensus protocol (BFT or CFT) depends on the use case. For example, a blockchain deployed for a single organization or operated by a trusted authority might assess a full BFT consensus as an unnecessary and excessive drag on performance and throughput.

Whereas in a multiparty and more decentralized use case, the BFT consensus protocol might be required (Hang & Kim, 2019).

3.3.1.3. Cryptographic Algorithms

To secure the communication, authentication, and message integrity have to be provided, which can be achieved in blockchain through cryptographic algorithms. **Authentication** describes the requirement that the parties involved in the exchange of messages need to be assured of the identity that created a specific message. The **integrity** or often called **immutability,** in the context of blockchain, of a message describes the assurance that a message cannot have been modified during its transmission. To meet these requirements, a digital signature mechanism is implemented. This mechanism requires each actor to hold two cryptographically connected keys, public and private keys, representing a wallet and verifying the identity of a user. The **public key** is made widely available and represents an authentication anchor. The **private key** is used to produce digital signatures on messages and maintained as private in the wallet (Asuquo, Ogah, Hathal, & Bao, 2020). The sender of the message signs it with its private key, which encrypts the message. The recipient of this message is then able to verify the origin and integrity of the received message by comparing the attached signature to the public key of the expected sender, consequently able to decrypt the message (Pavithran et al., 2020). The unique mathematical relationship between the keys enables secure communication. The private key is used to produce a signature on a message that only the corresponding public key can match, and only on the same message (Asuquo et al., 2020).

3.3.1.4. Blockchain structure

The transactions are recorded in units of blocks. As depicted in Figure 5, based on Pavithran et al. (2020) and Zhou et al. (2019), each block of the blockchain is constructed according to the same principle. The blockchain is initialized by a **Genesis Block,** representing the basis on which additional blocks are added and is commonly hardcoded in the software of an application (Pavithran et al., 2020).

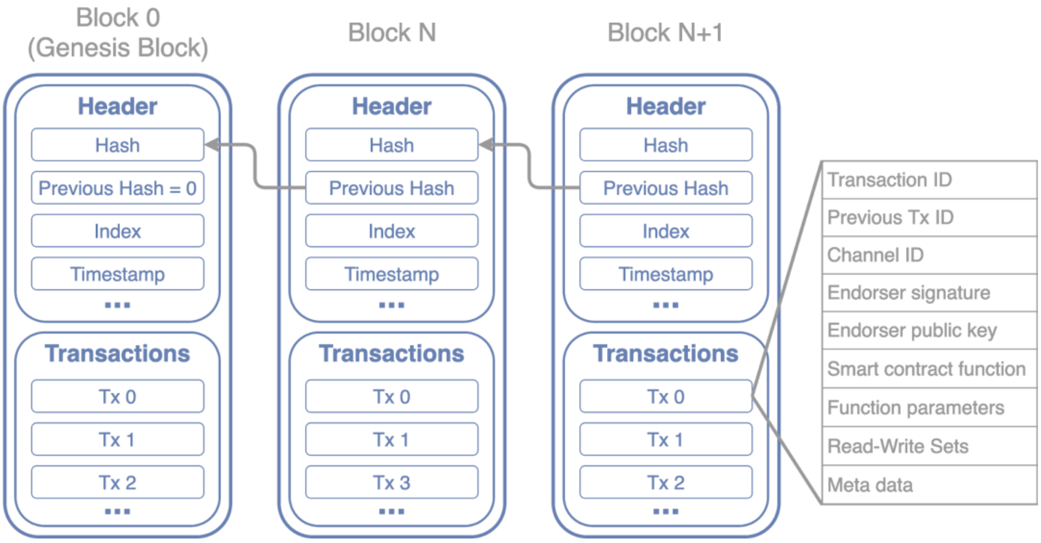


Figure 5: Example of a Block Structure

The block contains the data associated with the transaction, the hash[5] of the current block, timestamp, and the hash of the previous block (Pavithran et al., 2020). The hash value of each block can be compared to fingerprints (Rathee, 2020). If there are modifications made to a block in the blockchain, the hash will be modified, too. In other words, once a hash value of a block is changed, the block is not considered to be the same block. Conclusively, the hash value is a significant factor avoiding modifications in the block after it has been appended. To keep the chronological order of the transactions, the block holds the hash of the previous block resulting in the linkage of the current block to the previous block (**Previous Hash***)* (Dedeoglu et al., 2020).

3.3.1.5. Smart Contract

Commonly, contracts describe an agreement between two parties that define the execution or omission of action in exchange for something. In this sense, the concerned participants have to trust each other to fulfill the defined obligations. The same agreements are the basis of smart contracts, but the need for the common form of trust is removed due to its **autonomous nature** (Swan, 2015). Smart contracts allow the execution of code inside a blockchain as virtual space without centralized control. They are deployed independently and automatically on each node of the network in a stipulated manner, which is enforced correctly by a blockchain consensus protocol. Afterward, the smart contract is permanent and cannot be modified (Dedeoglu et al., 2020).

[5] Hash: A hash function is used to map data of arbitrary size to fixed-size values, resulting in an alphanumeric summary of the data. These algorithms essentially aim to produce a unique, fixed-length string – the hash value, or “message digest” – for any given piece of data or “message” (Gatteschi et al., 2020).

All concerned entities have verifiability of the smart contract during the process, as interactions include a digital signature. This results in the elimination of possible disputes as participants cannot disagree over the outcome (Christidis & Devetsikiotis, 2016). The resulting trust guaranteed by code, mathematics, and verification from the majority can also be considered as **"software-defined" trust** having the potential to significantly reduce the structural complexity of many systems (Yuan & Wang, 2016). Finally, smart contracts can represent **business logic** in an ample scope of applications such as resource allocation, traceability, process automation, and seamless communication (Dedeoglu et al., 2020).

3.3.2. Types of Blockchain Technology

It is common to categorize blockchains based on the implemented control mechanism, leading to the differentiation into permissioned and permissionless blockchains (Dedeoglu et al., 2020). An overview of the opposing types of blockchain in regard to network structure, control, efficiency, security, privacy, and use case examples is shown in Table 3 based on Dedeoglu et al. (2020).

3.3.2.1. Permissionless Blockchain

In many cases, a permissionless blockchain is referred to as **public blockchain** (Asuquo et al., 2020). A permissionless setup of the blockchain network allows anyone to join, meaning no permission is required to become part of the network and contribute to the consensus mechanism or participate in creating and verifying transactions. The governance of the network is transparent, enabling network participants to have a full overview of how the blockchain works, the history of transactions, and how consensus is achieved. The identity of each network's participant and the respective blockchain transactions are **anonymous**. The redundancy in the network and decentralized consensus mechanism leads to more resilience against attacks and node failures of the network. Nonetheless, the decentralized consensus mechanism entails latencies, inefficiency, and lower network throughput with a growing network. Economic incentives are created to persuade network participants to contribute to the consensus mechanism. The most popular examples of permissionless blockchains include Bitcoin and Ethereum (Dedeoglu et al., 2020).

3.3.2.2. Permissioned Blockchain

A permissioned blockchain can also be referred and subsequently divided into **private or consortium blockchain** (Asuquo et al., 2020).

The setup of a permissioned blockchain stipulates a single organization or a consortium as the **controlling unit** of the blockchain, which determines the rules of the network and has the power to dictate who can and cannot be part of its network. The privacy of transactions is improved as only nodes with the required **access permissions** are allowed to read the transactions on the blockchain. Additionally, the scalability, transaction times, and network throughput are enhanced compared to permissionless blockchains since a smaller amount of nodes allows more efficient performance, and the applied consensus mechanism can be less computationally expensive (Dedeoglu et al., 2020).

By forming a consortium as the controlling unit, some of the counterparty risks of having only one organization as the centralized control are mitigated. A determined equally powerful group of network participants function as validators and are responsible for managing the consensus mechanism and maintenance of the blockchain. The chain can be made visible to the validators, authorized individuals, or all network participants. Furthermore, adaptations can be easily rolled out, provided the validators can reach a consensus. Based on these characteristics of the blockchain system, the permissioned blockchain is most beneficial in a setting where **multiple organizations** operate in the same industry. The application of a blockchain enables a shared system for their transactions and information exchange across organizational borders. Hence, most organizations which want to streamline the communication amongst one another, utilize a permissioned blockchain (Dedeoglu et al., 2020).

	Permissionless	Permissioned
Network structure	Fully Decentralized	Centralized or partially decentralized
Controlled by	All network participants	Trusted entity (blockchain owner) or a predetermined group of network participants
Efficiency	Low	Medium to High
Security	Higher due to distribution	• Lower due to Centralization (private) • Average due to partial distribution (consortium)
Privacy	Low, as all transactions are transparent	• High if the access to data is controlled by the trusted entity (private) • Medium if the access to data is controlled by a group of network participants (consortium)
Use case examples	Cryptocurrency such as Bitcoin, Ethereum, Litecoin etc.	• Company-owned blockchains & government applications (private) • Consortium of companies, multiple government agencies

Table 3: Types of Blockchains

3.4. Blockchain & IoT

In the area of car sharing, new advancements, such as keyless authentication to unlock a car and collecting data with telematics to track safety or driving behavior events, are attributed to the progress in the IoT (Fraga-Lamas & Fernandez-Carames, 2019). Simply put, IoT is a network of things in the physical world. It has emerged as a set of technologies spanning from Wireless Sensors Networks (WSN) to Radio Frequency Identification (RFID), which are devices with limited computing power and capacity to sense, actuate and communicate over the Internet with a backend application (Reyna et al., 2018). The sensors or actuators can be placed within the device or attached to it. In recent years, the involved embedded computing hardware has undergone a steady advancement resulting in decreased size, less energy consumption, and reduced hardware cost. Together with evolved network technology, large-scale IoT systems are making it possible to integrate IoT into everyday objects (Pavithran et al., 2020). IoT plays a central role in converting traditional houses into smart homes, electrical grids into smart grids, and cities into smart cities (Reyna et al., 2018). Especially in mobility, smart vehicles are increasingly connected to roadside infrastructure (V2I), other vehicles in close proximity (V2V), end-users (V2P), and generally to everything on the internet (V2X) (Dorri et al., 2019). While the advancement in IoT technologies enables a broad range of new services, it also causes challenges of securing the vast amount of data and maintaining individual privacy. Current approaches to ensure IoT security and privacy are mostly centralized, which limits their scalability and imposes trust in a central entity. This raises the need for a decentralized trust mechanism, such as provided by blockchain technology (Dedeoglu et al., 2020). In the following subsections, the challenges of IoT and how blockchain can address some of them are examined. Besides, possible IoT blockchain architectures with concrete communication mechanisms are explained.

3.4.1. Challenges in IoT addressed by Blockchain

While IoT networks are of distributed nature consisting of resource-constrained and heterogeneous IoT devices, its security mechanisms are highly **centralized.** This leads to low scalability, many-to-one nature of network traffic, and single point of attacks. In many cases, the data collected by IoT devices contain privacy-sensitive information that makes it very critical to protect from **cyber attacks**. Likewise, communication models that are solely based on a centralized broker identifying, authenticating and connecting all devices through cloud servers are unlikely to **scale** with the increasing number of IoT devices (Dedeoglu et al., 2020). In contrast, a blockchain network of interconnected devices can eliminate the use of a central intermediary enabling the trustful transfer of real-time data from the sensor to every node in the network without any modification. Besides, blockchain allows IoT devices to communicate among themselves and make decisions automatically (Pavithran et al., 2020). This **P2P distributed** nature of blockchain ensures that there is no single point of failure or attack. Additionally, the decentralization of the blockchain architecture can improve the fault tolerance and system scalability preventing network bottlenecks (Reyna et al., 2018).

Usually, IoT applications require the devices to collect, process, and exchange an immense amount of **privacy-sensitive** data. Many IoT implementations ignore that critical issue despite the severe consequences (Dedeoglu et al., 2020). Indeed, with current standard protocols used in IoT, it is possible to secure the data with a standard username and password authentication as well as encryption on the network (TLS/SSL) or application layer (payload encryption) (Peniak & Bubenikova, 2019). This adds significant network overhead resulting in high energy consumption, which can be a problem for the resource-constrained IoT devices. Nevertheless, blockchain technology can treat device message exchanges as transactions **anonymously** using different public keys for each transaction that increases the difficulty of inferring any explicit information about the initial message (Dedeoglu et al., 2020). Those can be validated by smart contracts and, in this way, **secure communications** between devices and the blockchain network. Consequently, current moderately secure standard protocols used in the IoT can be optimized with the application of blockchain (Reyna et al., 2018).

In regard to **identity management**, every IoT device requires a unique identity. As many organizations are mainly focusing on a quick launch of new IoT projects, they are usually less concerned about the level of access these devices have to sensitive and non-sensitive data (Pavithran et al., 2020). However, to name just one example concerning smart vehicles, illegal access to such devices can have tremendous effects on the safety of the user. In P2P car sharing, only the rightful user who requested a specific car should be able to open that car. In a blockchain system, participants can identify every single device by the creation of digital twins (i.e., digital copies of physical objects) while the provided data is immutably stored. In addition, blockchain can provide trusted distributed **authentication** and **authorization** of devices and users for IoT. Even over time, participants of such a **reliable** system are capable of verifying the authenticity of the data and can be certain that it has not been manipulated, ensuring the sensor data's traceability and accountability (Reyna et al., 2018). After all, advanced identity management in the form of digital twins for all devices is seen as the major benefit of using blockchain technology for IoT resulting in an optimized IoT device access control (Hang & Kim, 2019).

In summary, blockchain can enrich IoT applications by providing a trusted sharing service, where information is reliable and traceable. The origin of the data can be identified at any time, and data stays immutable over time, increasing its security. In cases where IoT information should be securely shared between many participants, be it infrastructure, devices ("things"), or people, this integration may be a fundamental revolution (Reyna et al., 2018).

3.4.2. Communication between IoT Network and Blockchain

Regardless of the possible advantages of utilizing blockchain technology for IoT, its adoption depends on the design of blockchains fitting to IoT applications. Scalability, high resource usage, and processing delay of transactions are ongoing problems for the integration of blockchain in IoT. In addition, the essential blockchain functionalities in terms of network structure, control, consensus mechanisms, and access can vary across IoT applications (Dedeoglu et al., 2020).

Along these lines, Pavithran et al. (2020) suggested and analyzed different approaches for an IoT blockchain architecture pointing out the necessity of taking into consideration various key components that have to be determined before creating a blockchain for IoT. Such components include the identification of IoT device types (e.g., heterogeneity, owner, type of node), security requirements (e.g., confidentiality, authentication, key management), data and storage requirements (e.g., cloud, gateway, device identity), type of applications (e.g., B2C, B2B, industrial) as well as the suited type of blockchain and parameters (e.g., permissioned/permissionless, type of consensus and platform). In addition, Reyna et al. (2018) note when integrating blockchain, it needs to be decided where the IoT interaction (i.e., communication between the IoT devices and network) will take place. The three alternatives are within the IoT (IoT-IoT), through the blockchain (IoT-Blockchain) or a hybrid design involving IoT and blockchain. If the use case has reliable IoT data with low latency in IoT interaction, the **IoT-IoT** approach is recommended where only a part of the IoT data is stored on the blockchain, but the IoT interaction itself happens independently. In contrast, the **IoT-Blockchain** approach ensures that all interactions are going through the blockchain, which makes them traceable but, at the same time, increases the bandwidth and adds a delay in processing transactions. Lastly, the **hybrid** approach is a mix of the previous two, where only part of the interactions and data take place on the blockchain and the rest within the IoT network. This approach could leverage the benefits of blockchain and real-time IoT interactions despite the challenge of choosing which interactions should go through the blockchain.

While the IoT-Blockchain and hybrid approach seem suited for some applications, the primary challenge remains in the adaptation of blockchain technology that is suited to embedded IoT devices and gateways with limited resources (Hang & Kim, 2019; Liu et al., 2020; Pavithran et al., 2020; Reyna et al., 2018). Indeed, there is an increasing number of blockchain integrations, such as Rapsnode (for Bitcoin, Litecoin & Ethereum) and EthEmbedded (for Ethereum) for Raspberry Pi. However, most embedded devices have too low computing power, limited data storage, and battery so that even Rapsnode states it would be useless to perform mining on IoT devices (Hang & Kim, 2019).

It is crucial to implement a solution that meets the requirements of a practical IoT network by connecting numerous IoT devices through different constrained networks to a single blockchain. On this basis, our overall artifact adopts the proposed approach by Hang and Kim (2019), who designed an IoT blockchain platform that is suitable for resource-constrained IoT architecture, scalable, and lightweight. In the course of this, IoT devices are not directly integrated with the blockchain network, but alternatively, a Representational State Transfer (REST) Application Programming Interface (API)[6] is defined that handles requests from devices to enable cross-platform communication between devices and the blockchain network (Hang & Kim, 2019; Liu et al., 2020). Consequently, the blockchain is used as an external service to provide reliable and secure storage as well as access control while transactions made by IoT devices are validated in the blockchain network without the need to download the entire blockchain (Hang & Kim, 2019).

3.4.2.1. IoT Blockchain Architecture

Based on the mentioned considerations of Hang and Kim (2019), Pavithran et al. (2020) and Liu et al. (2020), Figure 6 shows a generic and modular IoT blockchain architecture that our artifact relies on, comprising the IoT Physical Domain, Connectivity Domain, IoT Blockchain Service Domain, and Application Domain.

The **IoT Physical Domain** consists of different devices, both sensors and actuators, that can be connected. They are equipped with storage, computing resources, and communication ability (Hang & Kim, 2019). However, IoT devices generally do not have strong computing ability, enough storage, and durable battery, resulting in the inability to be deployed directly as peer nodes of the blockchain. IoT devices have unique IDs that ensure the distinction to other devices. Whenever the device generates a new resource, a message with a payload is sent to the gateway that functions as a message broker within the Connectivity Domain (Hang & Kim, 2019; Liu et al.,

[6] A REST API is a software architectural style that represents a way for two computer systems to communicate over HyperText Transfer Protocol (HTTP) or other protocols in a similar way to web browsers and servers (Buckler, 2020). In this way it provides interoperability between computer systems on the Internet, in our case this is the IoT gateway (connected to devices) and blockchain network.

2020). For this broadcast, a message transmission protocol is needed, which is introduced more in-depth in the next subsection.

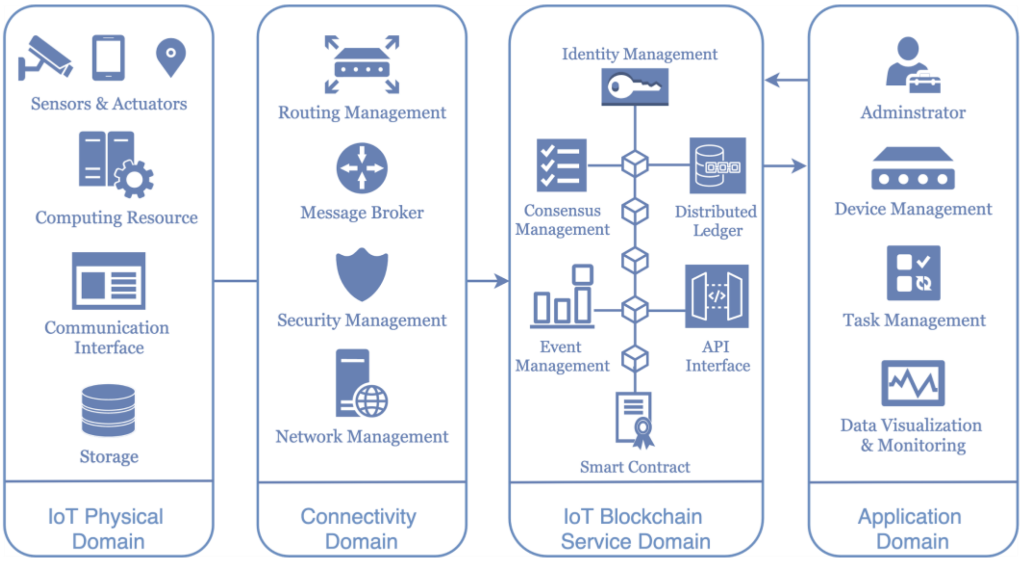


Figure 6: Generic IoT Blockchain Architecture

The **Connectivity Domain** serves as a bridge between the IoT Physical and IoT Blockchain Service domains. As the primary function, it provides the routing management that ensures the self-organization for the Physical Domain, which itself does not have a global internet protocol (IP) (Hang & Kim, 2019). Overall, the message broker receives the message from various devices, bundles them, and routes the content to the blockchain while making sure that the transmission is secure. This domain avoids the pressure on the blockchain caused by otherwise direct access of devices (Liu et al., 2020).

As a next step, the **IoT Blockchain Service Domain** can record the device configuration and sensing data from the Physical Domain routed via the Connectivity Domain in its secure ledgers distributed across the peer nodes. Any changes to the ledger can be reflected in all copies in a minimal time period. Besides, it offers standard services that provide the known features of a blockchain such as identity management, consensus, and smart contracts. Every time a new block is added to the ledger, a new event is sent. The event management can also trigger events based on the condition within the smart contract that could, for example, send back a message to the physical domain causing an action (actuator). To access the services provided by the IoT Blockchain Service Domain, a REST API provides a connection to the application domain in the form of a client (Hang & Kim, 2019).

Finally, in the **Application Domain,** the admin can manage the blockchain network (including its smart contracts), and a regular user can manage its devices (manipulate or control them) as well as visualize data (Hang & Kim, 2019; Liu et al., 2020).

3.4.2.2. Messaging Protocol

IoT applications typically use publish-subscribe or request-reply messaging models to exchange data between IoT Physical and Blockchain Services Domain via the Connectivity Domain. While request-reply messaging models are widely used on the internet by HTTP, it is not ideally suitable for resource-constrained IoT systems. In contrast, **publish-subscribe messaging models** ensure low communication overhead and high resource efficiency (Ramachandran, Wright, & Krishnamachari, 2018). Message Queuing Telemetry Transport (**MQTT**), as an asynchronous and event-based protocol, is particularly lightweight, designed with low bandwidth, versatile, and relatively simple to implement, making it the most widely used in IoT. The transportation of data usually occurs over TCP/IP, but different transport protocols can be used, especially concerning adding more security, TLS/SSL shall be preferred (Fakhri & Mutijarsa, 2018).

As illustrated in Figure 7 based on Thantharate, Beard, & Kankariya (2019), the MQTT architecture has three main components, a client as the publisher, a broker, and another client as the subscriber. A central **message broker**, as also seen in Figure 6 (p. 33), receives the data as a message from one or multiple **publishers**, which are usually IoT sensors. Once the message has been received, the broker sorts and passes the data to subscribers according to categories called "topics". **Subscribers** get push notifications when certain **topics** have new messages. This also means the subscriber has to subscribe to the respective topics before data is published; otherwise, it will not receive it. In the case of an active event management system, the client which subscribed to the data is also able to become the publisher to send data back to the IoT broker to trigger an actuator (Thantharate et al., 2019).

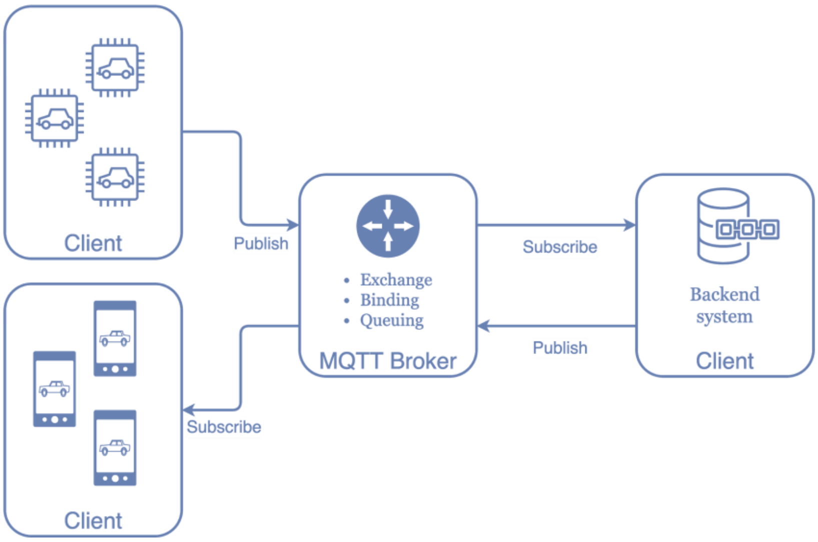


Figure 7: Exemplary MQTT Architecture

More in-depth, the MQTT broker plays a critical role by receiving messages from the publisher and forwarding them to the subscriber. It uses the list of different topics to filter the MQTT clients that are supposed to receive a specific message. Essentially, the topic creates a virtual channel between the particular publisher and subscriber. This avoids the blocking of one client while waiting for the message (Thantharate et al., 2019).

Bringing it in the context of vehicle communication, the MQTT publish/subscribe architecture allows for each vehicle to be decoupled from other vehicles and the backend, enabling a persistent, always-on push connection to the cloud or in our case blockchain. As one of the advantages of MQTT, its queuing system allows the buffering of data when the vehicle is offline. As soon as the vehicle receives a network connection, it publishes the queued data immediately to an MQTT broker, which then can be subscribed by either other cars or the backend system (HiveMQ, 2019).

3.5. Blockchain Platform for IoT

After introducing the interaction between IoT and Blockchain, a reliable, energy-efficient, and scalable platform has to be selected as a critical basis for the demonstration of the designed artifact. Beyond the basic requirement of a decentralized trusted ledger, substantial differences for the implementation can be found within various platforms, e.g., the control mechanism, security, and privacy requirements, consensus mechanism. At the moment, Hyperledger Fabric (HF), Ethereum, and IOTA can be seen as the three most widely utilized implementations of DLT and relevant prospects for an IoT integration (Pustišek & Kos, 2018). In the course of this, the three aforementioned platforms are compared to each other, and then HF, as the applied platform in this paper, is explained in more detail.

3.5.1. Comparison of different Blockchain Platforms

IOTA is an open-source DLT enabling connected devices to transfer data and so-called IOTA tokens without a fee (IOTA Foundation, 2020). The initial idea of IOTA is to design a blockchain technology coping with the challenges of IoT, resulting in design considerations such as scalability, transaction fees, and rapid transaction confirmations (Pustišek & Kos, 2018). IOTA utilizes the so-called Tangle consensus and its own cryptocurrency to account for transactions in its network in a lightweight manner. Compared to other protocols which use cryptographic algorithms, IOTA utilizes quantum-resistant cryptography[7]. This results in IOTA's advanced processing speed and scalability. One major drawback is the absence of a rule which two nodes should be chosen for approval (Pavithran et al., 2020; Popov, 2018).

Ethereum can be described as a trusted computational platform with its own native currency on top of the decentralized peer-to-peer network (Mohanty, 2018). It provides a generalized technology that can serve as a basis for transaction-based state machine concepts (Pavithran et al., 2020). The digital content is saved in a smart contract, written in its native language, Solidity, which is then transferred between the corresponding peers. As a core innovation, the Ethereum Virtual Machine (EVM) eases the development of blockchain applications so that developers can utilize the platform to build their transaction formats, state transition functions, and rules rather than coding everything from scratch (Wood, 2014).

Hyperledger (HL) is an open-source collaborative effort, originally developed by IBM and now hosted by the Linux Foundation. The goal of this project is to advance cross-industry blockchain technologies by providing and improving different blockchain technologies, including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, and sample applications (Hyperledger White Paper Working Group, 2018).[8]

All in all, the most widely used project of HL is the **Hyperledger Fabric** (HF) blockchain for Business-to-Business (B2B) applications due to its high degree of confidentiality, flexibility, resilience, modularity, and scalability (Pavithran et al., 2020; Saghiri, HamlAbadi, & Vahdati, 2020). The architecture of HF is highly modular to provide scalable components including encryption, authentication, consensus algorithm, smart contract, and data storage, which can be configured according to one's needs. This design allows for a broad range of industrial applications as it enables innovation, versatility, and optimization. Up to now, HF is one of the first DLT platforms incorporating smart contracts written in general-purpose programming languages, e.g., Java, Go, and Node.js (Hyperledger, 2019; Pavithran et al., 2020). In Table 4, a more detailed comparison of these three platforms is provided in regard to a variety of characteristics (Pavithran et al., 2020).

[7] Existing cryptography faces the problem that a sufficiently powerful quantum computer could easily solve the mathematical problems that are currently used by most encryption algorithms. Quantum-resistant cryptography refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer (van Rijmenam, 2019).

[8] See more about all Hyperledger projects here: Blockchain Technology Projects

Characteristics	IOTA	Ethereum	Hyperledger Fabric
Control mechanism	Permissionless access	Permissioned and permissionless access	Permissioned access
Type	Not fully open source	Open-source	Open-source
Governance	IOTA foundation	Ethereum developers	Organized under the umbrella of the Linux Foundation
Consensus	Tangle (lightweight consensus designed specifically for IoT)	Customizable	Pluggable consensus (e.g. PBFT, Crash Fault Tolerance)
Smart contract	Currently no support for smart contracts	• Smart contract code (Solidity) • Integrated into the core architecture • Distributed and operated by all nodes within EVM	• Smart contract code (e.g. Go, Java) • Runs inside docker containers • non-deterministic approach
Decentralized data storage	• The implemented protocol is not decentralized or trusting • Usage of a number of central components to maintain its functionality	• Provision of all functions for truly decentralized applications • Decentralization is anchored in the architecture	• Distribution and storage of data by all members of the private HL consortium • Limiting decentralization to attending members
Data security and privacy	• Inclusion of a few measures for data privacy • Suitable communication protocol not yet released	Less extensive range of enterprise and data privacy functions than HF	• Enabling private transactions; accessible only by involved parties • Trust depends on the owner of the blockchain
Immutability & persistency	• No permanent and unchangeable storage of data • No verifiable sources to reconstruct the transaction history	• Decentralized architecture of public chain ensures immutability • Private/consortium chains: central authority possible	• DLT ensures that data cannot be changed • Persistency of data is achieved through DLT

Table 4: Comparison of IOTA, Ethereum and Hyperledger Fabric

IOTA is identified as an unsatisfactory platform due to its permissionless nature. To temper the lack of confidentiality, permissionless systems issue their own tokens to incite costly mining or smart contract execution. The transaction cost and speed can be immensely affected by negative associations with cryptocurrencies. Moreover, it hinders the interaction with other distributed systems such as IoT networks, since the token used in both systems must be unified. In contrast, a permissioned network reduces the risk of a participant intentionally introducing malicious code through the smart contract. These participants are known to each other, and all actions are recorded on the blockchain, based on the endorsement policy established for the network and transaction type (Hang & Kim, 2019).

Overall, Pavithran et al. (2020) confirm HF as the most preferred platform due to its pluggable consensus and provided confidentiality to the data after conducting performance evaluations between Ethereum, HF, and IOTA. This is specifically essential in the case of IoT due to the sensitive nature of the data. Besides, it identified BFT as the most widely used consensus for IoT blockchain due to the minimal requirement of computation effort. As an IoT network needs to be able to handle high throughput, BFT, or CFT consensus protocols should be utilized (Hang & Kim, 2019).

3.5.2. Hyperledger Fabric

Based on the comparison of the most widely used blockchain platforms for IoT in an industrial setting, we decide to build our prototype within the HF platform. Thus, the business network and consensus mechanism of HF is explained in more detail in the following.

3.5.2.1. Business network

The programs related to HF run in docker containers[9]. A separation of the physical resources and application program is given based on the provision of a sandbox environment by the container. The isolation of the containers leads to ensuring the security of the application. Based on the permissioned nature of the HF network, several different consensus mechanisms that can achieve quick consensus in large-scale application scenarios, are provided (Liu et al., 2020).

As a primary communication mechanism in an HF network, **channels** can be created, which allows a consortium of **organizations** to communicate with each other privately. Hence, privacy-sensitive data can be shared between the members of a consortium and provide privacy from other channels and the network. One organization can take part in multiple channels at the same time. In this way, HF enables organizations to efficiently share infrastructure while maintaining data and communication privacy (Hyperledger, 2019). Figure 8 is based on the documentation of HF and demonstrates the simplest HF network with two organizations (*Org1* and *Org2*) joining the same *Channel A,* which is governed according to the policy rules specified in its channel configuration (*CCA*) (Hyperledger, 2019).

[9] Docker is a set of platform as a service products that uses OS-level virtualization to deliver software in packages called containers. Containers are isolated from one another and bundle their own software, libraries and configuration files; they can communicate with each other through well-defined channels (Docker, 2013).

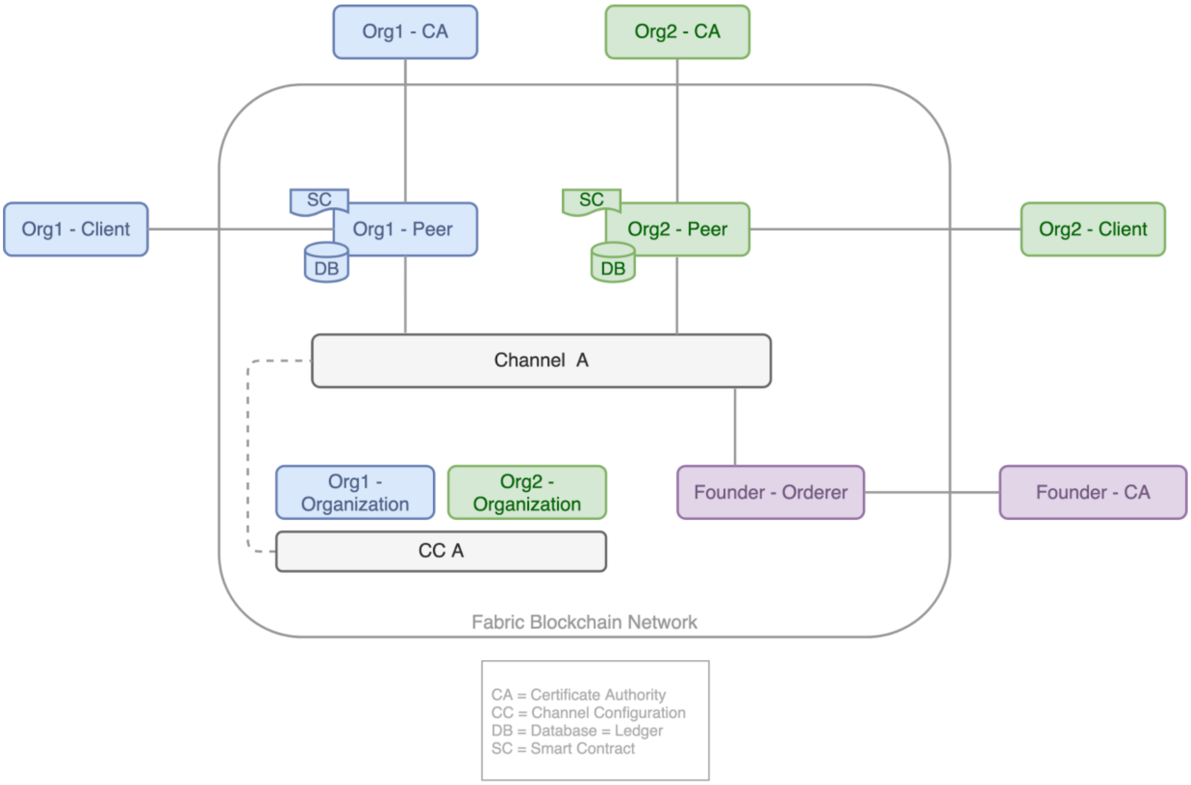


Figure 8: Hyperledger Fabric network with one channel

The first step in defining a network is the set-up of an **ordering service** (*Founder - Orderer*), which is made up of a cluster of orderer nodes. The ordering service can be seen as the initial administration point for the network and is one of the organizations (*Org1* or *Org2*), initially configuring, hosting, and starting the ordering service. The responsibilities of the ordering service include the acceptance of transactions sent by the peer node, the sorting of transactions based on predefined rules, the packaging of transactions in blocks, and the distribution to the peer node. The local ledger (*DB*) is then updated with new blocks by the peer node and reaching consensus. There are several different implementations for achieving consensus on the strict ordering of transactions between ordering service nodes, which are introduced more in-depth in the next subchapter (Hyperledger, 2019).

The **Certificate Authority (CA)** (*Org1 - CA; Org 2 - CA; Founder - CA*) is needed to issue or cancel certificates to administrators and network nodes. These are used to identify components in the network as belonging to a specific organization. These certificates represent the digital identity of the actors. The importance of those digital identities stems from their ability to determine the exact permissions over resources and access to information that actors have in a blockchain network. Furthermore, certificates play an essential role in the transaction generation and validation process. The certificates are used to digitally sign transactions during the client application transaction proposals and the smart contract transaction responses (Hyperledger, 2019).

Client Applications (*Org1 - Client; Org2 - Client*) are outside of the network and can use a channel to connect to specific network resources. The Client Application is the interaction gateway of the external world with the chaincode deployed on the Fabric network. The interactions are enabled by Software Development Kits (SDK). A client application receives an identity associating it with an organization. Each access of the client application with the ledger is managed by a smart contract called in HF, a **chaincode** (*SSC; SC*). The chaincode defines the common access patterns to the ledger. In other words, it provides a defined set of ways by which the ledger can be queried or updated. Chaincodes are created by application developers and define business processes shared by the consortium members (Hyperledger, 2019).

As another network component, **peer nodes** (*Org1 - Peer; Org2 - Peer*) are hosting the copies of the blockchain ledger. Each peer node receives an identity issued by the central authority, which associates the peer with the corresponding organization and allocates the permissions for this particular peer. Two main types of peers are defined in HF: endorser and committer. Endorsing peers are responsible for the verification, simulation, and endorsing of transactions. Each committing peer receives blocks of generated transactions that are subsequently validated and then committed to the peer node's copy of the ledger as an append operation (Hyperledger, 2019).

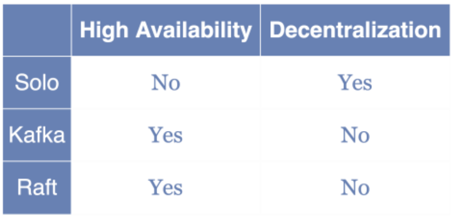
3.5.2.2. Consensus Mechanism

Fabric supports pluggable consensus protocols which enable the platform to be more customizable to particular use cases and respective trust models. The consensus protocols do not require cryptocurrency incentives for mining or fueling the execution of smart contracts. HL offers three different types of ordering service implementations: Solo, Kafka, and Raft (Hyperledger, 2019), which are summarized in regard to availability and decentralization in Table 5.

Solo can be utilized to evaluate proof of concepts and test the logic for applications and smart contracts. This is based on the fact that Solo implements only a single ordering node, resulting in losing the advantage of the network of being fault tolerant. Hence, the Solo network should not be utilized for the production environment but is beneficial for prototyping (Hyperledger, 2019).

Kafka is a multi-node ordering service and utilizes a leader-follower configuration. As only the leader executes the ordering and the so-called in-sync replicas can be voted as the leader, Kafka provides CFT, and the finality happens in a matter of seconds. However, Kafka is not BFT, resulting in the prevention of reaching an agreement in case of malicious or faulty nodes (Hyperledger, 2019).

Raft can be compared to Kafka, also following a leader-follower configuration. The design allows the contribution of nodes to a distributed ordering service by different organizations (Hyperledger, 2019). Raft is the first step toward HF's development of BFT ordering service and to more decentralization (Dedeoglu et al., 2020).



	High Availability	Decentralization
Solo	No	Yes
Kafka	Yes	No
Raft	Yes	No

Table 5: Comparison of consensus mechanisms in HF

3.6. Blockchain & Car Sharing

After examining the domains blockchain and car sharing separately, next, it is essential to explore the existing research of blockchain in the context of car sharing and leasing. As P2P car sharing is the focused model in this thesis, only its specific interface with blockchain is examined.

3.6.1. Blockchain for P2P Car Sharing

For many people renting out a car is a particularly sensitive topic due to its monetary but also psychological value. While most P2P car sharing platforms aim to establish trust towards an unknown person with common rating and review processes, such traditional reputation systems often reach their limits so that users lack confidence in a neutral damage event regulation (Bossauer et al., 2019). To address this ongoing **lack of trust**, some providers started to implement telematics into the private vehicles to track the location, mileage, fuel consumption, and much more. Even though this generated personal data aims to make lending the car more trustful, it can also cause a new problem: suspicion in regard to the usage of data. While a centralized membership system and pricing scheme could make it possible to use such personal data to undermine fairness[10] and privacy, a **decentralized solution** would be able to protect the privacy of users and preserve their trust (Madhusudan et al., 2019). As an example, with

[10] As an example, Uber charges its customers based on an algorithmic prediction of how much they are willing to pay rather than the services they receive (Newcomer, 2017). Another issue might be the targeted exclusion for their services such as Airbnb has been in the news about it (Collins, 2018).

blockchain, the link between the real identity of a user and a particular route driven may be protected (Dorri et al., 2019).

From a business point of view, P2P car sharing providers are usually cooperating with various stakeholders, especially insurance companies. In this regard, it could be a fairer and more convenient way for all parties involved to charge for insurance based on usage with the help of telematics. These processes can be optimized by using blockchain, providing a **secure sharing of data** with one single truth instead of relying on siloed databases of each stakeholder that are disconnected from each other (Gösele & Sandner, 2019).

Overall, it is questionable whether a P2P car sharing company connecting and tracking a large number of vehicles could scale with a centralized brokered communication model where all users and private vehicles are identified, authenticated, and authorized through a central cloud server. A centralized cloud server may remain a bottleneck and a **single point of failure** that can break the entire network (Dorri et al., 2019; Valastin et al., 2019). In contrast, when data is distributed and processed over a whole network of nodes like blockchain, it is practically impossible to tamper the service (Nakamoto, 2008).

3.6.2. Blockchain for Car Leasing

As car leasing exists already for years, many of its processes are traditionally cumbersome, such as customer bank validation, along with multiple phases of the transaction set-up in compliance with know-your-customer (KYC), and much more (Guhathakurta, 2018). To ease these processes, blockchain can connect the involved stakeholders, perform **KYC checks** before leasing a vehicle, store the leasing contracts, and automate the payment while leveraging **secure communications** and eliminating data risks. The retrieved data can be used for analytics and for monitoring consumer behavior (KYC) in car leasing or rental (Fraga-Lamas & Fernandez-Carames, 2019). Eventually, the leasing provider can assess more accurately the residual value of the vehicle at the end of a lease. Again, a telematics connected vehicle could capture the needed data and send it to a shared ledger that all parties had access to, including the lessee, insurance company, and manufacturer. On the one hand, this would enable the leasing provider to achieve a higher price at a subsequent onward sale, on the other hand, it provides **transparency** for the lessee to help eliminate end of lease disputes (Guhathakurta, 2018).

Overall, this domain, blockchain for car leasing, is still a relatively unexplored area where most publications only mention it as a side example within the application blockchain for the automotive industry. However, pilot projects such as Visa and DocuSign demonstrate that this area has slowly started to gain some traction.[11]

While the domain blockchain for car sharing has attracted some research interest, so far, most academic publications have focused on either the technical implementation or the socio-behavioral aspects of blockchain in mobility from a user perspective without assessing the greater impact on the industry. In addition, most scholars demonstrate blockchain applications in the context of carsharing with the Ethereum blockchain platform leading to a lack of concrete implementation with HF and the integration of IoT. Finally, the domains of car sharing and leasing, in combination with blockchain, are researched solely separately.

We aim to fill this gap by following the design science research method for the development of a blockchain-based platform streamlining car sharing and leasing processes while demonstrating the applicability of an IoT and blockchain integration in HF. Thus, we are evaluating both the technical implementation and the industrial impact on OEMs, P2P car sharing providers, and municipalities.

[11] In 2015, Visa and Docusign implemented a blockchain for a car leasing pilot service where the user can configure the lease and insurance within minutes inside the show-cased car *(*Hirson, 2015*)*.

4. Design & Development

Based on the literature review, we can derive the motivation for the design and desired functionality of the artifact. The artifact consists of a **conceptual design** and **high-level architecture** demonstrated by implementing a transaction as **prototype**. It represents our overall idea of a blockchain-based P2P car sharing platform that brings together various stakeholders involved in the car sharing and leasing process streamlining their workflows. In the following, the problem identification and derived key design principles that lead to the designed artifact are explained in detail. In the course of designing the artifact, certain assumptions are made to focus on the major features and maintain a feasible scope.

4.1. Problem Identification

Inspired by the two current movements, car sharing and usage of blockchain within the automotive industry, we aim to explore more in detail how blockchain could facilitate a seamless P2P car sharing experience initiated by OEMs. So far, this combination does not exist per se as P2P car sharing is commonly undertaken by a third party platform (Münzel et al., 2020). While especially the last decade attracted many traditional businesses and new players to develop various car sharing business models, it has yet not found the right deployment at a commercial scale.

P2P car sharing represents the smallest percentage of providers and is available in the least countries compared to B2C car sharing models. Nevertheless, it has the greatest potential of expanding quickly within one country due to its **strong network effects**, resulting in P2P car sharing being active in more cities than other models (Phillips, 2019). More in-depth, P2P car sharing providers experience challenges to overcome the barrier of **country-specific** insurance regulations as well as the **trust** of car owners to share their cars. But once these issues are remedied, it is relatively effortless to add a large number of vehicles to the network since the cost of ownership is transferred to the individual owner instead of the fleet management firm (Münzel et al., 2020). Along these lines, B2C car sharing models, usually operated by an OEM, affirmatively have to invest in an entire car **fleet** resulting in **enormous operation costs** making car sharing only beneficial for the OEM if the market size is sufficiently large (Ke, Chai, & Cheng, 2019; Shaheen et al., 2012). The faster **network growth pace** of P2P car sharing, once established in one country, and the substantial experience and **resource capacity** of OEMs serve as motivation to design a P2P car sharing platform initiated by OEMs that could provide the sufficient market size while keeping the operational costs low.

At the same time, leasing in the automotive industry has been growing rapidly in the last few years and has become more attractive to be managed by the OEMs themselves than a bank (Pfeifle et al., 2017; Sultan, 2016). Fleet management with **leasing** is gaining importance, especially in a world of changing mobility where the trend towards sharing is visibly influencing the strategic decisions of OEMs (Pfeifle et al., 2017). Since leasing can keep OEMs in the loop of the **customer value creation** and give the customer the **feeling of owning** (i.e., psychological ownership) (Guhathakurta, 2018; Guyader & Piscicelli, 2019; Paundra et al., 2017; Peck & Shu, 2018), car leasing can be seen as a potential bridge to enable the P2P car sharing concept initiated by an OEM. This can ease the process for users and companies alike through collaboration on data, resources, and contracts (Fraga-Lamas & Fernandez-Carames, 2019; Guhathakurta, 2018). Thus, an all-in-one platform approach that involves the entire process from leasing a car, getting insurance to P2P car sharing, paying off the leasing fee, may be able to move forward car sharing.

As another motivation, there is a need to address the problem of **data silos** progressively caused by the growing amount of car sharing providers. Whenever a user is interacting with a different car sharing business, a **new digital persona** is created, which is disconnected from each other, leading to data silos that do not communicate with each other. This raises costs in the form of reconciliations, lost time, and missing records that may result in errors, waste of resources, fraud, and abuse (Ferdous, Chowdhury, & Alassafi, 2019). As one example, a deceptive user who committed fraud at one car sharing platform may easily just switch the platform and repeat the same behavior without the new platform knowing about his fraudulent history.

Finally, the sharing of telematics IoT data collected by vehicles is crucial for streamlining the processes of car sharing and leasing on one platform (Dorri et al., 2019; Gösele & Sandner, 2019). However, this results in a need for a **persistent and scalable IoT infrastructure** and network (Dedeoglu et al., 2020; Reyna et al., 2018). Various research confirms that blockchain can address some of these IoT challenges (Dedeoglu et al., 2020; Hang & Kim, 2019; Pavithran et al., 2020; Reyna et al., 2018). Nevertheless, there is a **lack** of a detailed and hands-on demonstration **integrating IoT with blockchain**.

Identified by the comparison in chapter 3.5.1 Comparison of different Blockchain Platforms, the **modularity of HF** can be utilized to support the development of an inclusive platform spanning from OEMs over leasing and insurance companies to end-users. Current implementations and example use cases of HF (e.g., P2P ride-hailing) shows the applicability of HF for such use cases (Hyperledger White Paper Working Group, 2018; Shivers et al., 2019). Now, we aim to utilize the collected knowledge of such use cases to explore the implementation of HF in combination with IoT as a possible approach to build a blockchain-based car sharing platform.

Conclusively, an artifact for a blockchain-based car sharing platform is designed, and the HF implementation for a part of it is demonstrated to eventually answer how blockchain may be able to advance car sharing in the future.

4.2. Key Design Principles

To develop a suitable artifact aiming to resolve the identified problems, five key requirements and design principles are derived from the literature review.

Security & Privacy
Due to the tremendous amount of data exchanged between stakeholders (Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019; Le Vine et al., 2014), the platform has to handle privacy-sensitive data of each user securely and reliably, for instance, personal information related to leasing contracts, driver's license, and telematics data (e.g., location, mileage, fuel consumption). The system is required to prevent any possible data breaches and manipulation or sharing to inadmissible stakeholders. Consequently, the common third party as the central authority (e.g., car sharing platform) needs to be eliminated leading to a decentralized design to avoid a single point of failure (Christidis & Devetsikiotis, 2016; Dedeoglu et al., 2020; Hawlitschek et al., 2020; Rathee, 2020; Reyna et al., 2018). In addition, an corresponding encryption mechanism has to be implemented, and the immutability of the data needs to be ensured (Pavithran et al., 2020; Reyna et al., 2018). Finally, a permissioned network with a consensus mechanism of at least CFT is needed to make sure that only the participating organizations have access to the data they need or the data owner is willing to give access to (Hang & Kim, 2019; Xiao et al., 2020).

Authenticity
The required tracking of telematics data and access tools leads to a vast amount of connected IoT devices. The illegal access to IoT devices and related data has to be avoided to address the common trust problem in P2P car sharing. In other words, IoT devices need to be authenticated in a secure way to make sure that only eligible stakeholders can access and use its data (Pavithran et al., 2020; Reyna et al., 2018). In addition, every user of the system needs to be identified in a secure way getting a unique digital identity that can be used for all the different services with access to the required data on the platform. This can be achieved by implementing a suitable digital identity management system where every entity can be identified and traced (Hang & Kim, 2019). As a result, the current problem of duplicate digital personas and data silos created across various platforms is eliminated (Ferdous et al., 2019).

Traceability & Reliability

The sharing of a car includes the consideration of the monetary and psychological value the car owner associates with it (Paundra et al., 2017; Peck & Shu, 2018). Especially when interacting and sharing a valued possession with an unknown person, uncertainty about, e.g., odometer fraud or damage has to be minimized (Bossauer et al., 2019; Madhusudan et al., 2019). On the platform, data from different sources will be shared, and various transactions will be executed, e.g., signing a leasing contract, renting a car, choosing an insurance plan. This leads to the requirement of one single truth of the stored data, resulting in the assurance for each user that the same data is shared (Gösele & Sandner, 2019). The reliability that the recorded data is correct, short- and long-term, needs to be facilitated. Consequently, the system requires an immutable history log of the executed transactions and car-related data (e.g., damages). It is essential for each participant involved to be certain about the serviced car and the traceability of the car in case of, e.g., fraud, theft, or damages.

Scalability

As the platform aims to incorporate many different participants and IoT devices that generate a large data stream, a well-considered architecture is needed (Hang & Kim, 2019; Liu et al., 2020). In this way, there is a need to assess to which extent the IoT interaction takes part within the blockchain to meet different criteria in regard to security, storage, and especially scalability (Pavithran et al., 2020; Reyna et al., 2018). Moreover, the system and its network will be used by many different participants exchanging various forms of data (Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019). Consequently, the system and the IoT network have to be scalable to a large degree.

Interoperability

Due to the involvement of many different stakeholders and complex interdependent processes within the car sharing and leasing process, it is necessary to optimize processes within each business but also in combination. Today, each of the stakeholders has its own established business logic, which needs to be aligned with each other to be able to collaborate on one platform (Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019; Guhathakurta, 2018). This can be reached by automating processes and streamline those which overlap.

The ease of use has to be ensured to minimize the effort of affiliating the differing systems and align the business processes since a significant number of different users with varying technical and business skills will access the system. Consequently, a modular architecture of the system is needed, which enables the system to be customizable to the different use cases and stakeholders (Pavithran et al., 2020).

4.3. Assumptions

As the whole P2P car sharing process incorporates many different stakeholders and industry-specific requirements, assumptions need to be made to provide a feasible artifact and focus on the core functionalities.

Overall, the conceptual design is simplified, consisting of the main processes derived from the research so that some smaller details are disregarded (especially in regard to the detailed car ordering and KYC process). In the same manner, it is assumed that the car dealer is included in the stakeholder OEM in the form of direct sales.

First, it is assumed that one or more OEMs are willing to set up the network and take on the role of the initial admin adding the different stakeholders (e.g., leasing company, insurance company). This assumption is necessary as a blockchain network needs to be developed and initialized by a capable entity or consortium of entities. Additionally, it is assumed that OEMs have the capabilities to manufacture cars that include the needed technology and add cars to the blockchain.

Based on the focus of this thesis on the business aspects of implementing blockchain for car sharing, the government is not included in the conceptual design. The government takes on a relevant role in the setup of the car sharing network, which will be elaborated in the evaluation and discussion (cf. 6 Business Evaluation of Artifact & 7 Discussion).

Concerning the leasing company, the assumption is made that the leasing contract legally allows each lessee to rent out the respective car via a P2P car sharing platform. Evaluating the details and restrictions of leasing contracts exceeds the scope of this artifact. Thus, car leasing serves solely as a bridge to enable the blockchain-based car sharing platform but is not examined in-depth.

Moreover, it is assumed that the leasing and insurance companies collaborate, hence the leasing package includes insurance. In the same manner, the leasing company can be both external and internal independent of the OEM.

Lastly, it is assumed that each payment is made in the form of cryptocurrency or other tokens[12]. This avoids the reliance on payment service providers (PSP), leading to almost fee-less payment transfers. As the blockchain-enabled payment options are more advanced concerning research

[12] Tokens can represent any form of economic value. In the context of blockchain, cryptographic tokens are programmable assets or access rights managed by smart contracts and underlying distributed ledger (Voshmgir, 2019).

and implementation, the inclusion would distort the focus of the artifact and will be included in the chapter 7 Discussion.

4.4. Designed Artifact

Based on the literature review and the derived key design principles, the design of the artifact is drawn that encompasses a **conceptual design** and **high-level architecture** enabling **use cases**. The conceptual design represents an all-in-one platform showcasing how blockchain can be able to bring together different stakeholders streamlining the leasing and car sharing processes by recording and executing agreements as well as monetary transactions securely and reliably. It aims to support the movement of shifting from ownership to access inherited in the concept of car sharing while enabling lessees to pay off their monthly leasing fee by renting out the car when it is not in use. Besides the described conceptual design, the possible high-level architecture on which our platform is based as well as an overview of potential use cases of the **blockchain-based car sharing platform**, is outlined.

4.4.1. Conceptual Design

Overall, the upcoming description of the conceptual design focuses on the rather conceptual layout than the technical implementation, which will be elaborated in-depth in the chapter 5 Demonstration of Keyless Vehicle Access Control. The conceptual design, shown in Figure 9 (p. 51), involves four main stakeholders, *Short-term renter* (representing the car sharing renter), *Lessee*, *OEM,* and *Leasing Corp,* which incorporates the insurance company. It describes the ten main steps in a scenario where a *Lessee* orders a car via the *Leasing Corp* and rents out the leased car to a *Short-term renter* to help pay-off the leasing fees. This scenario is handled in one platform unifying and securing all processes in the blockchain. In the following, these steps and processes with the needed blockchain registrations and smart contracts are described in detail, referring to the specific step with its respective blue highlighted number from Figure 9.

As a first step, one or multiple *OEMs* **initiate the blockchain network** taking on the role of the developers, general administrators, and founders. Afterward, other stakeholders can be **registered** to the blockchain network, and the *OEM* lists all available car models with the information about color, fuel, transmission, motor, extra features like roadside assistance, and more on the blockchain (1). Naturally, it would be possible to transfer all the data of the existing car models to enable the shift from a central database to the blockchain. Once the stakeholders are registered to the blockchain, every entity receives a unique **digital identity** by the certificate authority of the blockchain. This identity, which includes a wallet with a public and private key, is fundamental for the involved stakeholders to interact with the platform. Both the *Lessee* and *Short-term renter* need to submit essential documents such as driver licenses and ideally link their banks with their digital identity.

After all available car models are listed on the blockchain, the potential *Lessee* can browse the different models and eventually **select a car** choosing different preferences and customizations (2). In the course of this, the *Lessee* also needs to choose a suited leasing and insurance plan. All this data is stored securely in the blockchain and made available to only those stakeholders who need the data to process the leasing contract. In addition, the *Lessee* can select whether the soon-to-be leased car for short-term rental should be listed, helping to pay-off the monthly leasing fee. In case that option is chosen, the car is listed tentatively and will be turned into a confirmed listing automatically as soon as the *Lessee* receives the car.

As a next step, a smart contract between the *Lessee* and the *Leasing Corp* is triggering a leasing request event on which basis the *Leasing Corp* can perform the KYC check efficiently within the platform. This requires that the potential *Lessee* provided access to bank history by linking his/her digital identity with his/her bank. Once the **lease is approved** (3), the *Leasing Corp* can store the leasing contract on the blockchain, order the car and track the **car production** right from the *OEM* within the blockchain (4a), bringing great visibility across the leasing journey. Overall, the *OEM* can use the same blockchain-based platform to get an end-to-end supply chain experience creating, updating, and verifying documentation as well as seamlessly process payments with all parties involved.

After a successful KYC check and production of the respective car, the *Lessee* **receives the car** (4b). The delivery of the car is tracked in the blockchain and automatically initiates the confirmation of the listing for short-term rental in case the *Lessee* chose this as an option. In this regard, the *Lessee* can adjust the availability of the car for short-term rental by providing a suited schedule in which the car is automatically made available for rent. To ensure trust, the mileage, fuel, and other IoT telematics data of the car are immutably and securely stored in the blockchain avoiding odometer fraud and ensuring transparent handling of insurance claims. While the **tracking** of telematics data is only displayed during the rent between the *Lessee* and the *Short-term renter* (8b), it applies to the entire period of the car usage, both leasing and short-term rental (hence as soon as (4b) starts).

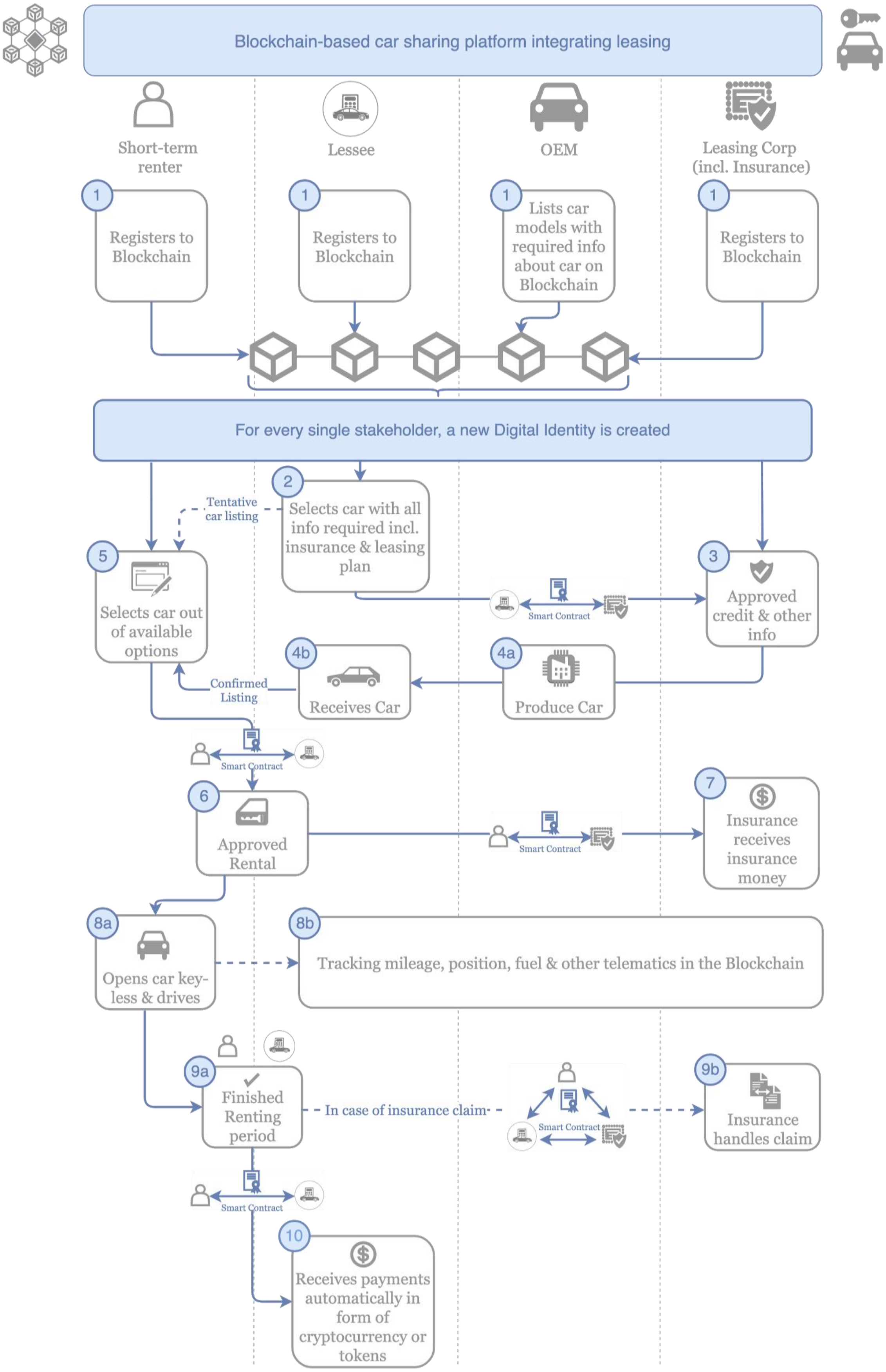

Blockchain-based car sharing platform integrating leasing
Short-term renter
Lessee
OEM
Leasing Corp (incl. Insurance)
1
Registers to Blockchain
1
Registers to Blockchain
1
Lists car models with required info about car on Blockchain
1
Registers to Blockchain
For every single stakeholder, a new Digital Identity is created
Tentative car listing
2
Selects car with all info required incl. insurance & leasing plan
5
Selects car out of available options
Smart Contract
3
Approved credit & other info
4b
Receives Car
4a
Produce Car
Confirmed Listing
Smart Contract
6
Approved Rental
Smart Contract
7
Insurance receives insurance money
8a
Opens car key-less & drives
8b
Tracking mileage, position, fuel & other telematics in the Blockchain
9a
Finished Renting period
In case of insurance claim
Smart Contract
9b
Insurance handles claim
Smart Contract
10
Receives payments automatically in form of cryptocurrency or tokens

Figure 9: Conceptual design of a blockchain-based car sharing platform integrating leasing

Assuming that there have been several leased cars made available for short-term rental, the **Short-term renter** is now able to **select a car** near-by from available options varying in type and time availability (5). The short-term rental includes usage-based insurance, ensuring that both the *Lessee* and *Short-term renter* can be certain of an all-time insured car. Next, a smart contract between the *Short-term renter* and *Lessee* provides the necessary background check in regard to driver licenses and the validity of both parties with the help of their digital identities.

This leads to an **approved rental** (6) where the **insurance money** included in the renting price is automatically transferred to the insurance company based on the execution of another smart contract between the *Short-term renter* and the insurance company (7). After the approved rental request, the *Short-term renter* can **open the car** keyless with a smartphone at the requested time entering the unique private key and the license number of the respective car (8a). Now, he/she can drive the car during the agreed time. Due to the continuous storing of telematics data, potential damages on the car, as well as fuel and parking expenses, can be transparently tracked on the blockchain (8b). In the course of this, the platform will automatically charge the *Short-term renter* a fee in case of extended driving time.

Once the **rental period is finished**, the *Short-term renter* closes the car with the smartphone, which triggers an event in the blockchain that changes the status of the car as being securely closed (9a). All information regarding possible damages that happened during that rental period is cross-checked with the previously stored data in the ledger and alarming the *Lessee* in case of any discrepancies. In case of actual damage or even accident, the insurance is automatically notified and can securely access all the needed telematics data from the car on the shared ledger to process an **insurance claim** in the form of another smart contract (9b).

Finally, *Lessees* receive the appropriate **payment** for renting out their cars in the form of cryptocurrency or other tokens, ensuring an almost fee-less payment transfer for the *Lessees* and *Short-term renter* (10). Again, this is handled through a smart contract to ensure a fair payout based on the actual usage of the car. Once the rental process is completed, the status of the car is automatically changed back to available so that it is listed for a new rental.

4.4.2. High-level Architecture

A reliable platform needs to base on a well-designed system architecture. Inspired by Hang & Kim (2019), Liu & Han (2020), and Yuan & Wang (2016), we derived the high-level architecture shown in Figure 10. This also serves as the foundation for the prototype demonstrated in chapter 5 Demonstration of Keyless Vehicle Access Control. The architecture consists of the same main parts from Figure 6 on page 33, *IoT Physical Domain*, *Connectivity Domain*, *IoT Blockchain Service Domain,* and *Application Domain*. The architecture is extended with reference to the conceptual design to give a more detailed insight, especially in regard to the *IoT Blockchain Service Domain*.

The **IoT Physical Domain** encapsulates various embedded devices; in our case, mainly, the vehicles are equipped with a unique digital identity, inbuilt telematics, storage, computing resources, and communication interfaces. In general, IoT devices do not hold strong computing ability and enough storage so that in this architecture, the IoT devices are not directly deployed as peer nodes of the blockchain (Hang & Kim, 2019; Liu et al., 2020). The generated vehicle and real-time data (e.g., driving behavior, telematics) can be securely recorded through the connectivity layer into the immutable ledger of the blockchain. As soon as the device generates data, it is published as payload to a relevant topic on the MQTT broker located in the *Connectivity Domain*.

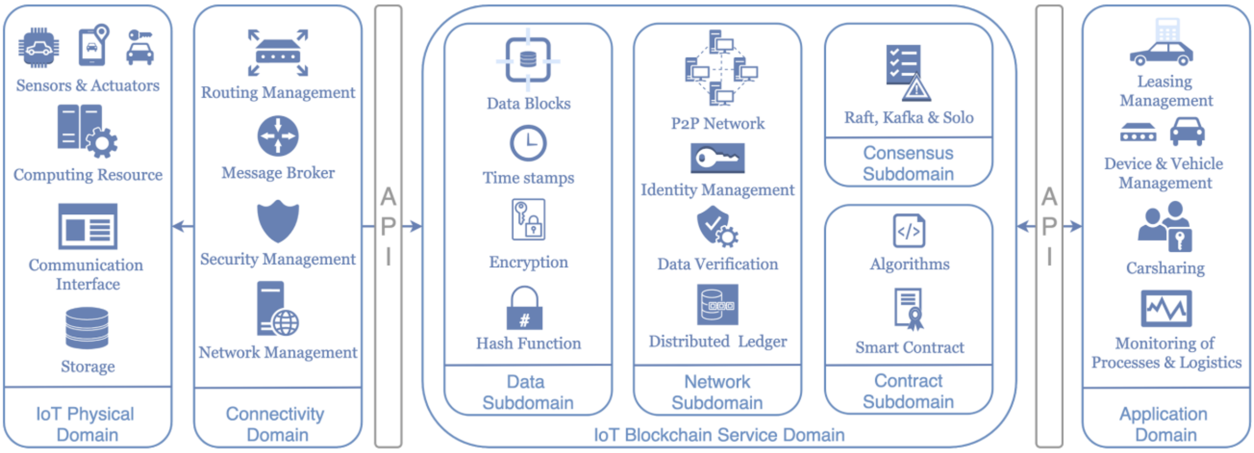


Figure 10: High-level architecture for the conceptual design

Serving as a bridge between the physical devices and the blockchain, the **Connectivity Domain**'s messaging broker receives the payload from various vehicles and checks whether any backend server, the blockchain network, subscribed to the respective topic. Then, the payload is bundled and routed securely via TIP/SSL to the *IoT Blockchain Service Domain*. Similarly, the blockchain network can publish a message with control information to the broker in the *Connectivity Domain* to trigger a specific action within the vehicle (*IoT Physical Domain*), e.g., unlocking the car after checking the validity of the driver. This time the vehicle subscribes to the registered control topic to receive the message. Overall, the purpose of the *Connectivity Domain* is to reduce the pressure on the blockchain that would otherwise be caused if the devices accessed the blockchain network directly.

As the core of the system, the **IoT Blockchain Service Domain** exposes REST APIs to access for users (e.g., short-term renter or lessee) in the *Application Domain* and message brokers in the *Connectivity Domain*. In other words, all the product-specific services provided by the blockchain network are accessible through REST APIs, which can be invoked by either web clients (*Application Domain*) or IoT devices (via the *Connectivity Domain*). The *IoT Blockchain Service Domain* consists of four subdomains, namely *Data*, *Network*, *Consensus,* and *Contract Domain*. As a possible scenario, a candidate block is created from the IoT data, which ensures the appropriate encryption, timestamping, and hashing of the data (**Data Subdomain**). Afterward, the block is broadcasted to the P2P network in the **Network Subdomain**. The network consists of all stakeholders involved in the conceptual design, while each of them has different kinds of permissions and access to smart contracts, especially in regard to the ability only to read or also write. Even the read permissions are limited to some of the stakeholders, for example, the *Short-term renter* should not have access to anything related to the leasing contract between the *Lessee* and the *Leasing Corp*. These permissions are defined in the identity management of the *Network Subdomain* and self-executed by smart contracts.

Once every node receives the transaction proposal, the received block can be verified according to predefined specifications in a smart contract. The decentralized nodes reach a consensus based on a defined **consensus** mechanism, in our system Kafka, Raft, or Solo, by using the permissioned blockchain platform, HF. Once consensus has been reached, the block is ready to be appended to the blockchain and distributed to every node's immutable ledger.

More in-depth, smart contracts are self-verifying, self-executing, and self-enforcing state-response rules that are stored on and secured by the blockchain. Before a smart contract can be self-executed on each node during the transaction verification process, one or more parties consent to all the terms within a smart contract signing it cryptographically and broadcast it to the nodes that need that particular smart contract (Yuan & Wang, 2016). In the conceptual design, smart contracts are used for different use cases from managing vehicles and their real-time data to authorizing the unlocking of a car based on an existing rental request (cf. Figure 9, p. 51).

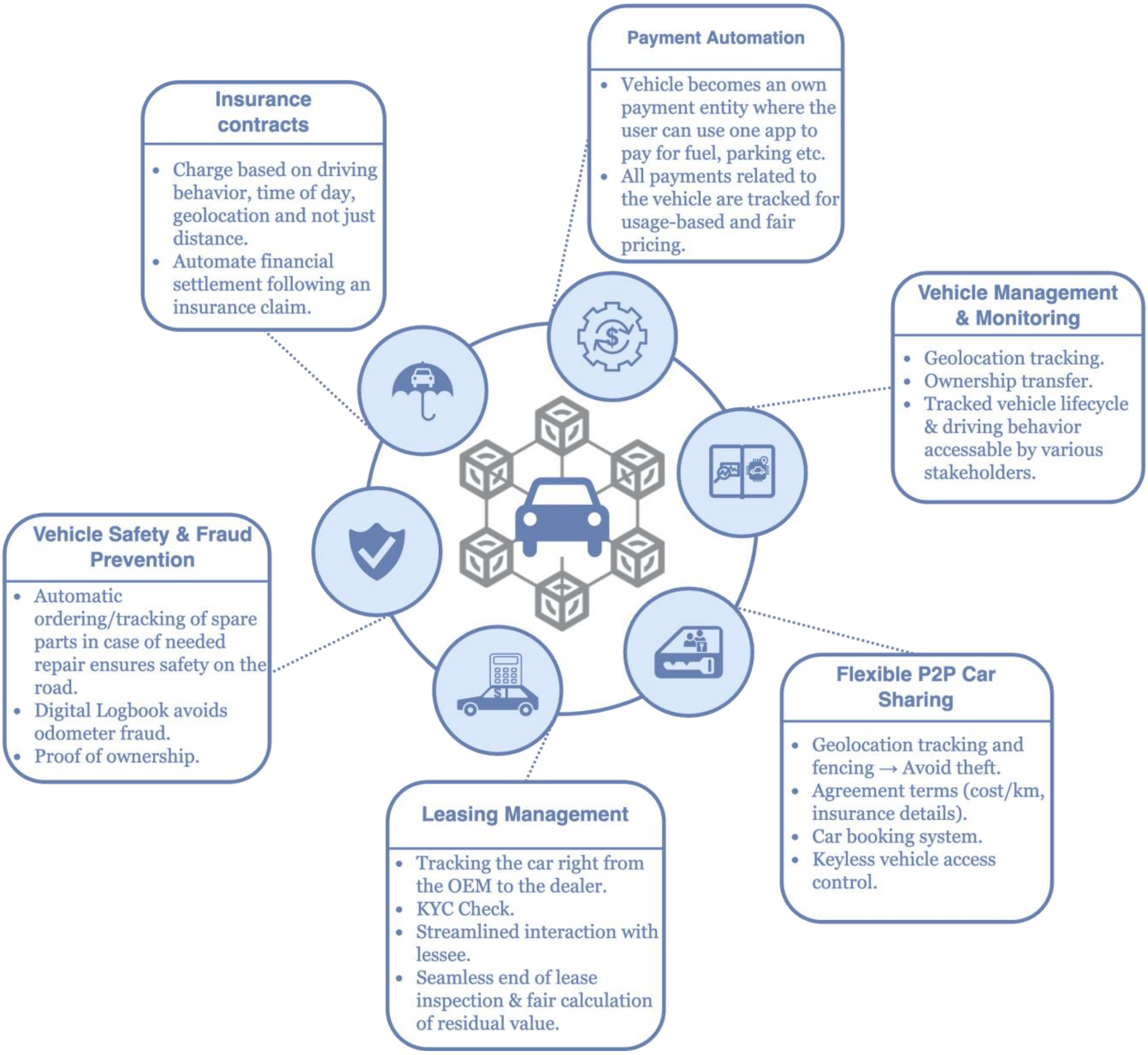
Besides verifying transactions that are triggered by the IoT network, another REST API can expose access to the blockchain coming from the **Application Domain**. It packages potential application scenarios and use cases of the conceptual design (Yuan & Wang, 2016).

Administrators can add and upgrade smart contracts as well as manage the overall blockchain system. In the conceptual design, the *OEM* is the one initiating and administering the network. Nevertheless, other stakeholders can receive similar permissions through respective certificates handed out by the *OEM*. On the other side, the regular user, e.g., the *Short-term renter*, can send attribute-based authorization requests to the blockchain system (Liu et al., 2020) to register, make a car sharing request and handle the insurance. There are various use cases that the conceptual design encompasses involving different stakeholders, which are described more in-depth in the next subchapter.

In summary, we adopt a **lightweight solution** where the blockchain is used as an external service to provide reliable and secure storage as well as trustful and seamless identity management that may drive the collaboration between different stakeholders of the conceptual design. Thus, the architecture aims to avoid integrating blockchain technology directly into the IoT network, including devices and gateways.

4.4.3. Overview of Use cases

During the description of the conceptual design, various use cases have been introduced, ranging from usage-based insurance to flexible P2P car sharing. The overview shown in Figure 11 represents the six main use cases that the conceptual design enables. Each use case can be split into further sub use cases, of which we demonstrate one in the next chapter (*Keyless Vehicle Access Control*).



Payment Automation

- Vehicle becomes an own payment entity where the user can use one app to pay for fuel, parking etc.
- All payments related to the vehicle are tracked for usage-based and fair pricing.

Insurance contracts

- Charge based on driving behavior, time of day, geolocation and not just distance.
- Automate financial settlement following an insurance claim.

Vehicle Management & Monitoring

- Geolocation tracking.
- Ownership transfer.
- Tracked vehicle lifecycle & driving behavior accessable by various stakeholders.

Vehicle Safety & Fraud Prevention

- Automatic ordering/tracking of spare parts in case of needed repair ensures safety on the road.
- Digital Logbook avoids odometer fraud.
- Proof of ownership.

Flexible P2P Car Sharing

- Geolocation tracking and fencing → Avoid theft.
- Agreement terms (cost/km, insurance details).
- Car booking system.
- Keyless vehicle access control.

Leasing Management

- Tracking the car right from the OEM to the dealer.
- KYC Check.
- Streamlined interaction with lessee.
- Seamless end of lease inspection & fair calculation of residual value.

Figure 11: Overview of use cases enabled by the conceptual design

5. Demonstration of Keyless Vehicle Access Control

After describing various use cases of the chapter 4.4.1 Conceptual Design, we decided to focus on the use case of **keyless vehicle access control** to demonstrate a simplified and scoped-down version of the conceptual design. Since there is a need for a secure communication channel to facilitate a trusted interconnection between smart vehicles and a user (Dorri et al., 2019), we see the particular use case as a suitable example to demonstrate a technical implementation of the conceptual design. Due to the complexity of the proposed artifact, we have seen the need to scope down the artifact to the particular **use case** and finally to just **one transaction** within the use case involving only the *Short-term Renter*. We refer to this scoped-down use case as a “prototype” in the remaining part of this thesis.

By **implementing a prototype**, we aimed to get a better understanding of how one of the blockchain platforms, HF, works together with IoT. In this way, we can evaluate blockchain’s applicability for car sharing not just from a theoretical but also practical perspective. In addition, the prototype aims to provide hands-on implementation of an HF application that is not only understandable for technical but also business audience.

First, the transaction process of the overall use case, keyless vehicle access control, is outlined, followed by diving into the implementation of the prototype comprising the development environment, deployment, and results. Finally, the implementation is evaluated based on our observations and gained knowledge from the literature review.

5.1. Transaction Process of Use Case

In the following, the selected use case between *Lessee Clien*t and *Short-term Renter Client* is described, disregarding, for now, the elaboration on the technical implementation of the interaction with the rented car. The transaction process starts after the rental request has been sent by the *Short-term Renter Client* and accepted by the *Lessee Client*. We outline in detail the use case chaincode functions activated by each entity involved and the subsequent events.

In the following setup, three classes are defined, namely *car*, *lessee,* and *short-term renter*. The class *car* defines the attributes related to each car registered in the blockchain network, of which we focus on only the relevant ones for our prototype shown in Table 6. In the same manner, the attributes of a *lessee* and *short-term renter* are defined where their IDs are used as a reference in the corresponding *car* object. Each object of the class *car* is used to track the rental history of the respective car. Hence, the focus lies on the changes made to this object and the corresponding updates to the ledger. Once the lessee orders a car, an object of the class *car* is created.

Attributes	Description
licenseID	License plate of the respective car (unique value)
lesseeID	Unique ID of the owner of the respective car; received from the respective *lessee* object
renterID	Unique ID of the renter for the booked time frame; received from the respective *short-term renter* object; default: empty
startTime	Start time of the accepted renting period; default: empty String
endTime	End time of the accepted renting period; default: empty String
carLocation	Location of the car at all times; values: longitude/latitude; default: empty array
status	Indicates in which phase the car resides; possible values: available, requested, located, unlocked, completed; default: available

Table 6: Overview of needed attributes of class car

The transaction process, shown in Figure 12, encompasses the transactions directly related to our use case. It is assumed that the status of the *car* object is first set to *available* after a confirmed listing (cf. 4b in Figure 9, p. 51) and then set to *requested* once the *Lessee Client Application* accepts the rental request. Consequently, the following described transaction process starts with the status *requested* and has the *rentalID* of the respected *Short-term Renter Client Application*. During the transaction process, the values of the attributes *status*, *startTime*, *endTime,* and *carLocation* will be continuously changed.

The following chaincode functions provide the core functionality of the proposed use case and will be called by the client application of the *Short-term Renter*. Subsequently, the created transaction is validated by endorsing peers. In addition, the *Lessee Client Application* receives continuous updates about the progress of the rental in the form of events. Conclusively, each chaincode function represents a transaction that is tracked in the ledger where the world state shows the current status, and the transaction log (i.e., blockchain) serves as a history log of the entire rental period.

Locate Car: Once the ride request is accepted, the short-term renter has to be able to locate the car through a client application and a certain time frame before the actual rent starts. Therefore, the client API triggers the *Locate Car* chaincode function to send a location request to the *Chaincode on Endorsing Peers*. Afterward, the *car* object is updated to include the location coordinates, *longitude* and *latitude*, in the attribute *location*. The *Short-term Renter Client*

Application receives access to the location coordinates, and the short-term renter is physically able to locate the car. The attribute *status* is changed from *requested* to *located*. Finally, this function triggers the *Locate Request Event,* which is automatically sent to the *Lessee Client Application*.

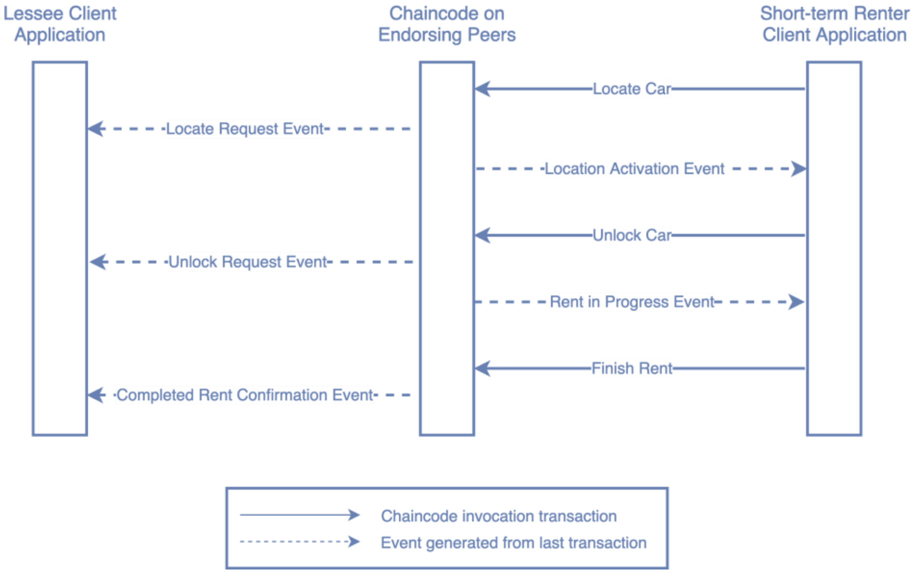

Lessee Client Application
Chaincode on Endorsing Peers
Short-term Renter Client Application
Locate Car
Locate Request Event
Location Activation Event
Unlock Car
Unlock Request Event
Rent in Progress Event
Finish Rent
Completed Rent Confirmation Event
Chaincode invocation transaction
Event generated from last transaction

Figure 12: Transaction flow of Keyless Vehicle Access Control

Unlock Car: When the short-term renter physically unlocks the car, this chaincode function is called. Then, the ledger is checked whether the respective short-term renter is allowed to open the car. If the endorsing peers approve the transaction, the short-term renter can physically access the car. The value of attribute *status* is changed to *unlocked,* and *startTime* is set to the time of the chaincode function activation. Finally, the *Opening Request Event* is sent to the *Lessee Client Application*.

Finish Rent: When the short-term renter physically ends the rental, this chaincode function is called. The attribute *status* is changed from *unlocked* to *completed*. The attribute *endTime* is updated to the time of the physical completion of the rental by the short-term renter. Conclusively, the chaincode function also creates the *Completed Rent Confirmation Event*.

Once the lessee was able to check the rental period data, he/she confirms the successful execution of the rental. The *renterID, startTime,* and *endTime* attribute values are set to its defaults in the world state.

5.2. Implementation of Prototype

In total, the described use case consists of five transactions, whereby we built a prototype for only one of them. In the course of this, we decided to simulate the unlocking of a car by having a **Raspberry Pi** (RPi) representing the server of the car, an **RFID sensor** as the car lock, and the **RFID tag** as the keyless option that would be in reality a smartphone application. Overall, our focus in this prototype has been to explore the interaction between an IoT device (RFID with RPi) and the **blockchain network (HF)**. Before the actual deployment of the prototype, the development environment for the IoT device and broker, as well as the IoT blockchain network of HF, are outlined. Then, the results of the submitted transaction are showcased, and finally, the implementation of the prototype is evaluated.

5.2.1. Development Environment

The prototype consists of two main hardware components, a Virtual Machine (VM) for the HF network and an RPi for the connection of the IoT device and broker. These two parts are described more in-depth in regard to technical specifications and decisions we made.

5.2.1.1. IoT Device & Broker

As the IoT device server, a Raspberry Pi3 Model B+ with ARM Cortex-A53 @ 1.4GHz processor and 1024 MB memory is used. The RPi is using the standard Raspbian operating system (version 10, Buster). The chosen programming language is Python 3.3.6 to read the data from the RFID sensor and handle the communication with MQTT. The RFID sensor is connected to the RPi by using a breadboard (GPIO Extension) and jumper wires (cf. Appendix 1, p. 120). The SimpleMFRC522 library is used to read the data coming from the RFID sensor on the RPi. Simulating a smartphone, we use an RFID tag (Mifare S50 non-standard), which is held against the sensor (cf. Figure 13). An overview of the technical specifications for the IoT device is depicted in Table 7.

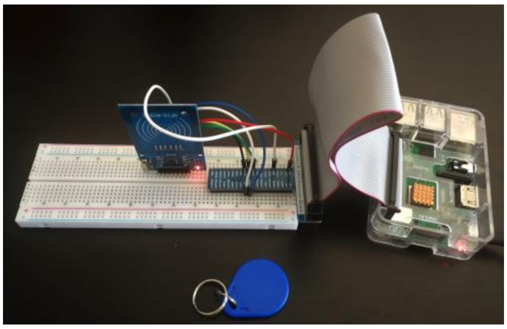
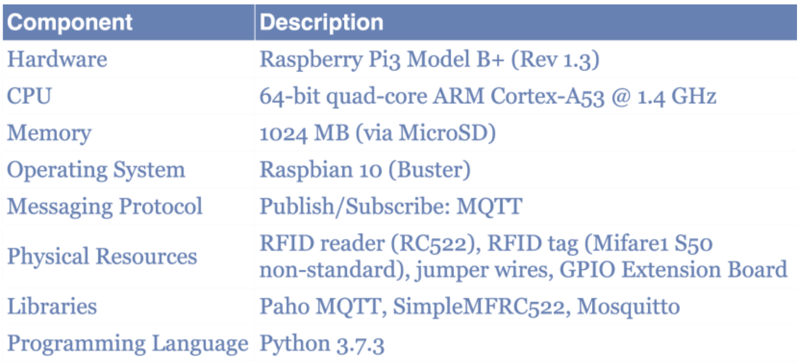


Figure 13: IoT Device Setup

To facilitate the communication between the IoT device server and the HF node, we make use of the before-mentioned messaging protocol MQTT. Due to the sake of simplicity, we decided to use the same RPi as both the publishing client and the MQTT broker instead of shifting the broker into a cloud service like HiveMQ. This decision will be further assessed in the chapter 5.3 Technical Evaluation of Prototype. In summary, the libraries Paho MQTT for the client and Mosquitto for the broker are used.



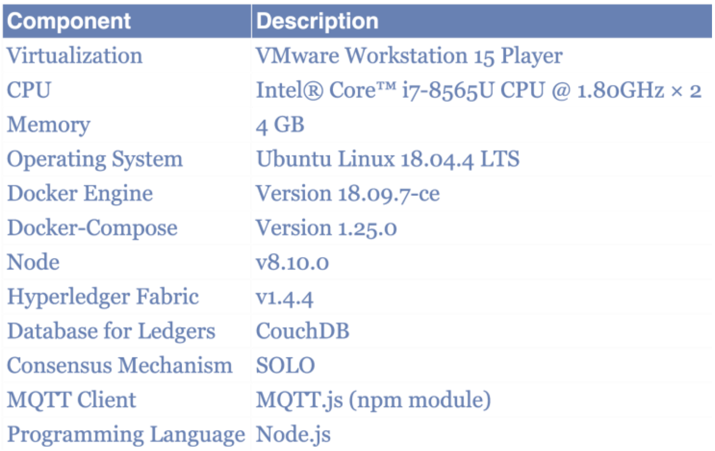
Component	Description
Hardware	Raspberry Pi3 Model B+ (Rev 1.3)
CPU	64-bit quad-core ARM Cortex-A53 @ 1.4 GHz
Memory	1024 MB (via MicroSD)
Operating System	Raspbian 10 (Buster)
Messaging Protocol	Publish/Subscribe: MQTT
Physical Resources	RFID reader (RC522), RFID tag (Mifare1 S50 non-standard), jumper wires, GPIO Extension Board
Libraries	Paho MQTT, SimpleMFRC522, Mosquitto
Programming Language	Python 3.7.3

Table 7: Development Environment for the Raspberry Pi-based IoT server

5.2.1.2. IoT Blockchain Network - Hyperledger Fabric

To implement the HF application, we have deployed the HF network only on one VM by VMware with operating system Ubuntu Linux 18.04.4 LTS with 4 GB memory and Intel® Core™ i7-8565U CPU @ 1.80GHz × 2 processor. We decided on keeping it simple and concentrating on the deployment of an application-specific smart contract instead of having an over-complex network with an actual distribution over several VMs (nodes). An overview of the technical specifications for the implementation of the IoT blockchain network in docker environment is shown in Table 8.

As the services of HF run in docker containers (cf. Docker images of nodes in Table 9, p. 63), the docker engine (version 18.09.7) is installed, which provides a docker running environment, and docker-compose (version 1.25.0), which serves as the integrated development environment to configure docker images and containers in the VM. While newer versions of HF (v14.5, v1.4.6 & v2.0) have been released in February, we decide to use HF v1.4.4 to ensure a stable version. We make use of the Node.js SDK provided by HF for both the chaincodes and applications due to our previous experience in Javascript. In this regard, we installed Node.js (v8.10.0) with NPM (version 3.5.2). To deploy an MQTT subscribing client on the HF node receiving the data from the IoT device, the MQTT.js npm module is installed.



Component	Description
Virtualization	VMware Workstation 15 Player
CPU	Intel® Core™ i7-8565U CPU @ 1.80GHz × 2
Memory	4 GB
Operating System	Ubuntu Linux 18.04.4 LTS
Docker Engine	Version 18.09.7-ce
Docker-Compose	Version 1.25.0
Node	v8.10.0
Hyperledger Fabric	v1.4.4
Database for Ledgers	CouchDB
Consensus Mechanism	SOLO
MQTT Client	MQTT.js (npm module)
Programming Language	Node.js

Table 8: Development Environment for IoT Blockchain Network

As another part of the development environment, the infrastructure of the used *First Network* is described and depicted in Figure 14. In the remaining part of this development environment and deployment of the prototype section, we refer to the official HF Documentation release-1.4 when explaining the HF network, transactions, and alike (Hyperledger, 2019). The *First Network* is not modified as we focus on the development of smart contracts and the interaction between the HF network and the IoT device. HF's pre-built docker images and the described infrastructure in Figure 14 are running as containers in the Docker runtime environment.

The namespace of the *First Network* is *example.com* initiated by the *orderer*. Three **organizations** and their namespaces originate from the respective namespace.

- Organization: orderer, example.com
- Organization 1 (e.g., an OEM): org1, org1.example.com
- Organization 2 (e.g., Leasing Corp): org2, org2.example.com

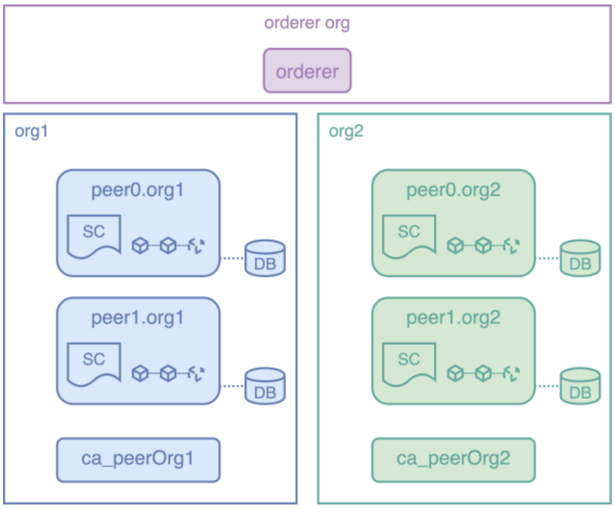
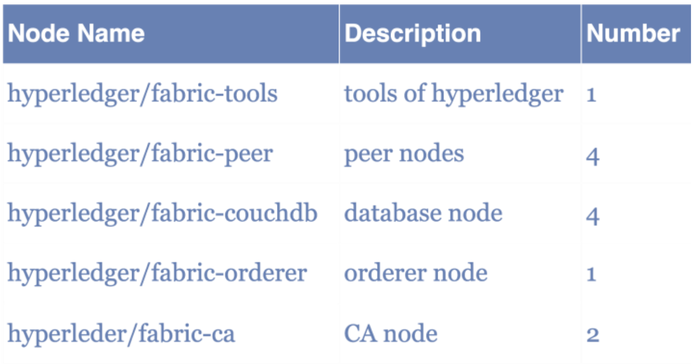


Figure 14: Infrastructure setup of First Network

At the node level, one node is allocated to the *orderer*. *org1* and *org2* each have two peer nodes (*peer0* and *peer1*) initialized, resulting in a total of the first five nodes running in separate containers on a host (cf. Docker images of nodes in Table 9). *org1* and *org2* each have a **Certificate Authority** assigned to them, which runs a *fabric-ca* software with the correct configurations. This configuration generates its own signing key and corresponding certificate for each node.



Node Name	Description	Number
hyperledger/fabric-tools	tools of hyperledger	1
hyperledger/fabric-peer	peer nodes	4
hyperledger/fabric-couchdb	database node	4
hyperledger/fabric-orderer	orderer node	1
hyperleder/fabric-ca	CA node	2

Table 9: Docker images of nodes

The **channel** *mychannel* is created by the *orderer* and the peers can join the channel once it is running. The channel creation includes the initialization of *genesis block* for the channel ledger which stores configuration information about the channel policies, members, and anchor peers.

The default **ordering service** *Solo* is deployed on the *orderer* node. On each peer node, the default **database**, *CouchDB*, is installed, representing the world state database. The implementation choices made concerning the ordering service and database will be assessed in 5.3 Technical Evaluation of Prototype.

5.2.2. Deployment of Prototype

In this section, we are diving into the actual deployment of the prototype outlining the entire workflow shown in Figure 15, whereby we refer to the respective step by indicating the number in blue. To see the full deployment in action, a demo video of the prototype can be watched here and is also attached to this thesis.

After setting up the previously described HF network, the keyless vehicle access control **application** is ready to be **deployed** based on the FabCar sample provided by HF (0). In general, HF client applications can interact with the blockchain network by submitting transactions to a ledger or querying ledger content. In particular, a user of the application can invoke a smart contract which queries and updates the ledger through the smart contract API (e.g., *getNetwork()*, *getContract()*, *evaluateTransaction()*, *submitTransaction()* functions).

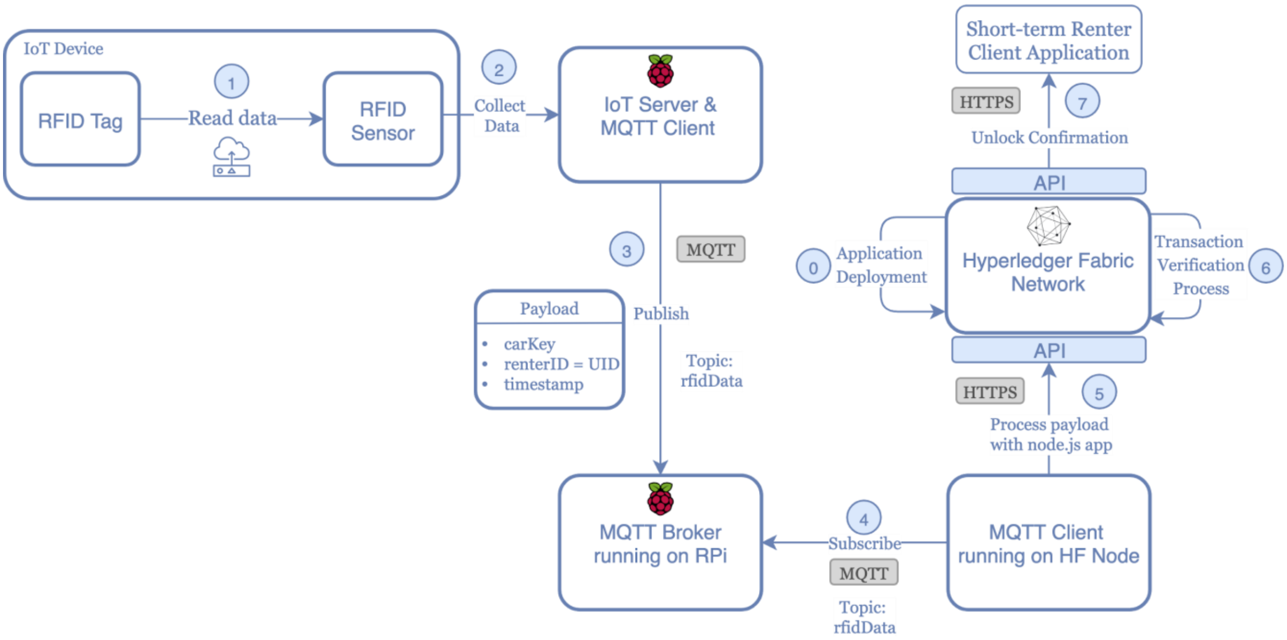


Figure 15: Workflow of transaction deployment

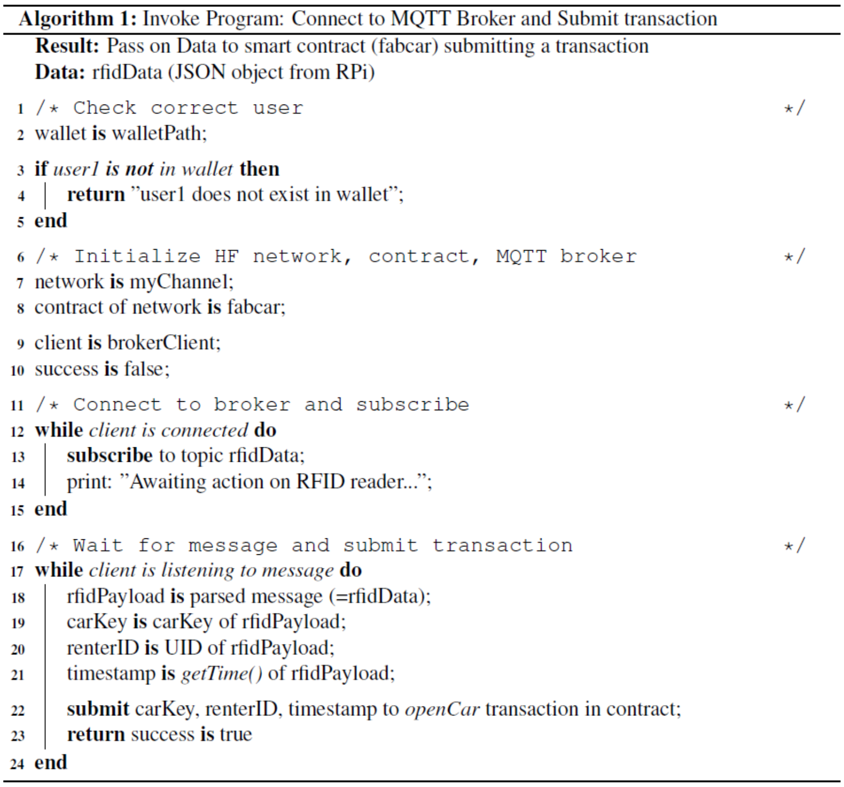
Consequently, the first step of deploying the application is to **initiate the smart contract** (i.e., chaincode) on each peer node and the shared channel of both organizations. By doing so, the *initLedger()* transaction is executed, which preloads sets of car data into the ledger (cf. Table 6, p. 58, & Appendix 2, p. 120). In this way, we could ensure that at least one car object has its status set to *located* to test the prototype. To later query the car data and change specific car objects, each of the cars receives a key value from *CAR0* to *CARN* (*carKey)*. In addition, the smart contract consists mainly of two other transactions (*queryCar* and *openCar*), which will be explained at the point of actual execution.

As the next step, a certificate and a public-private key pair are generated together with the CA so that the respective user can interact with the permissioned blockchain. Assuming the application dependencies of FabCar have been installed, we are creating identities for two users of the application, namely *admin* and *user1*. The *admin*, who has already been created during the deployment, is the registrar for the CA. *User1* representing our *Short-term Renter Client Application* is used to query and update the ledger. In the course of this, the programs *enrollAdmin.js* and *registerUser.js* are run to create a wallet with the respective certificate and keys for each user.

Now that the application is deployed on the blockchain network (0), the actual interaction with the ledger can start by submitting a transaction. In a nutshell, the aim is to send a packaged

JSON[13] object generated by the RFID sensor (reader) to the HF network, followed by submitting and verifying a transaction.

As mentioned in the development environment, an MQTT client is installed on both the RPi and the HF Node, whereby the RPi as the IoT server publishes the data to a topic called *rfidData* (3) and the HF Node subscribes to the same topic (4). Besides, the same RPi serves as the MQTT broker as the bridge between these two clients. Since the subscribing client has to start listening to a message before the publishing client can send data, as a next step, we run the *invoke* program in the HF network, which is demonstrated as pseudocode in Figure 16 and as implementable code in Appendix 3 on page 120. Besides the incorporated MQTT client, the *invoke* program also contains the later explained *submitTransaction* API. Once *invoke* is run, the client connects to the broker on the RPi and **subscribes** to the topic *rfidData* listening to an incoming message (4). So far, there is only action in regard to the MQTT client, but the transaction process (6) has not been triggered yet.



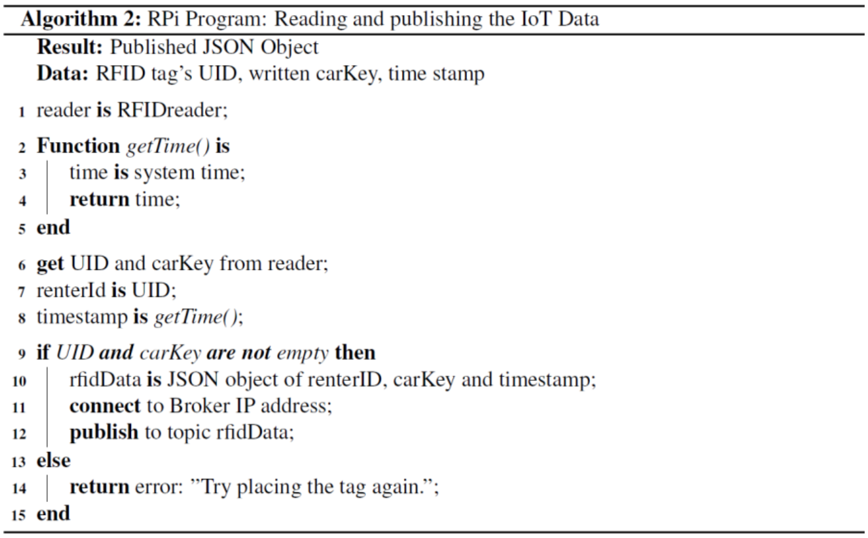
```
Algorithm 1: Invoke Program: Connect to MQTT Broker and Submit transaction
  Result: Pass on Data to smart contract (fabcar) submitting a transaction
  Data: rfidData (JSON object from RPi)
/* Check correct user                                          */
wallet is walletPath;
if user1 is not in wallet then
    return "user1 does not exist in wallet";
end
/* Initialize HF network, contract, MQTT broker                */
network is myChannel;
contract of network is fabcar;
client is brokerClient;
success is false;
/* Connect to broker and subscribe                             */
while client is connected do
    subscribe to topic rfidData;
    print: "Awaiting action on RFID reader...";
end
/* Wait for message and submit transaction                     */
while client is listening to message do
    rfidPayload is parsed message (=rfidData);
    carKey is carKey of rfidPayload;
    renterID is UID of rfidPayload;
    timestamp is getTime() of rfidPayload;
    submit carKey, renterID, timestamp to openCar transaction in contract;
    return success is true
end
```

Figure 16: Pseudocode of Invoke Node.js Program

Starting with the actual IoT data transmission, we can now turn to the RPi, which represents a car. As the RFID tag represents a mobile app, a user would type in its *renterID* and the reservation

[13] JavaScript Object Notation (JSON) is an open standard file and data interchange format that is lightweight for storing and transporting data (JSON, 2020).

confirmation number representing the *carKey*. In our prototype, the *carKey CAR1* is written on the RFID tag with a simple *write* script using the *SimpleMFRC522* library (cf. Appendix 2, p. 120). Additionally, every RFID tag has a unique ID (UID) that can be read with the RFID sensor. As a next step, another python script is run that **collects the data** from the RFID sensor (2) **reading** the UID and the written *carKey* from the RFID tag (1). The UID corresponds with the *renterID* stored in *CAR1*. In addition, a timestamp is generated from the current system time. These three values (*carKey*, *renterID*, and *timestamp*) are packaged as a JSON object and **published** to the MQTT broker (3), which is demonstrated as pseudocode in Figure 17 and implementable code in Appendix 4 on page 121.



```
Algorithm 2: RPi Program: Reading and publishing the IoT Data
  Result: Published JSON Object
  Data: RFID tag's UID, written carKey, time stamp
  reader is RFIDreader;
  Function getTime() is
      time is system time;
      return time;
  end
  get UID and carKey from reader;
  renterId is UID;
  timestamp is getTime();
  if UID and carKey are not empty then
      rfidData is JSON object of renterID, carKey and timestamp;
      connect to Broker IP address;
      publish to topic rfidData;
  else
      return error: "Try placing the tag again.";
  end
```

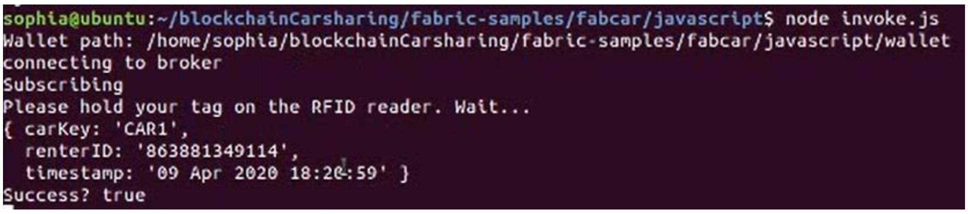
Figure 17: Pseudocode of Reading and Publishing Program on RPi

Back in the HF network, the published payload with the JSON object arrived and has been used in the *invoke.js* to **trigger the chaincode** function *openCar* by using the *submitTransaction* API (5). In this way, the received values *carKey*, *renterID,* and *timestamp* are passed on to the *openCar* transaction function, which is demonstrated as pseudocode in Figure 18 and implementable code in Appendix 5 on page 121. The *openCar* function mainly checks whether the sent renterID corresponds with the one stored in the ledger, sets an event *TransferConfirmed,* and sets the *status* of the car object (*carKey=CAR1)* to *unlocked* and *startTime* to the *timestamp*. The set event can be used in further development to trigger a new message published back to the RPi to actuate a LED or sound simulating the physical opening of a car door. Eventually, the ledger is updated accordingly.

```
Algorithm 3: Transaction function openCar: Update state in ledger
  Result: Changed world state in ledger and set event (TransferConfirmed)
  Data: rfidData submitted through invoke program
Function openCar(carKey, renterID, timeStamp) is
    /* Check validity of carKey                                        */
    get car object from worldState based on submitted carKey;
    if carKey is not in worldState then
        return error: "carKey does not exist";
    end
    /* Error checks                                                    */
    car is parsed car object;
    if renterID of car is not renterID then
        return error: "No match. Please request a car first.";
    end
    if status of car is "unlocked" then
        return error: "Car is already unlocked.";
    end
    /* Actual update of car object only if car is located              */
    if status of car is "located" then
        status of car is "unlocked";
        startTime of car is timeStamp;
        set Event to TransferConfirmed;
        update state of carKey in ledger;
    end
end
```

Figure 18: Pseudocode of our main transaction function openCar()

In a nutshell, the application submits the particular transaction to the blockchain network. Once it has been validated and committed (6), the application receives a **notification** that the transaction has been successful (7), shown as screenshot in Figure 19.



```
sophia@ubuntu:~/blockchainCarsharing/fabric-samples/fabcar/javascript$ node invoke.js
Wallet path: /home/sophia/blockchainCarsharing/fabric-samples/fabcar/javascript/wallet
connecting to broker
Subscribing
Please hold your tag on the RFID reader. Wait...
{ carKey: 'CAR1',
  renterID: '863881349114',
  timestamp: '09 Apr 2020 18:20:59' }
Success? true
```

Figure 19: Received JSON object and success notification

More in detail, the corresponding **transaction verification process** (6) that is triggered by *submitTransaction* is explained in the following.

In our network, *peer0.org1* and *peer0.org2* are the only endorsing peers who are shown in Figure 20. The initialization of the smart contract on every peer node supplies the endorsement policy of the transactions. The endorsement policy includes the description which organizations are needed to give their approval for a transaction before other organizations can accept them onto their copy of the ledger. Only after the installation of a chaincode on the peer nodes and the initialization on the channel (*mychannel*), the smart contract can be invoked by the client API (*submitTransaction*).

As shown in Figure 20, the transaction verification process proceeds as followed, whereby for the sake of simplicity, we only illustrate one peer per organization, but this process applies to the other peers as well. The respective numbers marked in grey are referring to the steps in the figure. The client application sends a **transaction proposal** to the defined endorsing peers (1) that is signed with the user's (*user1*) certificate by using the *submitTransaction* API. The received transaction proposal serves as input for the transaction *openCar*.

The endorsing peers verify the identity of the user and the corresponding authorization from the proposal payload. Then the endorsing peers **simulate the transaction** (*openCar*) and generate an endorsed transaction response. The endorsement is facilitated by signing the transaction response with the peer's certificate (2).

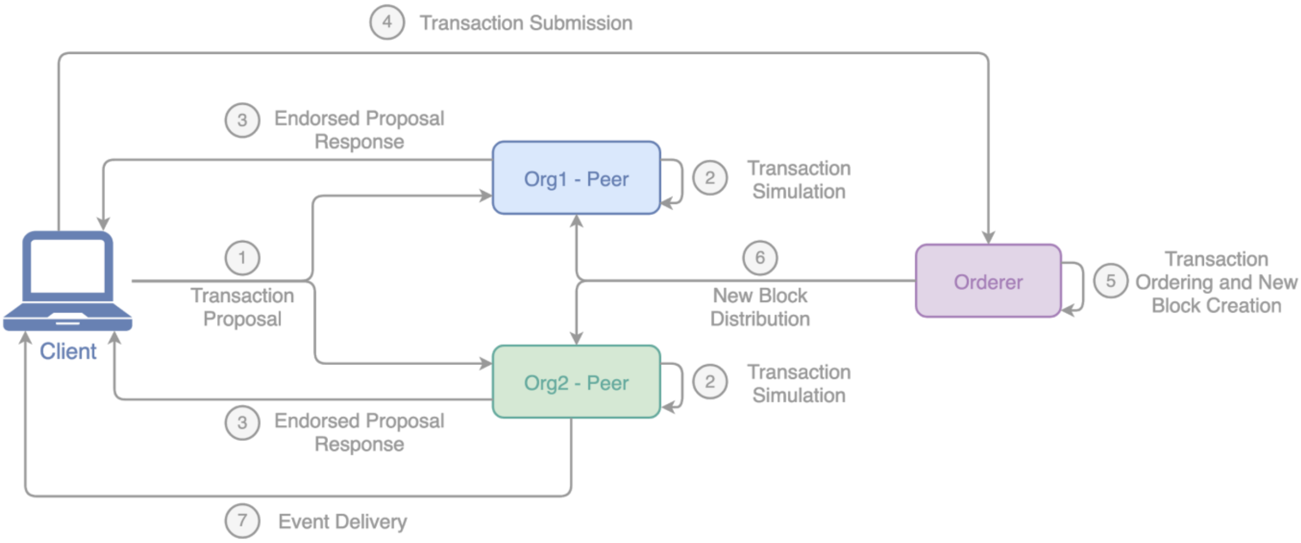


Figure 20: Schematic visualization of transaction verification process

The peer node then returns this endorsed transaction response to the client application, which automatically checks the accumulated **endorsed proposal responses** (3). The **transaction**, including the endorsed proposal responses, are **sent** to the *Orderer* (*order.example.com*) by the client (4). The Orderer receives and **sequences** the transactions into a block of transactions. The block is **signed** with the *Orderer*'s certificate (5). The new **block** is **distributed** to all peers on *mychannel*. Each peer (both endorsing and committing) has to ensure that the transaction in the received block was signed by the appropriate endorsing peers and compares the transaction with its ledger's world state. After this verification, the transaction is marked as valid, and each peer's world state is updated, and the **block** is **appended** into each peer's local blockchain (6). The client application receives the **notification** of the **successful transaction** (7).

After the transaction has been validated, a block is added to the blockchain, and the world state is updated. The updated world state can be checked by calling the *query.js* program that uses a read-only invocation of a smart contract employing the API to interact with the network to see the most recent data from the ledger. Compared to the sophisticated *submitTransaction* API of *openCar* that involves the whole network and updates the ledger, the *queryCar* transaction called by *query.js* is a bare evaluation of a transaction where the ledger is not updated. The results of this submitted transaction are outlined more in detail in the next chapter.

5.2.3. Results

After a verified transaction, the result can be inspected in both the **world state** by querying the current state and the newly added block. To identify the changes after the submission of a transaction, the CAR1 is queried (the specific leased car that is referred to in our prototype) before and after the submission of the transaction (i.e., located vs. unlocked car). As shown in Table 10, the light blue highlighted changes occurred where the empty *startTime* is replaced with the time stamp received from the RPi, and the status is changed from *located* to *unlocked*.

	Before Submitted Transaction	After Submitted Transaction
Query of CAR1	{"docType": car, "licenseID": 123a", "lesseeID": "456a", "renterID": "863881349114", "startTime": "", "endTime": "", "carLocation": ["55.6761","12.5683], "status": "located"}	{"docType": car, "licenseID": 123a", "lesseeID": "456a", "renterID": "863881349114", "startTime": "11 Apr 2020 09:33:37", "endTime": "", "carLocation": ["55.6761","12.5683], "status": "unlocked"}
Blockchain Info	**Block 4:** {"height": 5, "currentBlockHash": “5b83ekkxlFWY4hPevxu1UeWW3AkuGtC8Wr4HVzDnFfE=" "previousBlockHash": "zbO1gojMGkCk662Ue+3P7g9GSyEkBzmRIRpqrzeXzuw="}	**Block 5:** {"height": 6, "currentBlockHash": "CwAJAIOL9mVrCzej+Zl7kbFxz36hemY8FA+jRM24Lew=" "previousBlockHash": "5b83ekkxlFWY4hPevxu1UeWW3AkuGtC8Wr4HVzDnFfE="}

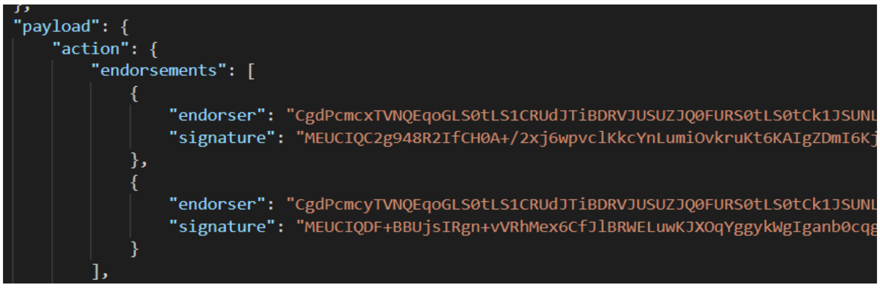
Table 10: Output of query and blockchain info before and after the submitted transaction

Besides the updated world state, we can look at the specific block created. As a first comparison, we checked the blockchain info before and after the submitted transaction. As seen in Table 10, the **height** of the blockchain **changed** from five to six. The already higher number of the initial blockchain means that all the setup activities in regard to the network and the application (e.g., joining the channel, initiating smart contracts) are already immutably tracked in the blockchain. With the changed height to six, we see that our submitted transaction has resulted in a newly added block. In this regard, the hash of Block 4 is added as *previousBlockHash* in Block 5.

Diving even deeper into the blockchain, the most recently added block 5 is inspected by fetching it from one of the peer node docker images and converting it to a readable JSON file (cf. Figure

21 & 22). There are two main details in the block that are of particular relevance, while most of the information is encrypted anyways.

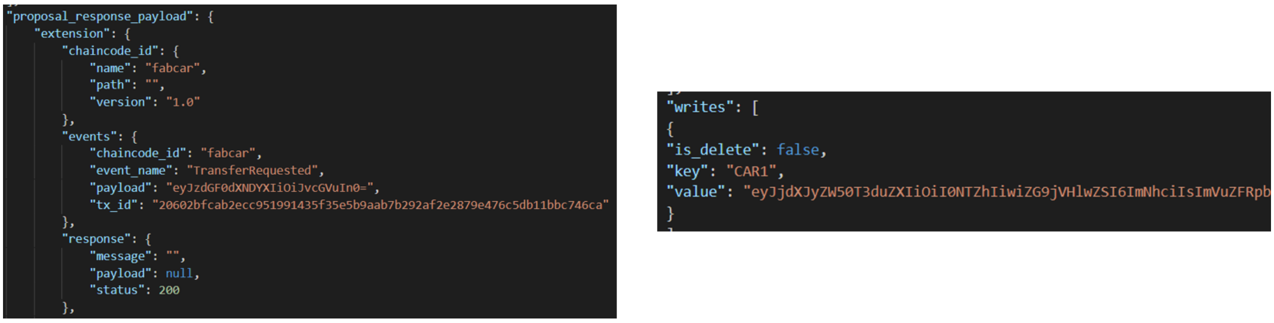
First, the block confirms that the submitted transaction is **endorsed** by two peers (the endorsing peers) and **signed** with their respective keys, which are not the same (cf. Figure 21).



```
"payload": {
    "action": {
        "endorsements": [
            {
                "endorser": "CgdPcmcxTVNQEqoGLS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNL
                "signature": "MEUCIQC2g948R2IfCH0A+/2xj6wpvclKkcYnLumiOvkruKt6KAIgZDmI6Kj
            },
            {
                "endorser": "CgdPcmcyTVNQEqoGLS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNL
                "signature": "MEUCIQDF+BBUjsIRgn+vVRhMex6CfJ1BRWELuwKJXOqYggykWgIganb0cqg
            }
        ],
```

Figure 21: Snippet of the block in regard to endorsement

Second, the proposal response payload contains the information about the **set event** *TransferRequested* mentioned before, as seen in the left image of Figure 22and the write request on the ledger for the key *CAR1* with the respective encrypted value, which is visible in the right image of Figure 22.



```
"proposal_response_payload": {
    "extension": {
        "chaincode_id": {
            "name": "fabcar",
            "path": "",
            "version": "1.0"
        },
        "events": {
            "chaincode_id": "fabcar",
            "event_name": "TransferRequested",
            "payload": "eyJzdGF0dXNDYXIiOiJvcGVuIn0=",
            "tx_id": "20602bfcab2ecc951991435f35e5b9aab7b292af2e2879e476c5db11bbc746ca"
        },
        "response": {
            "message": "",
            "payload": null,
            "status": 200
        },
```

```
"writes": [
{
"is_delete": false,
"key": "CAR1",
"value": "eyJjdXJyZW50T3duZXIiOiI0NTZhIiwiZG9jVHlwZSI6ImNhciIsImVuZFRpb
}
```

Figure 22: Snippets of the block in regard to event submission & ledger update

5.3. Technical Evaluation of Prototype

While successfully implementing a demonstration of one transaction, there are some considerations to evaluate, limitations to outline, and possible improvements to suggest for further development of our prototype. Overall, by taking into consideration the proposed IoT Blockchain architecture in the implementation of the prototype, we can confirm that the architecture is working as such. The technical evaluation of the prototype is conducted along with the four domains of the proposed architecture, IoT Physical, Connectivity, IoT Blockchain Service and Application Domain, forming the structure of this chapter. In addition, the fulfillment of the key design principles, security & privacy, authenticity, traceability & reliability, scalability, and interoperability, is assessed (the referred principle is highlighted in bold).

5.3.1. IoT Physical Domain

As mentioned before, using the RPi as an IoT server, the RFID sensor as car lock and MQTT as the messaging protocol have been solid choices for the implementation of our prototype.

Due to the provided interoperability between RPi and the given RFID sensor through detailed documentation and the ease of use, we believe there would not have been a better alternative to use as an IoT device for the use case. Of course, the market of various IoT devices is enormous, and concerning the performance, other devices should be tested as well. Regardless, for rapid prototyping, an RPi with its decent support system and available sensors is one of the best embedded systems to use. In contrast, the authenticity of accessing the IoT device could be improved by replacing the RFID with an NFC[14] sensor and the RFID tag with a mobile app. In this way, the users need to authenticate themselves by actually using their private keys instead of the pre-defined ID of the RFID tag. Indeed, the private key of the user is applied once the transaction is submitted in the HF network. Nevertheless, an improved **authenticity** already within the *IoT Physical Domain* may be advisable. While one RPi as an IoT server representing one car helped to prove our idea of using IoT and blockchain for keyless vehicle access control, it does not really reflect an appropriate IoT network with usually thousands of devices. Consequently, it is essential to test the prototype with at least three RPis to get an insight into the complexity of various permissions as well as be able to evaluate to which extent the prototype can meet **scalability**.

[14] Near Field Communication (NFC) is “a standards-based short-range wireless connectivity technology that makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch”(Pierre, 2019).

Finally, to truly complete the “unlock car” transaction, an actuator would be necessary to show the entire workflow from sending data into the blockchain but also back to the IoT device to trigger an action such as a LED lamp or sound. However, we decided against its implementation as our primary objective lies in the overall understanding, and we saw it as more important to complement the technical with a business evaluation through expert interviews.

5.3.2. Connectivity Domain

The chosen messaging protocol, MQTT, has been rewarding as its publish/subscribe model is secure and easy to understand as well as there are various libraries provided with solid documentation for all different programming languages. In fact, at DriveNow, MQTT is the go-to messaging protocol to handle an enormous fleet of cars, but it is using a scalable MQTT broker (HiveMQ) (Happ, Karowski, Menzel, Handziski, & Wolisz, 2017). Consequently, it is crucial to develop our prototype further by testing the interconnection with a broker that is placed outside of the RPi to enable better monitoring, coordination, and concluding scalability. By using a sophisticated MQTT broker such as HiveMQ, it is possible to monitor and analyze the incoming data stream taking into consideration a possible filtering which data goes on- and which off-chain (i.e., blockchain storage or not). As another alternative, IBM Watson IoT with IBM Blockchain (built on HF) using Bluemix cloud service should be tested. In this way, IoT devices could send data to the blockchain through the IBM Watson IoT Platform, which manages devices and allows data analysis and filtering. IBM’s Bluemix platform facilitates the integration of blockchain technology by offering it as a service. The use of this platform could speed up the application prototyping and help to reach **scalability** (Reyna et al., 2018). However, we aim to understand the raw development without an added abstraction layer. Therefore, we decided to neglect working with IBM’s offered platforms to truly comprehend the network setup and API logic within HF.

Moreover, the optimal interaction between yet another central third-party cloud-based platform (IBM platforms) and the blockchain needs to be evaluated in regard to contradicting **security** and **privacy**. In the same manner, it is also crucial to add encryption to the IoT network and application layer by using a secure SSL/TLS network connection and encrypting the payload before publishing it to the broker. Since our implementation represents just a prototype, we decided to not over-complicate the implementation, intentionally omitting to add encryption. Nevertheless, MQTT offers various implementation options in this regard that are not tremendously complex to accomplish.

In general, by using HF as a regular MQTT client, the integration of HF into a usual IoT architecture turned out to be feasible. Nevertheless, combining the event-driven programming of MQTT with the object-oriented programming of HF was a challenge for us with our limited background knowledge in regard to asynchronous programming, which is used in HF and could be better integrated with MQTT.

5.3.3. IoT Blockchain Service Domain

Keeping in mind our goal to understand the technical implementation of a blockchain application, we noticed that the setup of a blockchain network from scratch is resource and development intensive. Additionally, being entirely new to the technical implementation of blockchain and developing smart contracts, we realized that building a blockchain application for the use case requires extensive knowledge in computer science, network structures, and overall blockchain technology. This led us to the decision to use the *First Network* sample provided by HF. Nevertheless, we analyzed in-depth the network setup to extend our understanding of the different entities involved, e.g., ordering service, and to be able to assess the setup critically. The used network is suitable for our use case, but for further analysis and development, certain adaptations have to be made. First, more stakeholders, e.g., OEM, leasing, and insurance companies, and hence the definition of more organizations need to be involved in the network. Second, we only set up two peers per organization. In a more sophisticated network reaching a higher degree of distribution, more peers should be added, and a more definite distinction between committing and endorsing peers is required. Furthermore, to test the **security** of the blockchain network with performance tests, the network setup would have to include several physical nodes. This can be facilitated by implementing several VMs leading to the actual distribution of the network.

As another evaluation aspect concerning the **security and privacy** of the network setup, the chosen consensus mechanism has to be assessed. HF provides the described ordering services Solo, Kafka, and Raft. For the implementation, we decided to use the default ordering service, Solo, as it is suitable for development and proof of concept networks. Furthermore, Solo uses a single ordering node, which leads to minimal administrative overhead concerning the maintenance and upgrade of multiple nodes and clusters. However, the Solo ordering service is not CFT, hence for a production blockchain network, the ordering service Raft should be implemented and tested. Additionally, Raft should be preferred as it is easier to set up and manage than the Kafka-based ordering services. The implementation of Raft also enables a distributed ordering service as the design allows different organizations to contribute nodes and is expected to be further developed toward BFT (Hyperledger, 2019).

To facilitate the key design principle **traceability**, we decided to use the database CouchDB as the physical implementation of the world state providing efficient access to the current data about all assets in the network. CouchDB is argued to be a suitable option in production based on the support of several features such as JSON querying operations, database indexing, and replication. The default database LevelDB, on the other hand, only supports limited operations. Thus, the usage of CouchDB is recommended for further development of the prototype. The pluggable aspect of the implemented database enables high flexibility in accessing the ledger states. This enhances the **interoperability** as HF enables suitability to different types of problems as the database can be a relational data store, a graph store, or a temporal database that should be tested in further development (Hyperledger, 2019). After all, the implementation of the prototype showed that it is possible to execute the *keyless vehicle access control* transaction within a blockchain network, and the traceability of the transaction can be facilitated.

5.3.4. Application Domain

The application sample *FabCar* supported our prototype by relying on existing API structure and sample code, which saved us a significant amount of time. It is fairly relatable to the use case transaction besides providing a useful script that initializes the *First Network*, channel creation, and smart contract as well as existing Node.js programs that enroll the admin, create a user, query the world state and invoke a smart contract.

In general, we only set up two users for the application, while one of them is an admin being of a register than an actual user. In this way, we mainly focused on the short-term renter as *user1* who triggers the smart contracts by unlocking the door. The lessee is not implemented since, in our use case, he/she would solely receive event notifications tracking the rental period (cf. Figure 12, p. 59). In addition, we have registered the *admin* and *user1* on the same VM for the sake of simplicity and quick testing, but in reality, they would need to be registered on two different VMs. As a result, this limitation leads to a lack of **scalability** and **authenticity**. To test the scalability of our application in the future, it is essential to add more users, make use of actual private data with the help of JSON collection definitions as well as try out with different permissions going deeper into identity management in HF (Hyperledger, 2019). Nevertheless, getting a first insight to the enrollment and registration process of users in an application and the usage of wallets to trigger smart contracts, is of great value supporting us to evaluate the **authenticity** more in-depth in combination with our interviews in the next chapter.

The blockchain setup and its block structure of HF enable the **traceability** of the use case transaction as the blocks are immutable and ordered based on the block hashes. We can confirm the ordered hashing of the transaction but did not test it by, e.g., manipulating a block. Further development of the prototype should, in general, include a detailed security test of the blockchain application.

Moreover, with the prototype, we are not able to evaluate how we meet the **interoperability** of our overall artifact. To test this design principle, a way more extensive prototype is required and active iterative cycles together with an OEM. As this is out of scope for the implementation of the prototype, we will evaluate these design principles in the business evaluation by incorporating the input from our interviews.

Finally, the implemented application makes it challenging to evaluate the **scalability** as only one out of five stakeholders is involved utilizing a simplified network without real distribution on several VMs besides using only one RPi representing one car and the same RPi as our MQTT broker. Consequently, this restricts the generalizability of our experience to other transactions and use cases. Nevertheless, our initial aim is met by providing a comprehensible demonstration for a broad audience and gaining a proper understanding of the technical side of blockchain to draw an actual informed conclusion about the applicability of blockchain-based on experience and not just research.

6. Business Evaluation of Artifact

Since we aim to evaluate both the technical and business implication of the prototype and overall designed artifact, the business perspectives incorporating the **qualitative data collection** is evaluated next. As mentioned in the Research Methodology, we have conducted five expert interviews that give us insights to the feasibility of the artifact based on the evaluation of the key design principles, the relevance of the prototype as well as a general assessment of car sharing and blockchain in mobility. In this way, we can eventually discuss the designed artifact not only based on theoretical deduction (literature review) and technical feasibility (prototype) but also practical, **real-world insights**.

First, car sharing as a business model, including its potential from different perspectives and its processes with leasing are evaluated. Next, the five key design principles, security & privacy, authenticity, traceability & reliability, interoperability, and scalability, are assessed, and learnings for the artifact are derived. To give a short overview, we conducted interviews with Zuehlke (New Business Models & Technology researcher at VW), Ottensten (Product Designer & Head of Keyless Product at GoMore), Busch (Product Owner DLT Mobility at Bosch), Pietsch (Manager Product Strategy Mobility Services at BMW), and Mortensen (Smart City & Digitalization at Frederiksberg Kommune) (cf. more in detail in 2.4.6.3 Ex Post: Qualitative Data Collection).

6.1. Car Sharing as a Business Model

While identifying already in the literature review the need for car sharing, its various business models and objectives, we aim to evaluate its potential and processes together with leasing. In this way, this section seeks to validate the need and problem for the designed artifact.

From the viewpoint of OEMs BMW & VW, investing in car sharing is essential to reduce the carbon footprint within cities, setting an example as big cooperation, as well as to learn from new business models and respond to the transformation of the automotive industry (Y. Zuehlke, personal communication, March 06, 2020; D. Pietsch, personal communication, March 20, 2020). In general, Zuehlke believes that there is a need to reduce the mass of cars on the streets. It is time to give back the city to the citizens, freeing up parking space and streets to create green zones and other infrastructure, enhancing the life of the citizens. Whether car sharing is the model that will support that **transformation** is debatable, but VW and other OEMs need to lead the way and start learning (Y. Zuehlke, personal communication, March 06, 2020). The same is confirmed by Pietsch claiming that roughly ten cars could be replaced by one car sharing vehicle.

It can be concluded that within the broader category, shared mobility, the investment in car sharing makes naturally sense as OEMs possess the needed resources and knowledge in regard to vehicles. Nevertheless, VW is also investing in other modalities such as ridesharing and general Mobility as a Service (MaaS) with its service MOIA[15]. Overall, the low switching costs of most shared mobility modes from ride-hailing to car sharing is a remaining issue as the user usually wants to get from A to B without concern of the particular service that executes such trips (Y. Zuehlke, personal communication, March 06, 2020).

In regard to the target market, Pietsch thinks that car sharing is especially demanded by the younger generation, where many already do not own a car and most likely reject a car purchase, leading to the focus of BMW's car sharing service ShareNow on this target group. He points out that car sharing is a **challenging concept** as it is a regional business that requires more resources due to its closer contact with the customer compared to the early decoupling when selling a vehicle to a dealer. In combination with the high investment costs in providing and maintaining a fleet and the challenging regulations, this currently results in just moderate profitability of car sharing (D. Pietsch, personal communication, March 20, 2020). As Pietsch notes, how exactly car sharing will evolve in regard to scalability and profitability is yet to be figured out. Nevertheless, as Zuehlke highlights, car sharing is already serving as a strategic medium for promoting VW's Electrical Vehicles with WeShare car sharing service (personal communication, March 06, 2020). Besides, it is crucial to start investing now as Pietch expects that car sharing as a business model will become especially interesting once Autonomous Vehicles (AVs) are roadworthy, opening up a broader market (personal communication, March 20, 2020).

After all, it can be concluded that the investment efforts of OEMs into car sharing entails more **strategic** than financial intentions. In addition, Zuehlke believes that in the future, it is especially attractive to build a platform (i.e., "platformization") around any service, be it car sharing or other mobility services, to ensure regular traction. As another interesting note, he points out that cars are shifting from being pure hardware to complex software products. This leads to increasing competition with software companies like Google (e.g., AV Waymo) and changing revenue models, e.g., paying for the car per kilometer based on inbuilt telematics (Y. Zuehlke, personal communication, March 06, 2020). Thus, the ongoing digital transformation turning vehicles into moving data centers may have the potential to drive business models suitable for car sharing forward.

[15] Read more about the ridesharing service here: https://www.moia.io/en.

From the **perspective of a municipality,** Mortensen believes in the importance of the sharing mentality concerning the future potential of car sharing. Citizens are becoming more aware of the various shared mobility possibilities, but there is still a significant step to make towards widespread and scalable usage. **Frederiksberg Kommune** is working on **facilitating** the appropriate **conditions** for car sharing by freeing up parking space exclusively for car sharing providers. In addition, they aim to collaborate with private companies as well as politicians with whom they currently develop a new mobility strategy, but the executable and scalable plan is yet to be defined (C. Mortensen, personal communication, March 12, 2020).

From a P2P car sharing provider and leasing facilitator's point of view, Ottensten believes that the modern technical development can make car ownership smarter. Corresponding with Mortensen's evaluation, he thinks that, even though people are used to considering the car as an item they own, the **mindset** about ownership increasingly **changes** towards access due to similar transformations in other areas such as apartment sharing via Airbnb. Tendencies of the evolving mindset, from ownership to access, can also be noticed in the growth of leasing business. In this regard, he sees the combination of car leasing and P2P car sharing as the most profitable in the long-term. P2P car sharing alone is more profitable than fleet dependent models but less profitable than combining P2P car sharing with leasing. The reason behind the profitability is **GoMore**'s ability to build the needed telematics technology into the leasing cars enabling the keyless access of a P2P car without meeting the car owner. As a result, 60% of all keyless cars are leased through GoMore. In this way, keyless cars are rented out five times more, increasing overall rentals enabled by leased cars through GoMore (B. Ottensten, personal communication, March 11, 2020).

Going more in-depth into the **processes of P2P car sharing and leasing,** GoMore facilitates three different car sharing models on one platform, namely ridesharing, P2P car sharing, and leasing (B. Ottensten, personal communication, March 11, 2020). When leasing a car, the customer can choose one of the cars available online and make a reservation for one of the cars. GoMore collects and sends the reservation with the customer's information to one of their leasing partners. Then, the leasing partner contacts the potential lessee and takes care of the KYC, especially the credit evaluation. Due to the relatively high churn rate from the reservation to the completed contract (about 25%), Ottensten sees potential in GoMore stepping into the leasing business themselves. Besides leasing partners, GoMore has several local mechanics partnerships where the lessee eventually picks up the car and can bring it in for maintenance. The car is insured by GoMore's insurance partner, leading to the compilation of insurance and service in the lease agreement (B. Ottensten, personal communication, March 11, 2020).

Once lessees receive their cars, they can share their cars through the P2P car sharing service provided on the same platform in GoMore. When renters register at GoMore, they need to undergo a thorough approval process that is manually conducted. Assuming the leased car has the keyless technology built-in, *Cloudboxx* by *Invers*[16], the renter can locate the car with the GoMore app. The actual physical keys are inside of the car, but the engine of the car is blocked (immobilized) until the eligible renter is unlocking the car with the app preventing break-ins. This security layer is required by the insurance to allow the rental of cars without the owner being present. The insurance receives all the necessary data from GoMore only in case of an insurance claim. In addition, the owner of the car is responsible for documenting any damages beforehand. Besides unlocking the car, the *Cloudboxx* facilitates the standard tracking of telematics data accessible within the provided app. While GoMore's keyless product enables a more convenient and flexible pick-up and drop-off for the renter, the owner does not meet the renter anymore in person, which can result in trust issues. Therefore, GoMore also tracks the GPS of the car, in case of any possible theft or fraud. While the process of implementing the keyless technology entails additional effort and costs for GoMore, the resulting benefits, and increase of attractiveness and demand outweigh. The combination with leasing does not only lead to a more straightforward implementation of the *Cloudboxx* but also ensures the relatively new condition and model of the car (B. Ottensten, personal communication, March 11, 2020).

6.2. Security & Privacy

As a major finding, Busch identified the importance of adequately analyzing where blockchain and other DLT technology make sense. He emphasizes that DLT is only interesting concerning the need for decentralized connectivity, safety, and security. While for many applications the classic connectivity is sufficient enough, Busch recommends to use blockchain only in use cases where an **added security layer** is needed. Especially concerning the further expansion of digital identities for various mobility services, secure authentication and data storage is essential (cf. more under 6.3 Authenticity) (personal communication, March 15, 2020).

On the contrary, Mortensen and Zuehlke raise the concern of **personal data protection** in alignment with GDPR compliance. Mortensen points out that, so far, General Data Protection Regulation (GDPR) is not flexible enough to comply with blockchain questioning who would take on the responsibility (personal communication, March 12, 2020). Adding to this point, Zuehlke notes the grey zone and general restriction of sharing data across companies in compliance with

[16] Read more about the technology here: https://invers.com/cloudboxx/

GDPR for personal data stored on immutable shared ledgers. In this regard, he emphasizes the importance of keeping control over the data (personal communication, March 06, 2020). This balance between centralization and decentralization, together with an appropriate permission setup, needs to be considered when choosing a suitable blockchain platform. According to Busch, HF, as a **permissioned blockchain**, is most stable, scalable, and especially secure while being manageable due to the control over permissions (personal communication, March 15, 2020). As an example, BMW and VW have seen a great suitability of the decentralized nature of blockchain for the shared charging access cutting off the less secure intermediaries (D. Pietsch, personal communication, March 20, 2020; Y. Zuehlke, personal communication, March 06, 2020).

Ottensten confirms the recurring **trust issue** of their car owners concerning their valuable assets. Thus, GoMore addresses this issue by collecting GPS data and ensuring a thorough approval process of its users (B. Ottensten, personal communication, March 11, 2020). However, even though the GDPR compliance of blockchain may be a problem, it is questionable whether such **privacy-sensitive data** is secure enough when handled solely by a central authority. On the other side, decentralization through blockchain needs to take into consideration the change of control over data, as mentioned by Zuehlke (personal communication, March 06, 2020). This confirms the relevance of appropriate permission policies in our designed artifact where the collected privacy-sensitive data should be accessible by only those stakeholders who need it, and its handling should not rely on just one central authority.

Surprisingly, it is notable that privacy and security in regard to the storage of data per se do not seem to be the decisive argument to use blockchain. Nevertheless, securing digital identities enabling authenticity as part of security is one of the most significant benefits of using blockchain, which is addressed in the next section. After all, it still can be confirmed that using a permissioned blockchain, especially HF, for our designed artifact is recommendable while it is necessary to find the right balance between centralization and decentralization. Finally, the interviews show that the need for security and trust requires an assessment for every single use case and transaction within our designed artifact resulting in the questions of what should run on- or off-chain (cf. more within 6.4 Traceability & Reliability).

6.3. Authenticity

According to Busch, the **digital identity technology** based on blockchain and other DLT systems, also called Self-Sovereign Identity (SSI), has the potential of driving the development of the automotive industry and various mobility services including car sharing. In the future, he sees the need to fuse devices, especially vehicles, with the human user to facilitate a seamless interaction of the vehicle and its surrounding (personal communication, March 15, 2020). Pietsch raises the requirement of a standardized state-regulated digital identity for any citizen that could also be used by mobility services and already exists in most European countries, e.g., Denmark. However, some technological developments cannot move forward as long as such a digital identity is not implemented throughout all countries in the EU (D. Pietsch, personal communication, March 20, 2020).

Thus, VW started to develop its own mobility ID systems to sign into different mobility services, such as MOIA, with the same ID, eliminating the need to register to every service separately. In theory, it is an attractive idea to build a decentralized multimodal platform that is usable across cities. However, the **liability** for the data validation remains an issue as, for example, ShareNow provided by BMW would probably not like to take the liability of assuming the correctness of a previously uploaded driver license to WeShare offered by VW (Y. Zuehlke, personal communication, March 06, 2020). As a result, Zuehlke states that a collaborative platform requires **building trust** not just to their customers but also between the companies who collaborate on that platform. In the same manner, he believes that blockchain for car sharing makes especially sense concerning the verification of IDs and allocating earnings as blockchain has its best applicability where a natural trust issue exists, and increased transparency is needed (Y. Zuehlke, personal communication, March 06, 2020).

As another example, the *Deep Parking* project of Bosch, together with Siemens, demonstrates the importance of authenticity through a secure digital identity. This project addresses the problem of too many unused parking spaces in garages of apartment blocks. Blockchain-enabled digital identity management is used to determine who is allowed to enter the garage and when. With the suggested solution, a user can reserve a parking spot and drive into the underground parking area by using his **unique and universal SSI** without the need to register newly. In the same way, the user can charge or share the car with someone else while using the same blockchain-enabled SSI (P. Busch, personal communication, March 15, 2020).

Going deeper into the development of SSI, Busch states that blockchain is suitable for cryptographic encryption of SSI and its respective security, but to make it scalable and fast, it is dependent on other technologies. In this regard, he introduces the World Wide Web Consortium, which is working on a standardization of SSI, called Decentralized Identifiers (DID). It is an advancement of blockchain towards a global decentralized identity network enabling scalability and smart interconnection of all entities while ensuring a certain security standard. Realizing the importance of digital identity management, HL is also advancing towards new models of digital identity, especially the projects Indy[17] and Aries[18], which seem to be promising (P. Busch, personal communication, March 15, 2020).

Based on the mentioned statements, it can be confirmed that authenticity enabled by digital identities is indeed a crucial feature of blockchain and essential for the future of mobility, including car sharing. In addition, authenticity-empowered trust plays a significant role in facilitating a collaborative platform. Consequently, this validates the relevance of our demonstration, keyless vehicle access control, as one notable example of V2P interconnection in the future.

6.4. Traceability & Reliability

The seamless tracking of the **telematics data** during the lifecycle of a car is of great importance within P2P car sharing. Based on the monetary investment made by car owners, it is crucial to track IoT telematics data to avoid odometer and insurance fraud or theft, establishing trust in a P2P car sharing platform (B. Ottensten, personal communication, March 11, 2020; D. Pietsch, personal communication, March 20, 2020).

In this regard, Pietsch mentions the mileage verification of a vehicle as an example of an applied blockchain use case. The tracking of the mileage within the blockchain provides reliable and traceable proof at each point, eliminating the chance of counterfeit (D. Pietsch, personal communication, March 20, 2020). As mentioned before, Ottensten notes the importance of suitable telematics technology and the corresponding access to it concerning different car models and implemented technological standards available. The implemented *Cloudboxx* by GoMore provides tracking of the needed telematics and the immobilization of the car to prevent break-ins. The automatic mileage tracking minimizes the effort of the lessee as the renter is automatically charged with the exact consumption, and both can trust in the correctness of the data (B. Ottensten, personal communication, March 11, 2020). Additionally, Pietsch specified that once the handling of fraud and damage claims is not processed within one parent company (e.g., BMW Group Financial Services as its own financial service provider), the utilization of a blockchain makes sense, as the **data transmission or access between companies** where trust is not naturally established is made feasible. Especially in cases of customized insurance (e.g., pay as you drive) or leasing contracts, blockchain can ensure the reliability of the telematics data (D. Pietsch, personal communication, March 20, 2020).

[17] Read more about the technology here:: Hyperledger Indy
[18] Read more about the technology here:: Hyperledger Aries

As another essential evaluation aspect, the consideration of executing transactions **on- or off-chain** is necessary. Zuehlke mentions that it is vital to evaluate the need for secure data sharing between companies (personal communication, March 06, 2020). The shift of the execution of a transaction onto the blockchain becomes necessary in case there is a trust problem concerning the reliability of data and involved stakeholders (D. Pietsch, personal communication, March 20, 2020; Y. Zuehlke, personal communication, March 06, 2020). In the same manner, the blockchain-based car sharing platform will incorporate a high number of transactions, leading to a restriction of the applicability of a classic blockchain (P. Busch, personal communication, March 15, 2020). Hence, many transactions have to be executed off-chain. Along these lines, only in case a proper verification, identity authentication, and security standard are needed, the blockchain should be applied (P. Busch, personal communication, March 15, 2020; Y. Zuehlke, personal communication, March 06, 2020). Busch points out that the scalability of the network will play a major role in the decision to execute transactions on- or off-chain. He estimates that this factor may lead to the usage of standard connectivity for most transactions, and only security-related actions are executed on-chain (e.g., identification of an entity) (P. Busch, personal communication, March 15, 2020). According to Zuehlke, transactions concerning the verification of IDs and the allocation of assets require a corresponding security standard and should be executed on-chain to ensure the traceability and reliability (personal communication, March 06, 2020). Additionally, Pietsch indicated that transactions should be executed on-chain if manipulation of data needs to be controlled in inter-company collaboration leading to the prerequisite of an immutable transaction log (personal communication, March 20, 2020).

Based on the interview statements, we can conclude that for each use case, the trade-off between the needed security and traceability for each transaction, as well as the feasibility of executing on-chain, has to be evaluated. The demonstrated use case of our artifact, keyless vehicle access control, needs a certain level of security for the authentication as well as reliability of the data. Whether the actual transaction process could be shifted to off-chain is discussable.

6.5. Scalability

Busch states the goal of Bosch is to connect any product to the internet. As part of this overall goal, they aim to enable **V2X communication**. As the number of connected IoT devices increases immensely, the infrastructure needs to be highly scalable, stable, and fast while providing the optimized usage of resources. Apart from DLT, other critical technologies need to be developed further (e.g., 5G/6G, quantum computing), and innovations need to be taken into account to enable the scalability of such a platform (personal communication, March 15, 2020).

The evaluation of possible blockchain platforms suitable for the development of a blockchain-based car sharing platform is relevant to facilitate the scalability of the whole architecture setup. Overall, the **technological maturity** of the available blockchain platforms is critical, and the suitability to a use case needs to be evaluated individually (P. Busch, personal communication, March 15, 2020; Y. Zuehlke, personal communication, March 06, 2020; D. Pietsch, personal communication, March 20, 2020). Apart from the maturity of the technologies, the blockchain platform providers promise more than they fulfill at the moment. For example, Ethereum promised to release Eth2.0 in January 2020 but has already postponed it twice. This makes it difficult for OEMs to advance collaborative product development and evaluate which technologies are scalable and suitable (Y. Zuehlke, personal communication, March 06, 2020; D. Pietsch, personal communication, March 20, 2020). The pressure on each blockchain platform provider increases as the market consolidates and providers, who do not meet their promises to various enterprises, will be driven out of the market (Y. Zuehlke, personal communication, March 06, 2020). Nevertheless, this strain may lead to the actual progress of technological development, resulting in scalable and **industry-ready** platforms for the mobility industry (D. Pietsch, personal communication, March 20, 2020). Apart from the existing cryptocurrency applications, e.g., Bitcoin and Ethereum, there is no real-life evidence whether those protocols would be applicable in regard to the vast number of connected vehicles (P. Busch, personal communication, March 15, 2020).

According to Busch, **Ethereum** accounts for the majority of implementations at the moment but shows problems concerning scalability and costs (personal communication, March 15, 2020). **IOTA** seems to be too immature and caught up in arising technological problems (P. Busch, personal communication, March 15, 2020) as well as struggling to meet their development promises (Y. Zuehlke, personal communication, March 06, 2020). **HF** appears to be one of the most stable platforms and shows improvement concerning scalability and security. As HF is a permissioned blockchain, the management effort seems feasible, but at the same time, compromises have to be made as the network is not public. Therefore, so far, HF might not be the best solution for an extensive public network, incorporating an entire industry, to work with it efficiently. More demonstratively, HF may work with fleet operators in a network of 20-30 nodes, but on a larger scale, suitable for an entire industry, administration and scalability issues will arise (P. Busch, personal communication, March 15, 2020).

As mentioned, the evaluation of **on- or off-chain** execution of transactions is essential, especially concerning the scalability of the network. The tremendous amount of transactions which would be needed for our artifact may lead to the need to execute most of the transactions off-chain. Especially concerning the energy efficiency within an IoT blockchain architecture, the shift of transactions off-chain is sensible to assess (P. Busch, personal communication, March 15, 2020). Thus, blockchain should be utilized for identification and transactions which need an added security layer (P. Busch, personal communication, March 15, 2020; Y. Zuehlke, personal communication, March 06, 2020).

Based on the interviewees' statements, the challenge of enabling everything connectivity to move forward car sharing and other mobility services and, at the same time, ensuring the scalability of such an immense system is visible. Therefore, DLT technology, such as blockchain, alone will not be the only technology that provides the scalability of such a system, but it will also rely on general network and communication technology (e.g., 5G/6G). Nevertheless, it is of high relevance to consider carefully which transactions should run on- or off-chain as well as select a blockchain platform that supports scalability, HF may be one of its kind.

6.6. Interoperability

The importance of interoperability concerning shared assets in the form of **inter-company collaboration** is confirmed by Pietsch and explained based on the example of ChargeNow[19] (personal communication, March 20, 2020). The single-brand operation for charging stations does not make sense as a critical mass is required on the build infrastructure to gain relevance (network effects). ChargeNow only acts as an access provider as the charging stations are aggregated and not offered by the company itself, leading to the advantage of attracting a broader, not company-specific, range of customers (D. Pietsch, personal communication, March 20, 2020). Realizing the relevance of interoperability, VW already uses blockchain for electrical charging with its initiative Share&Charge[20]. It represents a decentralized charging infrastructure enabling every person (individual or company) to add their charger to the network based on a standard (Y. Zuehlke, personal communication, March 06, 2020).

To maximize the **value creation** with the customer, OEMs already collaborate with and incorporate insurance and leasing companies, blurring the line between leasing and rental. But these steps are taken by OEMs separately (D. Pietsch, personal communication, March 20, 2020), leading to the fragmentation of the business processes, platforms, and databases. According to Pietsch, the implementation of a blockchain makes sense as soon as these processes are shifted outside a company, and trustful collaboration between different companies is needed (personal communication, March 20, 2020). According to Zuehlke, the advancement of blockchain

[19] Read more about service here: https://chargenow.com/web/chargenow-global
[20] Read more about service here: https://shareandcharge.com/vwfs-partnering/

applications builds up pressure on various organizations to enable inter-company solutions, finding a way on how to work and collaborate, especially within the same industry. Although it makes sense to utilize blockchain for streamlining inter-company processes, the implementation is resource-intensive, costly, and time-consuming resulting in long-lasting projects (personal communication, March 06, 2020). An important aspect is the number and type of stakeholders involved in the setup of inter-company collaboration. Pietsch states that cooperation on the data and process side, as well as a competition on the service side, is needed, leading to a so-called **co-opetition**. In this regard, he thinks that to reach an actual consensus it makes more sense to establish a consortium of only two to three big players in a closed form and afterward open it up for the rest of the industry instead of an extensive consortium such as Mobility Open Blockchain Initiative (MOBI)[21] (personal communication, March 20, 2020).

The aforementioned statements demonstrate the need for a platform facilitating inter-company collaboration, which leads to the necessary evaluation of which stakeholders would have the most considerable interest and ability to set up such a blockchain-based car sharing platform. Busch confirms that large OEMs are already invested in applying blockchain for different use cases. Nevertheless, it is unfeasible for one OEM, even the global corporations, to implement DLT without collaboration. Therefore, the traditional big players of the industry must move closer together and advance their digitalization strategies with **joined effort** while also including relatively new automotive market entrants, e.g., Google and Tesla (personal communication, March 15, 2020). Pietsch points out that the traditional OEMs already have the necessary experience with the resources, car manufacturing expertise, and the whole industry compared to the newer entrants. Especially bare mobility service software providers, such as Uber, who have limited knowledge about the hardware technology within a car, should not get involved in the initialization of the platform. More in-depth, the current value creation logic of a car involves several cycles and subsequent risks (e.g., residual value risk), which needs to be accounted for when setting up such a platform (personal communication, March 20, 2020). Thus, it can be concluded that OEMs may be better positioned based on their longstanding experience within the industry even though they are not seen as the pioneers in terms of digitalization.

Compared to traditional players, **smaller companies** are more agile, and the degree of innovation is higher (Y. Zuehlke, personal communication, March 06, 2020). At the same time, new technologies and business features have to be developed faster, and the deployed technology needs to be flexible, simple, and scalable. As a result, it may be concluded that it is not feasible for a smaller company to set up our blockchain-based car sharing platform (B. Ottensten, personal

[21] Read more about the initiative here: https://dlt.mobi/

communication, March 11, 2020). According to Mortensen, a possible scenario could involve the joint effort and collaboration of **OEMs**, bigger **industry-related stakeholders**, and startups on initializing such a blockchain-based car sharing platform (personal communication, March 12, 2020). Mortensen additionally confirms our assumption that the **government** would be part of shaping the city and governmental infrastructure to provide the circumstances for a successful implementation. Nevertheless, car sharing per se stays in the responsibility of the private sector and needs to be initiated by a company and not the government (personal communication, March 12, 2020).

Apart from the interest and ability, the **incentive** of a company to invest in a blockchain-based car sharing platform needs to be evaluated. The possibility of sharing the development and operational costs of the platform with suitable partners can be seen as one incentive to start the platform. But as of now, the **monetary** incentive of providing the resources for the development is not clear since the platform will be used in a decentralized manner. In other words, a decentralized product leads to no direct derivable monetary benefit; therefore, the financial attractiveness of the investment is questionable. Moreover, companies have a responsibility towards their employees, and investing in a burdensome financial project without a clear indication of disruptive success leads to doubts besides its benefits (Y. Zuehlke, personal communication, March 06, 2020). As another aspect, a **suitable business model** for starting and owning the infrastructure of a blockchain-based car sharing platform appears to be missing so far. On the one hand, the possible loss of customers and price sovereignty seems to diminish the attractiveness for a company to get involved in such a concept. The companies want to keep their value-added chain to themselves as the value creation is simpler to oversee when kept in-house compared to a collaborative effort, e.g., calculation of acquisition costs compared to sales. On the other hand, the incentive to start a platform might stem from the potential to develop a **position of power** by controlling the platform and other stakeholders through margins, e.g., commission fees (D. Pietsch, personal communication, March 20, 2020). As a final note in regard to incentives, Zuehlke points out that **replacing** the PSP as an **intermediary** (such as Visa, Mastercard, or Paypal) with cryptocurrencies can reduce the costly fees and enable a more optimized cost allocation (Y. Zuehlke, personal communication, March 06, 2020). A similar argument has been brought up by Ottensten, who implies that only when the exchange of a significant amount of money is involved companies feel the urge to secure the valuable assets and saving costs due to unnecessary fees (personal communication, March 11, 2020).

From the aforementioned statements, we can confirm that the interoperability and seamless integration of the OEMs and leasing companies to set up a more attractive blockchain-based car sharing platform is indeed an important principle to take into account in our designed artifact.

There is a need to optimize the processes of leasing and car sharing to ensure better collaboration between all involved stakeholders. Incentives for a consortium of OEMs to set up the network are given as the administrative tasks are reduced to a minimum based on the system implementation and incorporation of the business logic in smart contracts as well as the allocation of administrative and operational efforts over several companies. Based on regulating and executing the whole leasing and car sharing process on one platform while sharing data securely, new features can be offered. For example, a usage-based insurance pricing model could be enabled by each insurance as the leasing and rental data is directly accessible. The possibility to create new features and revenue streams are required as incentives for other companies to join the network. The modular architecture of HF eases the integration of each organization's system. In conclusion, providing the right incentives can move forward the further development and applicability of our artifact while first, a profitable and scalable business model has to be identified.

7. Discussion

So far, the literature review led to the defined key design principles of the artifact, which is demonstrated on a small scale employing a prototype and then evaluated based on expert interviews. Next, all three sources, literature review, prototype, and interviews, are brought together to discuss the feasibility and need for the designed artifact that eventually gives us the ability to answer our research questions. The discussion is again structured along with the five key design principles and, in the end, summarized based on the interconnection of those principles.

7.1. Security & Privacy

The **trust issue** of sharing a valuable asset in P2P car sharing has been analyzed and noted by previous research (Le Vine et al., 2014; Madhusudan et al., 2019; Münzel et al., 2020; Shaheen et al., 2012). While many sharing platforms can solely rely on reputation and review systems to ensure trust between a host and guest (Bossauer et al., 2019), the technical advancement in vehicles has given P2P car sharing providers the ability to add another layer of trust by tracking telematics data of vehicles (Le Vine et al., 2014). This is also confirmed by GoMore, which is using telematics to ensure secure keyless access of the car as well as tracking of kilometers, GPS, and more to build trust (B. Ottensten, personal communication, March 11, 2020). While collecting such privacy-sensitive data may build trust, its insecure processing, access, and storage, as well as the unreliable traceability, could defeat the gained trust after all. As Dedeoglu et al. (2020) note, current centralized approaches to ensure IoT security and privacy impose trust in a central authority while limiting the scalability of extensive IoT networks, which are in high demand, especially in mobility enabling V2X connectivity. Therefore, a **decentralized trust mechanism** in the form of blockchain technology may ensure to eliminate the single point of failure and attack of existing centralized IoT security mechanisms (Christidis & Devetsikiotis, 2016; Reyna et al., 2018) as well as the distribution of control on several nodes (Rathee, 2020). In the course of this, the degree of decentralization and respective choice of a secure, privacy-preserving blockchain platform with a suitable consensus mechanism needs to be discussed. In addition, the implications of the **immutable chains** of IoT data storage in practice, that supposedly represents another benefit of blockchain, is reviewed concerning privacy-sensitive data.

7.1.1. Decentralization

While decentralization can ensure higher security and minimize possible data breaches by less secure intermediaries, it is pointed out by Zuehlke that it may lead to the loss of control over the data and the system (personal communication, March 06, 2020). This discord demonstrates the **trade-off** underlying the **decentralization** of a network where a system may be more secure, but participants are not willing to give up complete **control** over the data. This leads to the need to find the right balance between centralization and decentralization, together with an appropriate **permission setup**. This consideration is especially essential concerning the choice of a suitable blockchain platform. The application of a consortium blockchain seems to be the sensible choice as each entity receives a certificate with corresponding permissions; therefore, the participants are not anonymous, which is beneficial in a setting where multiple organizations operate in the same industry (Dedeoglu et al., 2020).

The characteristic of **HF** enables the deployment of the blockchain network by a consortium (Hyperledger, 2019), dividing the responsibility to manage the **consensus mechanism** and maintenance of the blockchain by a group of equally-powerful participants (Dedeoglu et al., 2020). The conducted business evaluation of our artifact led to the assumption that a group of OEMs is best positioned to initialize the platform. However, the collaboration of OEMs needs to be well-considered as a power imbalance within the system may demolish the benefits of secure decentralization. The validators have to reach consensus to set up and adapt the network (Dedeoglu et al., 2020), which could lead to an abuse of power by certain consortium members as they could make their agreement dependable on self-beneficial factors such as economic benefits. Within the HF setup, the applied consensus mechanism is **CFT** (Hyperledger, 2019), leading to an equal distribution of power between the validator nodes. However, in case one node acts malicious, the consensus mechanism will be affected by it (Xiao et al., 2020). As HF is working on the implementation of **BFT** consensus mechanism, which aims to avoid such malicious activity, future research should test the applicability and possible implications for an OEM-driven setup of a blockchain network with BFT consensus mechanism.

As mentioned in our evaluation, the security and privacy aspect regarding the storage of data seems not to be the decisive argument to apply blockchain. As both Zuehlke and Ottensten point out, the consideration of **cutting intermediaries** in a decentralized network is especially of relevance concerning PSPs (personal communication, March 06, 2020; personal communication, March 11, 2020). In this regard, it is naturally about saving the associated fees but also shows that there may be a tendency to think about security, especially in transactions and processes where significant monetary value is implicated. Due to the small sample of the qualitative data collection, further research is needed in this area to receive more insights of the incentives driving the implementation of secure decentralized systems.

In summary, the collaboration of OEMs needs to be well constructed, documented, and supported by respective contracts to maintain the benefits of decentralization, ensuring the security of the blockchain network and related data. The assessment of the benefits and incentives of such a decentralized network can be used as a basis for future research, discussing in-depth the positive and negative aspects. In addition, the stated discord shows the need to test and compare the security performance of different types of blockchains with various permission settings. Therefore, HF's development, other projects from HL as well as different blockchain platforms need to be compared to each other.

7.1.2. Immutable Chains

The positive aspect of immutability enabled by the ledger structure and consensus mechanism, needed for secure sharing of IoT data is confirmed (Reyna et al., 2018); D. Pietsch, personal communication, March 20, 2020). Nevertheless, the applicability and usefulness of applying **immutability to data storage** needs to be evaluated in-depth for each use case (Y. Zuehlke, personal communication, March 06, 2020), not only dependent on the privacy and security benefits but also its legal aspects. The data gathered for the proposed blockchain-based car sharing platform includes privacy-sensitive information. As individuals have the right to demand the erasure of their personal data (i.e., "**Right to be Forgotten**") according to the European GDPR (Regulation (EU) 2016/679, 2016, Art.17)[22], the tracking of the information on an immutable ledger poses the challenge of deleting the records and hence the compliance of the platform with the legal environment (Dedeoglu et al., 2020; Reyna et al., 2018). Therefore, the discussion of whether all transactions and subsequent data needs to be stored immutably has far-reaching impacts. Consequently, it is essential to conduct further research on how to make blockchain more flexible in changing data and thereby complying with legal regulations like GDPR while still maintaining the traceability.

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

7.2. Authenticity

According to previous research, the secure and reliable authentication with diverse levels of **access control** to IoT devices is of significant importance and blockchain can provide the necessary **identity management system** (Hang & Kim, 2019; Reyna et al., 2018). Pietsch indeed confirms that tracking mileage data to avoid counterfeit is a relevant use case for blockchain, but the authentication of vehicles with such privacy-sensitive data and its access control has not been mentioned. Instead, the authentication of users in the digital world has been more of concern for Pietsch in alignment with Busch and Zuehlke (personal communication, March 20, 2020; personal communication, March 15, 2020; personal communication, March 06, 2020). Taking the prototype as an example, we realized that the identity of the user seems to be more crucial to authenticate in the blockchain than the collected data from the vehicle, such as the timestamp. Along these lines, it can be argued that if the stored IoT data of a vehicle is delinked from the identity of the user, the focus on the authenticity of the end-user may be sufficient enough.

Continuing the elaboration on the user authenticity, Busch notes that in the future of smart mobility and city, not only the communication between V2V is of relevance but especially the seamless integration of the user and the city will revolutionize mobility (V2X) (personal communication, March 15, 2020). However, as long as the valid and reliable user's identity remains offline, this will not be possible. In this way, **digital twins** are a rising trend and concern for not just the automotive industry but entire countries (D. Pietsch, personal communication, March 20, 2020; P. Busch, personal communication, March 15, 2020). In the car sharing process alone, users are interacting with a growing number of different businesses. This raises the problem that every interaction with a new business entails newly created digital personas that are disconnected from each other. These split identities result in **data silos** that lead to costly, timely, and possible fraudulent data sharing (Ferdous et al., 2019). Bringing everyone together on one platform enabling secure data sharing with blockchain technology, one unique and universal identity can be created that allows the user to access the services provided by all businesses.

Concerning the sharing of identity data across companies to ensure seamless authentication, Zuehlke doubts the willingness of various stakeholders to take on the **liability** that the shared identity-related data is correctly validated. He claims that, at first, trust needs to be established between the stakeholders (personal communication, March 06, 2020). While this may be a reasonable concern, this exact trust problem about the validity of submitted data is in fact made void when using blockchain due to its traceability and reliability that a decentralized network has validated the submitted data. On the other side, Zuehlke's concern also shows that, especially in the combination of blockchain and sharing economy, the assessment of its **permission policies** and the degree of decentralization in alignment with the respective stakeholder and use case is of significant importance. In this context, it has to be noted that preserving authenticity across an entire platform is not just about end-users or IoT data but also in which participants in the blockchain network are allowed to access data. It may be argued that a higher degree of decentralization (i.e., public blockchain) could lead to a smaller need for trust in a central authority. However, findings of Hawlitschek et al. (2020) point out that complete **trust-free systems** are hardly transferable to the interactions in a sharing economy, and blockchain can replace trust in a platform to only some degree. Thus, it can be concluded that blockchain in an industrial context, where our designed artifact resides, will most likely never work without some kind of regulator leading to our confirmed choice of a permissioned blockchain instead of a permissionless blockchain. Elaborating further, as our designed artifact involves valuable assets, leasing companies commonly need to conduct a **KYC check**, which requires a blockchain network to reveal the digital identity of the respective lessee. Since Bitcoin and other public blockchains allow anyone to participate while keeping their identities anonymous, it has led to cases of money laundering and illegal transfers. This is aimed to be avoided by implementing KYC mechanisms also on blockchain operations, consequently resulting in a more controlled and “permissioned” network (Dedeoglu et al., 2020).

In summary, two overall findings can be concluded. First, there is a need to find the right balance between centralization and decentralization, meaning the allocation of control levels and permissions while ensuring transparency over both IoT and user data. Secondly, permissioned blockchain networks with an implemented thoughtful digital identity management can facilitate a somewhat trustless blockchain-based car sharing experience while ensuring authenticity for the involved businesses in the car sharing and leasing process and avoiding data silos. Whether blockchain is the only technology enabling the secure sharing of data with the needed decentralized digital identity for IoT devices and users alike, is discussable and needs to be observed in the future. Nevertheless, blockchain serves as an essential step to give a thought to the importance of authenticity and the need for digital identity management.

7.3. Traceability & Reliability

The examples of mileage tracking and usage-based insurance made by Ottentsen and Pietsch confirm that the applicability of blockchain for our use cases is reasonable to ensure the reliability of the stored data for each stakeholder (B. Ottensten, personal communication, March 11, 2020; D. Pietsch, personal communication, March 20, 2020). As the blockchain incorporates **one**

single truth, immutability, and reliability of data, the **trust** in the correct tracking and storing of data is enhanced. The designed artifact ensures that each transaction is logged from the ordering of a leasing car over the selection of an insurance package to the rental of a car. As the telematics data of a leasing car is stored and accessible by the lessee and leasing company, disputes at the end of a leasing period are minimized (Guhathakurta, 2018). The tracking of the IoT data ensures the certainty of the state of the car and cannot be manipulated, leading to reproducible history in case of fraud or damage. This data is also utilized to set the prices for insurance and rental fairly according to usage (Gösele & Sandner, 2019). After all, it gives back control and power to the short-term renter and lessee, especially needed in sharing.

Nevertheless, the implementation of the whole process for our use case, keyless vehicle access control, **on-chain** is discussable. The demonstration showed that the specific unlock transaction can be processed on-chain, but it is questionable whether all transactions should be processed on-chain, considering an implementation of a complete system for an entire industry. Based on the assessment from our interviewees, we conclude that most likely, only the authentication of the user and vehicle should be processed on-chain to ensure a stable system. In our use case, each status of the car, from available to completed, is first updated in the world state and then stored on the blockchain. This leads to an **immutable history log**, which allows the querying of the car status at all times. The question arises if the history log of the status is needed in an immutable manner or if a centralized data storage, accessible by the according stakeholders, is sufficient enough. As the status of the car does not entail any trust or security issues while keeping in mind the immense scale of our blockchain-based car sharing platform, it may make more sense to utilize central storage. In this case, the interaction with the blockchain would be restricted to authenticating the user and car once the location request is sent, providing the needed security layer for a trustful rental process. Consequently, for each transaction, a **careful evaluation** of the combination of decentralized and centralized storage of data, questioning the trade-off between scalability and traceability, is needed.

Along these lines, we suggest a thorough **risk assessment** for specific characteristics, such as the value of the car or the length of the leasing period. As mentioned before, the need for storing data in the blockchain increases with the risk of a possible breach in trust. As confirmed by Ottensten, the leasing partner conducts KYC checks only when a car is leased at least six months (B. Ottensten, personal communication, March 11, 2020). As a result, it can be assumed that the risk increases the longer the leasing period and hence the importance of storing the corresponding data immutable and reliable on the blockchain. The same applies to the value of the car, where it may be assumed that cars with higher monetary value also imply higher psychological value and trust issues leading to the need to store the transactions in the blockchain. For instance, a highpriced roadster may need to be traced more securely than a cheaper compact car. In conclusion, the decision of which data should be traceable and hence stored on-chain may not only be dependent on the use case itself but also other characteristics of leasing. The same may be applied to car sharing where such a short period of rent results in rather off-chain storage, but, depending on the rented car, some of its data could lead to otherwise higher relevance to store on-chain.

While these are mostly pure assumptions, it can be concluded that there is an immense need to assess the necessity of every single transaction to store on-chain, considering which transactions need traceability and reliability due to a trust issue. This required complex assessment proves the mentioned concern that using blockchain, especially across multiple companies, leads to resource-intensive and long-lasting projects (Y. Zuehlke, personal communication, March 06, 2020). While such collaboration may not be the easiest to facilitate during the initiation phase, it could lead to immense benefits in the long-term.

7.4. Scalability

The challenge of constructing a scalable system, being able to handle the increasing amount of IoT data, can be solved by incorporating blockchain technology (Reyna et al., 2018). Nevertheless, the construction of the system needs to include careful evaluation of which transactions and data should be handled **on- or off-chain**. As Busch mentions, blockchain is suitable as an underlying technology, but what makes the whole system actually scalable and faster will be the application and combination of different technologies, executing a lot off-chain (personal communication, March 15, 2020).

The implementation of the whole process of our use case, keyless vehicle access control, on-chain is discussable. The demonstration showed that the transaction can be processed on-chain, but considering a system for an **entire industry**, only the authentication of vehicle and user may be necessary to process on-chain to provide scalability of the system. The process of validating a transaction on-chain also entails the application of a decentralized consensus mechanism, which, depending on the chosen mechanism, endures a significant resource consumption, limited throughput, and delay. Especially the combination of **resource-constrained IoT devices** and high numbers of generated transactions makes the provision of real-time responses through on-chain transaction processing difficult, if not impossible (Dedeoglu et al., 2020). As the majority of the stored data in the demonstrated use case does not entail any trust or security issues, it makes more sense to apply a central storage when keeping in mind the possible immense amount of cars being rented out through the platform, straining the performance and energy efficiency of the blockchain. In this case, the interaction with the blockchain would be restricted to

authenticating the user and car, providing the needed security layer for a trustful rental process. After all, in alignment with Busch, for each transaction, a careful evaluation of the combination of decentralized and centralized storage of data is needed (personal communication, March 15, 2020), questioning the **trade-off between scalability and traceability**.

While **blockchain** can enhance **IoT** authenticity and privacy as well as the secure sharing of data (Dedeoglu et al., 2020; Hang & Kim, 2019; Reyna et al., 2018), its **integration** is deemed to be challenging. In our conceptual design and prototype, we have applied the approach of Hang and Kim (2019) and Liu et al. (2020), where the IoT device is not directly integrated with the blockchain network as its own node. We can confirm that with the help of an MQTT's broker model, the transmission of IoT data and its subsequent verification in the blockchain is indeed feasible. Nevertheless, based on our observation, HF is clearly in need of better and more seamless integration with IoT. At the same time, an extension of our prototype with the incorporation of the IBM Watson IoT platform and its blockchain integration might prove us wrong. As emphasized by all our interviewees, the future of mobility relies on the connection of vehicles to each other, its users, and surrounding. Thus, it is eventually inevitable to make **vehicles part of the blockchain network**. However, it remains a problem to install the computing-intensive consensus mechanisms on the resource-constrained IoT devices (Dedeoglu et al., 2020). To enable the seamless interconnection between users and vehicles, the development of **lightweight consensus mechanisms** and, at the same time, equipping vehicles with **stronger IoT devices** is an imperative requirement for the artifact and, in general, for the entire automotive industry. While IOTA addresses this with its lightweight consensus mechanism specifically designed for IoT, it has been criticized by Busch and Pietsch due to its unreliability to fulfill promised features, immaturity, and recent technological problems (personal communication, March 15, 2020; personal communication, March 20, 2020). This discord between needed everything connection and the immaturity of existing blockchain platforms makes it questionable how blockchain will evolve to an industry-ready technology. After all, it can be expected that large blockchain consortiums in the mobility industry may not only push forward the mobility industry but also the development of such blockchain platforms and protocols, especially concerning an appropriate IoT integration (cf. 7.5.3 Possible types of consortiums).

Assuming that IOTA resolves its technical problems, we can derive from the interviews and literature review that the combination of a scalable protocol with a strong IoT-interoperability (e.g., IOTA) with a more reliable, secure and modular blockchain platform (e.g., HF) may be the most promising. IOTA could be used to facilitate the V2V communication with lightweight consensus while eventually all the generated IoT data is bundled and stored traceable and long-term in a permissioned HF-based blockchain network where the data can be shared securely and reliably among different stakeholders. In fact, a bridge system has been developed by IOTA that enables its integration with HF (Sabolev, 2019). This may be an interesting research and development area to keep a close eye on in the future.

In conclusion, there is a visible race to provide the scalable infrastructure for IoT, enabling the desired V2X communication in transportation. Whether this will base on blockchain technology depends heavily on the speed of its scalable and reliable development in the near future.

7.5. Interoperability

Only if a system is interoperable with the various processes involved in an inter-company platform as well as usable by all stakeholders, our blockchain-based car sharing platform can be facilitated. Along these lines, enabled automation, shared operation costs, and the enhanced feature offering through the sharing of data are possible incentives that have to be addressed to ensure the actual interoperability and usability of our designed artifact. Above all, the decision who is interoperating with each other and how it is facilitated is the most critical to be made. In the course of this, it needs to be discussed to which extent smart contracts can facilitate automation, and process optimization, distributed shared ledgers are addressing the need for sharing of data, and the right type of consortium can impact an entire industry.

7.5.1. Smart Contracts

The potential to ease the interoperability of different stakeholders and increase trust in the system based on the implementation of the **business logic** through smart contracts is confirmed (Dedeoglu et al., 2020; Yuan & Wang, 2016). On the other hand, smart contracts and how they are designed today should not be put on the same level as paper contracts. In reality, smart contracts only **automate processes** while its design, interpretation, and legal status need to be discussed (Y. Zuehlke, personal communication, March 06, 2020). Once the smart contract is deployed, it cannot be modified, leading to possible system vulnerabilities based on logic or coding errors (Dedeoglu et al., 2020). This shows the immense importance of a carefully planned setup of the system logic and the incorporation of suitable stakeholders to avoid missing critical implications of processes. Moreover, it demonstrated the importance of selecting appropriate stakeholders with the needed experience and expertise within the industry, as already emphasized by Busch (personal communication, March 15, 2020).

Returning to the legal interpretation, a smart contract eliminates judicial disputes as the implemented code is the rule for the smart contracts. Any disputes are resolved by the applied consensus mechanism of the network. However, smart contracts are triggered by clients and executed on the network, which could span over several jurisdictions. Thus, the applicable law is challenging to determine. In many jurisdictions, smart contracts are **not legally binding** based on the fact that the legal opinions about their enforceability vary from court to court (Dedeoglu et al., 2020). These legal issues amplify the debate about the suitability and application of smart contracts for streamlining the business logic of the stakeholders and the ease of implementation. The **maturity** of the technical implementation and legal systems of each country could be seen as one significant barrier to the successful integration and interoperability of several stakeholders. According to Zuehlke, this situation will not change in the next ten years, especially in countries like Germany with an extremely cautious legal system, requiring laws before an implementation is allowed and not basing decisions on case law as it is done in the US (personal communication, March 20, 2020). Conclusively, the technological and legal development of smart contracts will have a far-reaching impact on the applicability of our blockchain-based car sharing platform and needs to be elaborated in further research.

7.5.2. Shared Database

The benefits of streamlining the car sharing and leasing process based on the collaboration on data and resources are confirmed by the literature (Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019; Guhathakurta, 2018). In the same manner, all interviewees emphasized the need for collaboration to **optimize processes** within the industry in a cost- and resource-efficient way. One of the major advantages for users and businesses alike is the minimization of needed registrations and the subsequent elimination of **data silos** (Ferdous et al., 2019). As HF ensures the feasibility of the different business logics due to its high degree of confidentiality, flexibility, resilience, modularity, and scalability (Pavithran et al., 2020; Saghiri et al., 2020), the further development and testing of our use case on an HF network are recommended. However, a proof of concept for an HF-based car sharing platform is missing. Besides, comparable end-results about which blockchain or combination of different technologies could be suitable, are yet to be published (P. Busch, personal communication, March 15, 2020).

Apart from the actual implementation of HF, the need for a blockchain platform for our use case is still discussable. In case secure and immutable data sharing is required, blockchain seems to be a suitable technology (Y. Zuehlke, personal communication, March 06, 2020; P. Busch, personal communication, March 15, 2020). Nevertheless, depending on the use case, a **traditional shared database** with according permissions for each stakeholder might be sufficient enough. This especially applies if one takes into account the development resources and efforts needed to set up a blockchain-based car sharing platform (Y. Zuehlke, personal communication, March 06, 2020). Each involved stakeholder already has an in-house backend solution, which, to some extent, could be either implemented within a blockchain network or a shared database. The actual assessment of which implementation would make more sense for what applications concerning benefits compared to its effort needs to be researched in-depth. All in all, the hype around blockchain pushes enterprises to start thinking about sharing data across companies and figure out a way on how to collaborate best (Y. Zuehlke, personal communication, March 06, 2020). Whether blockchain will be the actual applied technology is dependent on its development (P. Busch, personal communication, March 15, 2020).

7.5.3. Possible types of consortiums

As confirmed by our interviews, both car sharing and blockchain have yet not found a feasible business model and strategy within the automotive industry (Y. Zuehlke, personal communication, March 06, 2020; D. Pietsch, personal communication, March 20, 2020). Consequently, the combination of both leads to an even more **challenging business model** where most of the active projects and research are without proven long-term success. Despite that, we see the need for collaboration in regard to both the processes and data sharing within car sharing but also leasing that can be driven and facilitated by blockchain (Bossauer et al., 2019; Dorri et al., 2019; Fraga-Lamas & Fernandez-Carames, 2019; Gösele & Sandner, 2019; Madhusudan et al., 2019; Valastin et al., 2019). Therefore, our proposed artifact may be feasible under the common accordance of most interviewees that blockchain cannot be implemented as a solo project for neither enterprises nor small companies (P. Busch, personal communication, March 15, 2020; D. Pietsch, personal communication, March 20, 2020; Y. Zuehlke, personal communication, March 06, 2020; B. Ottensten, personal communication, March 11, 2020). Thus, we can derive that the advancement of car sharing and other mobility services with DLT technology, such as blockchain, is only feasible in a **consortium of several companies**.

As a subsequent arising question, it needs to be discussed how such a consortium should be constructed to move forward car sharing but also other mobility services in a scalable and sustainable way. Within our domain of an OEM initiated car sharing platform, the size of the involved companies and of the consortium itself is to be considered. Alternatively, there are types of consortiums that focus on other involved stakeholders as well as models that rely on a different kind of collaboration.

By fusing **small entrepreneurial companies** and **large established firms**, new ideas and the agile way of working of smaller companies can be combined with the market experience and resources of enterprises (Y. Zuehlke, personal communication, March 06, 2020; C. Mortensen, personal communication, March 12, 2020). Thus, the most innovative consortium for the blockchain-based car sharing platform may be a smaller company, with distinct blockchain expertise, together with an OEM enterprise. Toyota with Oaken Innovation has already proven the success of such a consortium with a car sharing and leasing platform and a blockchain-enabled car identity and history data storage (Oaken, 2020). These projects confirm the indeed potential of our artifact providing ubiquitous data storage for mobility capacity across all stakeholders without the need of intermediaries while ensuring authenticity for both users and vehicles.

Besides OEM enterprises, **software enterprises** like Google should not be ignored in such a consortium. As pointed out by Zuehlke, OEMs should take a close eye on the development of Google's software-focused autonomous car Waymo (personal communication, March 06, 2020). The possibility of Google joining forces with a smaller blockchain company also for Waymo is not that inconceivable considering their new partnership with Chainlink enabling on-chain data solution with BigQuery (Google, 2019).

As another consideration for the type of consortium, it is relevant to examine how large such a consortium should be. While Toyota and Oaken Innovation seem to move forward fast, it can be claimed that to have an impact on an entire industry, such a **small consortium** may not be the long-term solution. In fact, Toyota joined a significantly **larger consortium**, MOBI. BMW has been the lead initiator of MOBI, which originated in the US but gets increasing traction to participate in Europe, as well (MOBI, 2017).[23] Most notably, MOBI announced their project of a Vehicle ID (VID) that relates to our claimed need for creating digital twins for everything, including vehicles. While MOBI has renowned organizations on board and is driven by an impactful objective, Pietsch doubts that MOBI's "American" way of innovating within blockchain and DLT will work in Europe, which needs a co-opetition. As mentioned in the business evaluation, he expects that MOBI may be too big of an elephant to move significantly forward, as reaching consensus with an immense amount of organization seems obstructive (personal communication, March 20, 2020).

Going a step further than MOBI, Decentralized Autonomous Vehicles (DAV), as an even **larger consortium**, aims to create an open-source, decentralized transportation network based on Ethereum blockchain that enables any number of transportation services to participate with any number of users. This is in distinct contrast to today's situation where almost every mobility

[23] Most of the participating companies have been US based but growingly European organizations such as Deutscher Auto Dienst, IOTA Foundation and Swedish Blockchain Association have joined.

service provider, such as car sharing, ride-hailing, micro-transit, or mass-transit, is siloed from each other (Copel & Ater, 2017).

While MOBI and Toyota with Oaken Innovation are focusing on the digital identity of vehicles, DAV's approach goes towards a more fundamental setup of an entire network. Such as MOBI, DAV, is based on an even larger consortium that includes MOBI but seems to be already more advanced in its development and inclusive, inviting anyone to contribute to the project through GitHub. In contrast to MOBI, DAV has its origin in Europe, but its contributors are spread around the world.

After all, the critical question is which of the aforementioned consortiums will lead the way to revolutionize car sharing and other mobility services based on blockchain. One thing is clear, the potential of blockchain to aggregate car sharing services and other mobility services on one platform in the fashion of **MaaS will be the ultimate goal**. The transformation of the automotive industry through blockchain and related technologies will undoubtedly be significant, but which type of consortium will lead the way and be eventually the one breaking through is as such not determinable and has yet to be observed. There are benefits and drawbacks for both small and large consortiums, including small or big companies, but it all depends on the geographical location, the existing infrastructure, technological development within blockchain and its supporting network. It can be concluded that there is a tendency that our designed artifact has the potential to drive car sharing with the capability to be extended to much more, but it depends on its setup, the participating stakeholders, and its degree of inter-company collaboration.

7.6. Summary of Discussion

After discussing the artifact, some interconnections between the different key design principles can be observed, though provisionally and yet to be tested in-depth, which is graphically shown in Figure 23. Most notably, there is a visible trade-off between traceability (including reliability), security (including privacy), and scalability. The **traceability** and **security** of the collected telematics and privacy-sensitive data require transactions to be processed and stored on-chain in a decentralized manner, which goes along with the desired V2X communication making every single vehicle part of the blockchain network. However, this faces the challenge of **scaling** such an immense integrated IoT and blockchain network with the current state of network and communication technology. Moreover, the present lack of lightweight consensus mechanisms and powerful IoT devices hinders the ultimate scalability of our proposed blockchain-based platform.

Even within the design principle **security** and **privacy** is an incoherent observation to make. While the immutability of data is a significant feature of blockchain, affecting traceability and security positively, it seems to be incompatible with the current state of privacy legislation in Europe (GDPR), where one has "the right to be forgotten". The more decentralized the network is, the more anonymous the participants can act within the system, which restrains required identification in regard to, for instance, KYC checks for leasing a car. This leads to the need for a permissioned blockchain enabling **authenticity,** which represents overall the greatest need to be handled on-chain. On the other hand, it is questionable to which extent a less decentralized system (through permissioned blockchain) can ensure privacy, whereas this requires again to trust the permissioned participants handling the data confidentially. In the same manner, the more private the blockchain network is set up, the more debatable it is how **interoperable** the sharing of data between stakeholders may be. This is in line with the discussed challenge of power distribution in such a platform. Overall, finding an adequate level of traceability, security, scalability, and authenticity can positively affect the interoperability of the entire designed artifact.

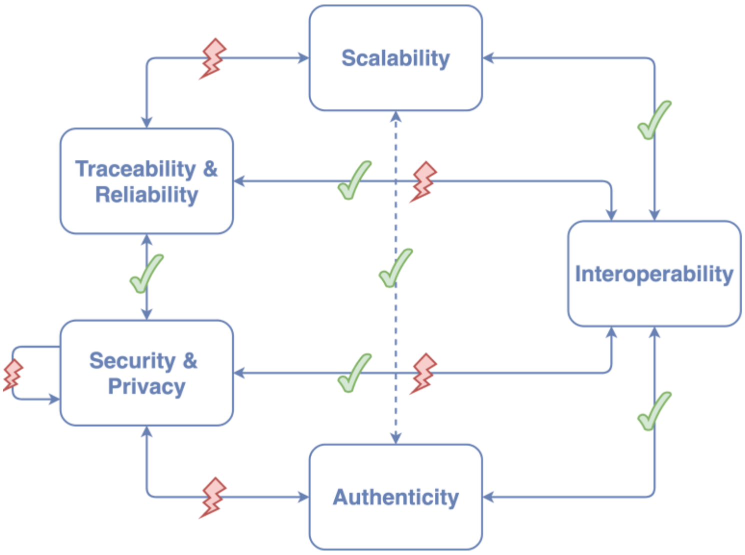


Figure 23: Summary of possible interconnections between key design principles

In conclusion, we see interoperability as more relevant in regard to open innovation, inter-company collaboration, and co-opetition than we initially inferred from the literature review. Moreover, especially scalability is more crucial and challenging to fulfill in a blockchain-based system than we initially assessed. This confirms the lack of research addressing the more industrial-focused impact of blockchain application. As a final note, it seems challenging to accomplish the five key design principles to their fullest simultaneously while significantly depending on the right balance between decentralization and centralization, as well as the decision of on- and off-chain.

8. Limitations & Future Outlook

Although we can confirm that blockchain can advance car sharing under the condition of the right balance between the key design principles, some limitations and subsequent research are needed to test and verify some of our findings as well as consider future technical developments. As the focus is on a holistic assessment of both the technical and business implications of the designed blockchain-based car sharing platform, this thesis incorporates only one cycle of iteration within the DSR process. The following identified limitations and improvements can be used as recommendations for performing subsequent iterative cycles to enhance the designed artifact.

With the implementation of a prototype for a keyless vehicle access control system, a successful hands-on **integration of the HF blockchain platform with IoT** is showcased. As the focus and overall goal of the implementation are on understanding the underlying technology and subsequent network, the prototype entails limitations that have to be addressed by further research. First, the setup of the prototype has to be scaled up to represent a real-world implementation more accurately, e.g., increase the number of nodes, users, and transactions. This leads to the need to perform extensive performance and security tests to verify HF for industrial applicability. Additionally, our motivation to especially investigate the IoT and blockchain interoperability leads to the sole reuse of an existing HF network instead of building the network from scratch. Therefore, the feasibility of adjusting the existing HF network more suitably to the car sharing application needs to be assessed from a technical and business perspective. The decision to use HF bases on a solely theoretical comparison between possible blockchain platforms. However, this needs to be verified and adjusted by testing and comparing the performance and different setups to other suitable platforms such as IOTA and Ethereum. Additionally, the potential of combining the different blockchain platforms to achieve better compatibility in regard to the key design principles should be assessed.

Based on the decision to emphasize the industrial impact of blockchain, this thesis does not take into consideration the **end-user perspective**. To gain complete insight into the effects of blockchain on car sharing, it is necessary to test and evaluate the designed artifact from the end-users' viewpoint in regard to the mentality of sharing, incentives for leasing as well as the general usability and the possible gain in flexibility. In particular, it may be an interesting research area to dive deeper into the potential positive stimulation of leasing on the mentality to share, leading to more trust to rent out the leased car.

The business evaluation of the artifact, complementing the technical evaluation of the prototype, involves five expert interviews with different stakeholders. Although this provides a well-founded assessment within the scope of this thesis, an **extension of the qualitative data collection** with more experts and other stakeholders is needed to enhance the **generalisability** of our findings. As an additional step, a case study of an existing blockchain application in mobility with one of the OEMs could give a more in-depth insight into the processes, resources, and technical implications that are accompanied in such a blockchain implementation.

In general, the **government perspective** is limited to solely one expert interview with the municipality Frederiksberg Kommune. Studying more in-depth the role of the government within car sharing and its advancement through technology, including blockchain, can provide an enhanced understanding of needed changes in regulations and infrastructure, especially concerning the future outlook on sharing of IoT data in smart cities. This more in-depth analysis and consideration of a possible collaboration with the government can support the further development of our blockchain-based car sharing platform.

Moreover, the **leasing and insurance processes** are not analyzed in-depth, so the assumption is made that the streamlining of these processes is possible. So far research about blockchain for leasing and insurance is only mentioned as small possible use cases within the overall automotive industry. This thesis indicates a potential for this interface, showcasing the need for researching these areas separately more in-depth, especially in regard to blockchain's feasibility to comply with KYC checks.

Overall, the advancement of car sharing through blockchain has far-reaching impacts on the entire automotive industry and entails various research topics. In line with the current transformation of the automotive industry driven by digitalization, there is a clear trend towards the **platformization** and **aggregation** of services leading to the development of new value creation processes. Especially once **AVs** will become roadworthy, car sharing may reach a new level of relevance in combination with advanced IoT and digital twin (**SSI**) technologies where the vehicle ultimately acts as an autonomous entity not only driving-wise but also service-wise (e.g., earning money for renting out the car and paying for fuel). Along these lines, the proposed, designed artifact needs to be extended with a detailed consideration of **cryptocurrencies** as well as SSI to understand the feasibility of acting autonomously service-wise entirely. Finally, due to the resource-intensive effort, building such a blockchain-based platform may not aim to address only car sharing. Instead, the ultimate goal will possibly be to aggregate all mobility services on such a blockchain-based platform in the fashion of **MaaS**, moving from a vehicle-centric to a user-centric approach.

9. Conclusion

Motivated by the growing interest of OEMs in car sharing with its ability to reduce congestion in cities as well as blockchain as the digital universal weapon, an artifact comprising a conceptual design and architecture of a blockchain-based car sharing platform based on derived key design principles is designed. The resulting findings serve as a foundation to answer overarchingly:

How can blockchain drive the advancement of car sharing?

By consolidating the gained technical understanding and the subsequent business-related insights, we can confirm that blockchain, as one possible technology, can take part in advancing car sharing by facilitating inter-company collaboration between several stakeholders within car sharing and leasing as well as eliminating the need for trust to some extent. However, the design of the underlying blockchain-based platform relies on the appropriate balance between security & privacy, authenticity, traceability & reliability, scalability, and interoperability. Depending on the priorities, the involved stakeholders face the challenge of finding the right balance between ensuring and eliminating the need for trust as well as determine the appropriate level between retaining and giving up control over data and processes while at the same time guaranteeing the scalability of the overall system.

Along these lines, the proposed car sharing platform, involving an immense amount of IoT data collected by millions of vehicles, faces the challenge of integrating IoT with blockchain scalably. In this thesis, we can demonstrate an integration where IoT devices are not part of the blockchain network as own nodes to answer the research sub-question:

How does blockchain interoperate with IoT based on the example of a keyless vehicle access control system?

While this thesis can confirm the interoperability of such an IoT and blockchain integration, it is inevitable to eventually make IoT devices part of the blockchain network to address the need for everything connectivity between vehicles, users, and the surrounding. However, this relies on the upcoming technical developments of more powerful IoT devices and lightweight blockchain solutions. This discord between needed everything-connection to advance car sharing and the immaturity of existing blockchain and IoT technology makes it challenging to evolve a blockchain and IoT interoperability towards an industry-ready solution. This results in the need of gathering various stakeholders from different industries (e.g., OEMs, blockchain, and IoT experts) within a consortium to best drive the development of a blockchain-based car sharing platform. As it comes to light that a blockchain-based platform may not only benefit car sharing but many other mobility services, it can be assumed that the ultimate goal of gathering such a consortium is the development of a multimodal platform and network in the fashion of MaaS instead of solely delimiting it to car sharing. The current development of a decentralized transportation network by the consortium DAV may be seen as the first step towards this respective goal.

Car sharing is expected to remain of significant relevance for the environment and society. Nevertheless, its economic growth relies on the further development of innovative concepts concerning technology and business models in which OEMs will play a significant role. Blockchain as one possible technology can be seen as one cause of thought for OEMs to collaborate with other stakeholders to not only advance car sharing but also support the transformation of the entire automotive industry to shift from the car as a product to car as a service. Regardless, blockchain alone will not be the only technical solution for taking car sharing to the next level. After all, the visible shift from sole hardware to digital solution provider shows that OEMs are well aware of the need to Uber themselves before they get Kodaked.

Bibliography

Asuquo, P., Ogah, C., Hathal, W., & Bao, S. (2020). Blockchain Meets Cybersecurity: Security, Privacy, Challenges, and Opportunity. In *Studies in Big Data* (pp. 115–127). https://doi.org/10.1007/978-981-13-8775-3_5

Ballús-Armet, I., Shaheen, S. A., Clonts, K., & Weinzimmer, D. (2014). Peer-to-Peer Carsharing. In *Transportation Research Record: Journal of the Transportation Research Board* (Vol. 2416, Issue 1, pp. 27–36). https://doi.org/10.3141/2416-04

Bardhi, F., & Eckhardt, G. M. (2012). Access-Based Consumption: The Case of Car Sharing. In *Journal of Consumer Research* (Vol. 39, Issue 4, pp. 881–898). https://doi.org/10.1086/666376

Baskerville, R., & Pries-Heje, J. (2010). Explanatory Design Theory. In *Business & Information Systems Engineering* (Vol. 2, Issue 5, pp. 271–282). https://doi.org/10.1007/s12599-010-0118-4

Belk, R. (2010). Sharing. In *Journal of Consumer Research* (Vol. 36, Issue 5, pp. 715–734). https://doi.org/10.1086/612649

Bossauer, P., Neifer, T., Pakusch, C., & Staskiewicz, P. (2019). *Using Blockchain in Peer-to-Peer Carsharing to Build Trust in the Sharing Economy*. 14th international Conference on Wirtschaftsinformatik.

Buckler, C. (2020). *An Introduction to REST and RESTful APIs*. SitePoint. Retrieved April, 23, 2020, from https://www.sitepoint.com/developers-rest-api/

Burghard, U., & Dütschke, E. (2019). Who wants shared mobility? Lessons from early adopters and mainstream drivers on electric carsharing in Germany. In *Transportation Research Part D: Transport and Environment* (Vol. 71, pp. 96–109). https://doi.org/10.1016/j.trd.2018.11.011

Chen, T. D., & Kockelman, K. M. (2016). Carsharing's life-cycle impacts on energy use and greenhouse gas emissions. In *Transportation Research Part D: Transport and*

Environment (Vol. 47, pp. 276–284). https://doi.org/10.1016/j.trd.2016.05.012

Chen, Y. (2009). Possession and Access: Consumer Desires and Value Perceptions Regarding Contemporary Art Collection and Exhibit Visits. In *Journal of Consumer Research* (Vol. 35, Issue 6, pp. 925–940). https://doi.org/10.1086/593699

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. In *IEEE Access* (Vol. 4, pp. 2292–2303). https://doi.org/10.1109/access.2016.2566339

Collins, K. (2018). *A running list of websites and apps that have banned, blocked, deleted, and otherwise dropped white supremacists*. QZ. Retrieved March, 20, 2020, from https://qz.com/1055141/what-websites-and-apps-have-banned-neonazis-and-white-supremacists/

Copel, N., & Ater, T. (2017). *DAV White Paper*. DAV Foundation. Retrieved April, 30, 2020, from https://dav.network/whitepaper.pdf

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R. C., Michelin, R. A., Zorzo, A. F., & Kanhere, S. S. (2020). Blockchain Technologies for IoT. In *Studies in Big Data* (pp. 55–89). https://doi.org/10.1007/978-981-13-8775-3_3

Denzin, N. K., & Lincoln, Y. S. (2011). Introduction: The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research* (Vol. 4, pp. 1–19). Sage.

Docker. (2013). *What is a Container? | Docker*. Docker. Retrieved March, 29, 2020, from https://www.docker.com/resources/what-container

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2019). A Blockchain-based Solution to Automotive Security and Privacy. In *Blockchain for Distributed Systems Security* (pp. 95–116). https://doi.org/10.1002/9781119519621.ch5

Ellis, T., & Levy, Y. (2009). Towards a Guide for Novice Researchers on Research Methodology: Review and Proposed Methods. In *Proceedings of the 2009 InSITE Conference*. https://doi.org/10.28945/3325

EU Parliament News. (2019, April 18). *CO2 emissions from cars: facts and figures*. Europa.eu. Retrieved May, 6, 2020, from https://www.europarl.europa.eu/news/en/headlines/society/20190313STO31218/co2-emissions-from-cars-facts-and-figures-infographics

Fakhri, D., & Mutijarsa, K. (2018). Secure IoT Communication using Blockchain Technology. In *2018 International Symposium on Electronics and Smart Devices (ISESD)*. https://doi.org/10.1109/isesd.2018.8605485

Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. In *IEEE Access* (Vol. 7, pp. 103059–103079). https://doi.org/10.1109/access.2019.2931173

Fraga-Lamas, P., & Fernandez-Carames, T. M. (2019). A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. In *IEEE Access* (Vol. 7, pp. 17578–17598). https://doi.org/10.1109/access.2019.2895302

Fraiberger, S. P., & Sundararajan, A. (2017). Peer-to-Peer Rental Markets in the Sharing Economy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2574337

Freenove. (2020). *Freenove/Freenove_RFID_Starter_Kit_for_Raspberry_Pi*. GitHub. Retrieved March, 18, 2020, from https://github.com/Freenove/Freenove_RFID_Starter_Kit_for_Raspberry_Pi

Gatteschi, V., Lamberti, F., & Demartini, C. (2020). Blockchain Technology Use Cases. In *Studies in Big Data* (pp. 91–114). https://doi.org/10.1007/978-981-13-8775-3_4

Goldkuhl, G. (2012). Design Research in Search for a Paradigm: Pragmatism Is the Answer. In *Communications in Computer and Information Science* (pp. 84–95). https://doi.org/10.1007/978-3-642-33681-2_8

Google. (2019). *Building hybrid blockchain/cloud applications with Ethereum and Google Cloud | Google Cloud Blog*. Google Cloud Blog. Retrieved April, 27, 2020, from https://cloud.google.com/blog/products/data-analytics/building-hybrid-blockchain-cloud-applications-with-ethereum-and-google-cloud

Gösele, M., & Sandner, P. (2019). Analysis of blockchain technology in the mobility sector. In *Forschung im Ingenieurwesen* (Vol. 83, Issue 4, pp. 809–816). https://doi.org/10.1007/s10010-019-00315-y

Gregor, S., & Jones, D. (2007). The Anatomy of a Design Theory. In *Journal of the Association for Information Systems* (Vol. 8, Issue 5, pp. 312–335). https://doi.org/10.17705/1jais.00129

Gregory, R. W., & Muntermann, J. (2011). *Theorizing in design science research: inductive versus deductive approaches*. *25*(3). Retrieved May, 5, 2020, from https://aisel.aisnet.org/icis2011/proceedings/engagedscholarship/2/

Guhathakurta, R. (2018). Blockchain in Automotive Domain. In *The Age of Blockchain: A Collection of Articles*. IndraStra Global.

Guyader, H., & Piscicelli, L. (2019). Business model diversification in the sharing economy: The case of GoMore. In *Journal of Cleaner Production* (Vol. 215, pp. 1059–1069). https://doi.org/10.1016/j.jclepro.2019.01.114

Hang, L., & Kim, D.-H. (2019). Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors* , *19*(10). https://doi.org/10.3390/s19102228

Happ, D., Karowski, N., Menzel, T., Handziski, V., & Wolisz, A. (2017). Meeting IoT platform requirements with open pub/sub solutions. In *Annals of Telecommunications* (Vol. 72, Issues 1-2, pp. 41–52). https://doi.org/10.1007/s12243-016-0537-4

Hawlitschek, F., Notheisen, B., & Teubner, T. (2020). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. In *Electronic Commerce Research and Applications* (Vol. 40, p. 100935). https://doi.org/10.1016/j.elerap.2020.100935

Hevner, A. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, *19*(2). Retrieved April, 20, 2020, from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1017&context=sjis&httpsredir=1&referer=

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. In *MIS Quarterly* (Vol. 28, Issue 1, p. 75). https://doi.org/10.2307/25148625

Hinkeldein, D., Schoenduwe, R., Graff, A., & Hoffmann, C. (2015). Who Would Use Integrated Sustainable Mobility Services – And Why? In *Sustainable Urban Transport* (pp. 177–203). https://doi.org/10.1108/s2044-994120150000007019

Hirson, R. (2015). *The Future Of Car Leasing Is As Easy As Click, Sign, Drive | DocuSign Blog*. DocuSign Blog. Retrieved March, 10, 2020, from https://www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive/

HiveMQ. (2019). *Enabling the Connected Car with HiveMQ*. HiveMQ. Retrieved March, 5, 2020, from https://www.hivemq.com/downloads/hivemq-enabling-the-connected-car.pdf

Hyperledger. (2019). *Hyperledger Fabric* (Version release-1.4). Linux Foundation. Retrieved February, 20, 2020, from https://hyperledger-fabric.readthedocs.io/en/release-1.4/whatis.html

Hyperledger White Paper Working Group. (2018). *An Introduction to Hyperledger*. Linux Foundation. Retrieved February, 27, 2020, from https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf

Iivari, J., & Venable, J. R. (2009). *Action research and design science research - Seemingly similar but decisively dissimilar*. 17th European Conference on Information Systems, ECIS 2009, Verona, Italy. Retrieved, April 28, 2020, from https://www.researchgate.net/publication/221407297_Action_research_and_design_science_research_-_Seemingly_similar_but_decisively_dissimilar

IOTA Foundation. (2020). *IOTA overview*. IOTA Foundation. Retrieved April, 5, 2020, from https://docs.iota.org/docs/getting-started/0.1/introduction/overview

Johnson, M. D., Herrmann, A., & Huber, F. (1998). Growth through Product-Sharing Services. In *Journal of Service Research* (Vol. 1, Issue 2, pp. 167–177). https://doi.org/10.1177/109467059800100206

JSON. (2020). *Introducing JSON*. Json.org. Retrieved March, 16, 2020, from https://www.json.org/json-en.html

Ke, H., Chai, S., & Cheng, R. (2019). Does car sharing help reduce the total number of vehicles? In *Soft Computing* (Vol. 23, Issue 23, pp. 12461–12474). https://doi.org/10.1007/s00500-019-03791-0

Klein, N. J., & Smart, M. J. (2017). Millennials and car ownership: Less money, fewer cars. In *Transport Policy* (Vol. 53, pp. 20–29). https://doi.org/10.1016/j.tranpol.2016.08.010

Klems, M., Eberhardt, J., Tai, S., Härtlein, S., Buchholz, S., & Tidjani, A. (2017). Trustless Intermediation in Blockchain-Based Decentralized Service Marketplaces. In *Service-Oriented Computing* (pp. 731–739). https://doi.org/10.1007/978-3-319-69035-3_53

Lee, J. S., Pries-Heje, J., & Baskerville, R. (2011). Theorizing in Design Science Research. In *Service-Oriented Perspectives in Design Science Research* (pp. 1–16). https://doi.org/10.1007/978-3-642-20633-7_1

Le Vine, S., & Polak, J. (2019). The impact of free-floating carsharing on car ownership: Early-stage findings from London. In *Transport Policy* (Vol. 75, pp. 119–127). https://doi.org/10.1016/j.tranpol.2017.02.004

Le Vine, S., Zolfaghari, A., & Polak, J. (2014). *Carsharing: Evolution, Challenges and Opportunities*. European Automobile Manufacturers Association. Retrieved March, 2, 2020, from https://www.acea.be/uploads/publications/SAG_Report_-_Car_Sharing.pdf

Liao, F., Molin, E., Timmermans, H., & van Wee, B. (2019). Consumer preferences for business models in electric vehicle adoption. In *Transport Policy* (Vol. 73, pp. 12–24). https://doi.org/10.1016/j.tranpol.2018.10.006

Lieber, R. (2012). Share a Car, Risk Your Insurance. *New York Times*. Retrieved March, 3, 2020, from https://www.nytimes.com/2012/03/17/your-money/auto-insurance/enthusiastic-about-car-sharing-your-insurer-isnt.html

Liu, H., Han, D., & Li, D. (2020). Fabric-iot: A Blockchain-Based Access Control System in IoT. In *IEEE Access* (Vol. 8, pp. 18207–18218). https://doi.org/10.1109/access.2020.2968492

Machado, C., de Salles Hue, N., Berssaneti, F., & Quintanilha, J. (2018). An Overview of Shared

Mobility. In *Sustainability* (Vol. 10, Issue 12, p. 4342). https://doi.org/10.3390/su10124342

Madhusudan, A., Symeonidis, I., Mustafa, M., Zhang, R., & Preneel, B. (2019). SC2Share: Smart Contract for Secure Car Sharing. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0007703601630171

McLaren, D., & Agyeman, J. (2015). *Sharing Cities: A Case for Truly Smart and Sustainable Cities*. MIT Press. https://books.google.com/books/about/Sharing_Cities.html?hl=&id=KhvLCgAAQBAJ

Mikula, T., & Jacobsen, R. H. (2018). Identity and Access Management with Blockchain in Electronic Healthcare Records. In *2018 21st Euromicro Conference on Digital System Design (DSD)*. https://doi.org/10.1109/dsd.2018.00008

MOBI. (2017). *MOBI – mobility open blockchain initiative*. Dlt.mobi. Retrieved April, 22, 2020, from https://dlt.mobi/

Mohanty, D. (2018). *Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity*. Apress. https://play.google.com/store/books/details?id=1Lx1DwAAQBAJ

Müller, R. M., & Thoring, K. (2011). Understanding Artifact Knowledge in Design Science: Prototypes and Products as Knowledge Repositories. *Seventeenth Americas Conference on Information Systems*, 9. Retrieved April, 26, 2020, from http://aisel.aisnet.org/amcis2011_submissions/216

Münzel, K., Boon, W., Frenken, K., Blomme, J., & van der Linden, D. (2020). Explaining carsharing supply across Western European cities. In *International Journal of Sustainable Transportation* (Vol. 14, Issue 4, pp. 243–254). https://doi.org/10.1080/15568318.2018.1542756

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved February, 24, 2020, from https://bitcoin. org/bitcoin.pdf

Newcomer, E. (2017). *Uber starts charging what it thinks youre willing to pay*. Bloomberg.

Retrieved March, 20, 2020, from https://www.bloomberg.com/news/articles/2017-05-19/uber-s-future-may-rely-on-predicting-how-much-you-re-willing-to-pay

Niehaves, B., & Ortbach, K. (2016). The inner and the outer model in explanatory design theory: the case of designing electronic feedback systems. In *European Journal of Information Systems* (Vol. 25, Issue 4, pp. 303–316). https://doi.org/10.1057/ejis.2016.3

Oaken. (2020). *Oaken Innovation Verticals*. Oakeninnovations.com. Retrieved February, 17, 2020, from https://www.oakeninnovations.com/verticals

Paundra, J., Rook, L., van Dalen, J., & Ketter, W. (2017). Preferences for car sharing services: Effects of instrumental attributes and psychological ownership. In *Journal of Environmental Psychology* (Vol. 53, pp. 121–130). https://doi.org/10.1016/j.jenvp.2017.07.003

Pavithran, D., Shaalan, K., Al-Karaki, J. N., & Gawanmeh, A. (2020). Towards building a blockchain framework for IoT. In *Cluster Computing*. https://doi.org/10.1007/s10586-020-03059-5

Peck, J., & Shu, S. B. (2018). Psychological Ownership and Consumer Behavior. In *Psychological Ownership and Consumer Behavior* (pp. E1–E1). https://doi.org/10.1007/978-3-319-77158-8_16

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research. In *European Journal of Information Systems* (Vol. 27, Issue 2, pp. 129–139). https://doi.org/10.1080/0960085x.2018.1458066

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. In *Journal of Management Information Systems* (Vol. 24, Issue 3, pp. 45–77). https://doi.org/10.2753/mis0742-1222240302

Peniak, P., & Bubenikova, E. (2019). Validation of IoT secure communication gateway for constrained devices. In *2019 International Conference on Applied Electronics (AE)*.

https://doi.org/10.23919/ae.2019.8866990

Pfeifle, S., Ley, C., Tauschek, F., & Enderle, P. (2017). *Fleet management in Europe*. Deloitte Consulting GmbH. Retrieved April, 25, 2020, from https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/consumer-and-industrial/cz-fleet-management-in-europe.pdf

Phillips, S. (2019). *Carsharing Market & Growth Analysis 2019*. Movmi.net. Retrieved April, 27, 2020, from https://movmi.net/carsharing-market-growth-2019/?fbclid=IwAR3FzRwofNQEfl2IJ26wyLAAYlhJAu746y1p8h-dlHmZrhi883IraGXc9Wg

Pierre, E. (2019). *NFC Forum - NFC Forum*. NFC Forum. Retrieved May, 4, 2020, from https://nfc-forum.org/

Popov, S. (2018). *The Tangle* (No. 1.4.3). Retrieved March, 7, from https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

Pustišek, M., & Kos, A. (2018). Approaches to Front-End IoT Application Development for the Ethereum Blockchain. In *Procedia Computer Science* (Vol. 129, pp. 410–419). https://doi.org/10.1016/j.procs.2018.03.017

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. In *IEEE Consumer Electronics Magazine* (Vol. 7, Issue 4, pp. 6–14). https://doi.org/10.1109/mce.2018.2816299

Ramachandran, G. S., Wright, K. L., & Krishnamachari, B. (2018). Trinity: A Distributed Publish/Subscribe Broker with Blockchain-based Immutability. *arXiv Preprint arXiv:1807.03110*.

Rathee, P. (2020). Introduction to Blockchain and IoT. In *Studies in Big Data* (pp. 1–14). https://doi.org/10.1007/978-981-13-8775-3_1

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (European Parliament 2016). Retrived April, 24, 2020 from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. In *Future Generation Computer Systems* (Vol. 88, pp. 173–190). https://doi.org/10.1016/j.future.2018.05.046

Sabolev, A. (2019, November 26). *Integrate Hyperledger Fabric with the IOTA Tangle - IOTA*. Medium. Retrived April, 15, 2020 from https://blog.iota.org/integrate-hyperledger-fabric-with-the-iota-tangle-9bc3ac873e82

Saghiri, A. M., HamlAbadi, K. G., & Vahdati, M. (2020). The Internet of Things, Artificial Intelligence, and Blockchain: Implementation Perspectives. In *Studies in Big Data* (pp. 15–54). https://doi.org/10.1007/978-981-13-8775-3_2

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students*. Pearson Education.

Schiller, T., Scheidl, J., & Pottebaum, T. (2017). *Car Sharing in Europe Business Models, National Variations and Upcoming Disruptions*. Deloitte GmbH. Retrived March, 6, 2020 from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-industrial-products/CIP-Automotive-Car-Sharing-in-Europe.pdf

Shaheen, S. A., & Cohen, A. P. (2013). Carsharing and Personal Vehicle Services: Worldwide Market Developments and Emerging Trends. In *International Journal of Sustainable Transportation* (Vol. 7, Issue 1, pp. 5–34). https://doi.org/10.1080/15568318.2012.660103

Shaheen, S., Cohen, A., Chan, N., & Bansal, A. (2020). Sharing strategies: carsharing, shared micromobility (bikesharing and scooter sharing), transportation network companies, microtransit, and other innovative mobility modes. In *Transportation, Land Use, and Environmental Planning* (pp. 237–262). https://doi.org/10.1016/b978-0-12-815167-9.00013-x

Shaheen, S., Mallery, M., & Kingsley, K. (2012). Personal vehicle sharing services in North America. In *Research in Transportation Business & Management* (Vol. 3, pp. 71–81). https://doi.org/10.1016/j.rtbm.2012.04.005

Shaheen, S., Martin, E., & Bansal, A. (2018). *Peer-To-Peer (P2P) carsharing: Understanding early markets, social dynamics, and behavioral impacts*. Retrived March, 2, 2020 from https://escholarship.org/uc/item/7s8207tb

Shaheen, S., Martin, E., & Hoffman-Stapleton, M. (2019). Shared mobility and urban form impacts: a case study of peer-to-peer (P2P) carsharing in the US. In *Journal of Urban Design* (pp. 1–18). https://doi.org/10.1080/13574809.2019.1686350

Shivers, R., Rahman, M. A., & Shahriar, H. (2019). Toward a Secure and Decentralized Blockchain-based Ride-Hailing Platform for Autonomous Vehicles. *arXiv Preprint arXiv:1910.00715*.

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research. In *Lecture Notes in Computer Science* (pp. 381–397). https://doi.org/10.1007/978-3-642-29863-9_28

Sultan, A. (2016). Leasing in the Automobile Industry: Who Lease Cars. In *The International Journal of Applied Economics and Finance* (Vol. 10, Issue 1, pp. 14–20). https://doi.org/10.3923/ijaef.2016.14.20

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. "O'Reilly Media, Inc." https://books.google.com/books/about/Blockchain.html?hl=&id=RHJmBgAAQBAJ

Tashakkori, A., & Teddlie, C. (2003). *Handbook of Mixed Methods in Social & Behavioral Research*. SAGE. https://books.google.com/books/about/Handbook_of_Mixed_Methods_in_Social_Beha.html?hl=&id=F8BFOM8DCKoC

Thantharate, A., Beard, C., & Kankariya, P. (2019). CoAP and MQTT Based Models to Deliver Software and Security Updates to IoT Devices over the Air. In *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and*

Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). https://doi.org/10.1109/ithings/greencom/cpscom/smartdata.2019.00183

Toyota Research Institute. (2017). *Toyota Research Institute Explores Blockchain Technology for Development of New Mobility Ecosystem | Toyota Canada*. Toyota Canada Newsroom. Retrived March, 1, 2020 from https://media.toyota.ca/releases/toyota-research-institute-explores-blockchain-technology-for-development-of-new-mobility-ecosystem

UNISDR. (2015). *Monitoring and evaluation framework*. Undrr.org. Retrived April, 27, 2020 from https://www.undrr.org/publication/monitoring-and-evaluation-framework

Valastin, V., Kost'al, K., Bencel, R., & Kotuliak, I. (2019). Blockchain Based Car-Sharing Platform. In *2019 International Symposium ELMAR*. https://doi.org/10.1109/elmar.2019.8918650

van Rijmenam, M. (2019, June 24). *Why We Need End-to-End Quantum-Resistant Encryption*. Medium. Retrived March, 17, 2020 from https://medium.com/@markvanrijmenam/why-we-need-end-to-end-quantum-resistant-encryption-3fe08c45d026

Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. In *European Journal of Information Systems* (Vol. 25, Issue 1, pp. 77–89). https://doi.org/10.1057/ejis.2014.36

Voshmgir, S. (2019). *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy*. https://books.google.com/books/about/Token_Economy.html?hl=&id=-Wp3xwEACAAJ

Wahlstrom, J., Skog, I., & Handel, P. (2017). Smartphone-Based Vehicle Telematics: A Ten-Year Anniversary. In *IEEE Transactions on Intelligent Transportation Systems* (Vol. 18, Issue 10, pp. 2802–2825). https://doi.org/10.1109/tits.2017.2680468

Wang, Y., Yan, X., Zhou, Y., Xue, Q., & Sun, L. (2017). Individuals' Acceptance to Free-Floating Electric Carsharing Mode: A Web-Based Survey in China. In *International Journal of Environmental Research and Public Health* (Vol. 14, Issue 5, p. 476).

https://doi.org/10.3390/ijerph14050476

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1–32. Retrived March, 11, 2020 from https://ethereum.github.io/yellowpaper/paper.pdf

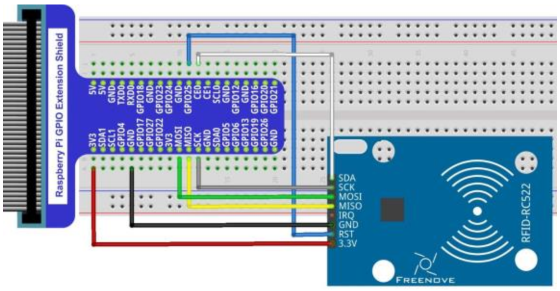
Wörner, D., Von Bomhard, T., Schreier, Y.-P., & Bilgeri, D. (2016). The Bitcoin Ecosystem: disruption beyond financial Services? *ECIS 2016 Proceedings*. Retrived February, 19, 2020 from https://cocoa.ethz.ch/downloads/2016/06/2201_ECIS_Bitcoin_Ecosystem_Final.pdf

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. (2020). A Survey of Distributed Consensus Protocols for Blockchain Networks. In *IEEE Communications Surveys & Tutorials* (pp. 1–1). https://doi.org/10.1109/comst.2020.2969706

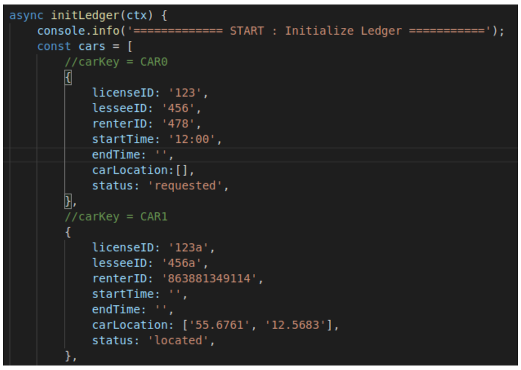
Yuan, Y., & Wang, F.-Y. (2016). Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC).* https://doi.org/10.1109/itsc.2016.7795984

Appendix

Appendix 1: Circuit board taken from Freenove (2020) tutorial

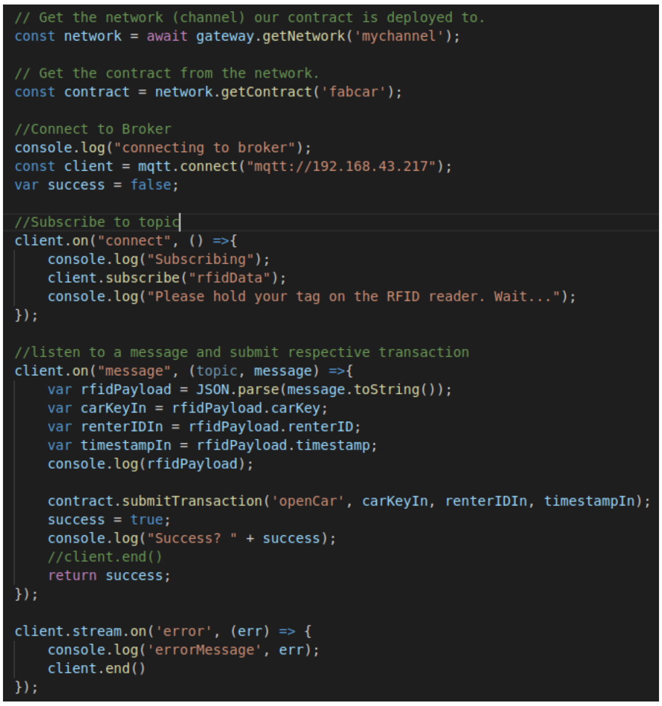


Appendix 2: Snippet of preloaded car objects within init transaction (Most values are dummies except renterID)



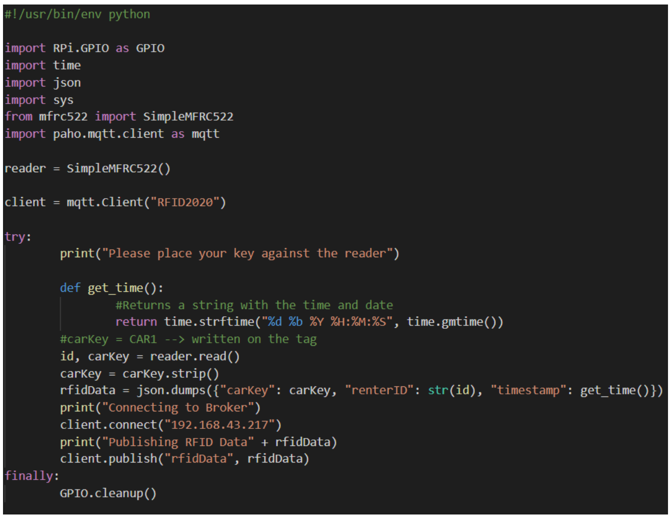
```
async initLedger(ctx) {
    console.info('============= START : Initialize Ledger ==========');
    const cars = [
        //carKey = CAR0
        {
            licenseID: '123',
            lesseeID: '456',
            renterID: '478',
            startTime: '12:00',
            endTime: '',
            carLocation:[],
            status: 'requested',
        },
        //carKey = CAR1
        {
            licenseID: '123a',
            lesseeID: '456a',
            renterID: '863881349114',
            startTime: '',
            endTime: '',
            carLocation: ['55.6761', '12.5683'],
            status: 'located',
        },
```

Appendix 3: Snippet of invoke.js that incorporates the MQTT client and submits the transaction openCar



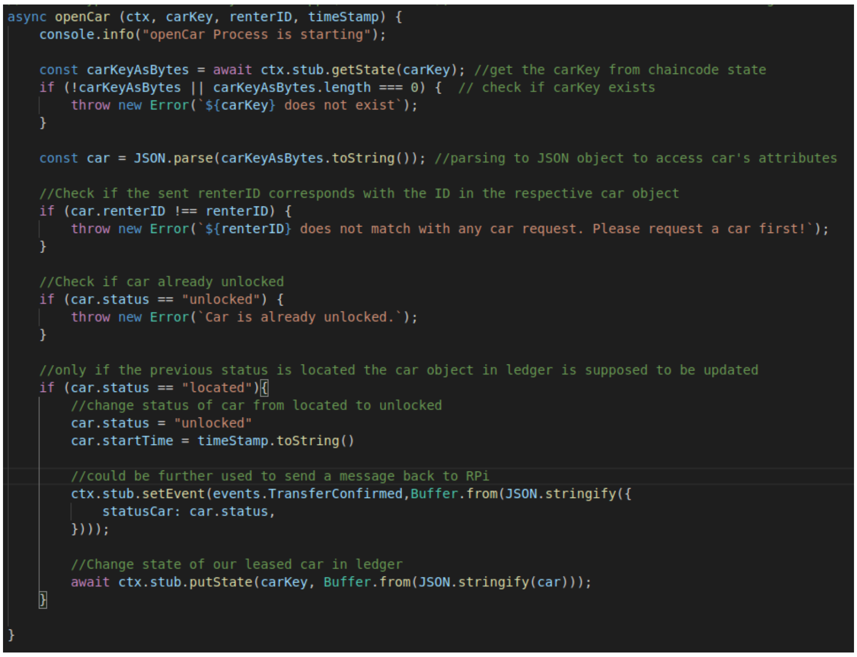
```
// Get the network (channel) our contract is deployed to.
const network = await gateway.getNetwork('mychannel');

// Get the contract from the network.
const contract = network.getContract('fabcar');

//Connect to Broker
console.log("connecting to broker");
const client = mqtt.connect("mqtt://192.168.43.217");
var success = false;

//Subscribe to topic
client.on("connect", () =>{
    console.log("Subscribing");
    client.subscribe("rfidData");
    console.log("Please hold your tag on the RFID reader. Wait...");
});

//listen to a message and submit respective transaction
client.on("message", (topic, message) =>{
    var rfidPayload = JSON.parse(message.toString());
    var carKeyIn = rfidPayload.carKey;
    var renterIDIn = rfidPayload.renterID;
    var timestampIn = rfidPayload.timestamp;
    console.log(rfidPayload);

    contract.submitTransaction('openCar', carKeyIn, renterIDIn, timestampIn);
    success = true;
    console.log("Success? " + success);
    //client.end()
    return success;
});

client.stream.on('error', (err) => {
    console.log('errorMessage', err);
    client.end()
});
```

Appendix 4: Python script read_publish.py collecting and publishing the IoT data



```python
#!/usr/bin/env python

import RPi.GPIO as GPIO
import time
import json
import sys
from mfrc522 import SimpleMFRC522
import paho.mqtt.client as mqtt

reader = SimpleMFRC522()

client = mqtt.Client("RFID2020")

try:
        print("Please place your key against the reader")

        def get_time():
                #Returns a string with the time and date
                return time.strftime("%d %b %Y %H:%M:%S", time.gmtime())
        #carKey = CAR1 --> written on the tag
        id, carKey = reader.read()
        carKey = carKey.strip()
        rfidData = json.dumps({"carKey": carKey, "renterID": str(id), "timestamp": get_time()})
        print("Connecting to Broker")
        client.connect("192.168.43.217")
        print("Publishing RFID Data" + rfidData)
        client.publish("rfidData", rfidData)
finally:
        GPIO.cleanup()
```

Appendix 5: Main transaction of our prototype: unlock car with openCar()



```javascript
async openCar (ctx, carKey, renterID, timeStamp) {
    console.info("openCar Process is starting");

    const carKeyAsBytes = await ctx.stub.getState(carKey); //get the carKey from chaincode state
    if (!carKeyAsBytes || carKeyAsBytes.length === 0) {  // check if carKey exists
        throw new Error(`${carKey} does not exist`);
    }

    const car = JSON.parse(carKeyAsBytes.toString()); //parsing to JSON object to access car's attributes

    //Check if the sent renterID corresponds with the ID in the respective car object
    if (car.renterID !== renterID) {
        throw new Error(`${renterID} does not match with any car request. Please request a car first!`);
    }

    //Check if car already unlocked
    if (car.status == "unlocked") {
        throw new Error(`Car is already unlocked.`);
    }

    //only if the previous status is located the car object in ledger is supposed to be updated
    if (car.status == "located"){
        //change status of car from located to unlocked
        car.status = "unlocked"
        car.startTime = timeStamp.toString()

        //could be further used to send a message back to RPi
        ctx.stub.setEvent(events.TransferConfirmed,Buffer.from(JSON.stringify({
            statusCar: car.status,
        })));

        //Change state of our leased car in ledger
        await ctx.stub.putState(carKey, Buffer.from(JSON.stringify(car)));
    }

}
```