Towards Blockchain-IoT Based Shared Mobility

Car-sharing and Leasing as a Case Study

Auer, Sophia; Nagler, Sophia; Mazumdar, Somnath ; Mukkamala, Raghava Rao

Document Version
Final published version

Published in:
Journal of Network and Computer Applications

DOI:
10.1016/j.jnca.2021.103316

Publication date:
2022

Journal of Network and Computer Applications 200 (2022) 103316

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case study

Sophia Auer [a], Sophia Nagler [a], Somnath Mazumdar [a], Raghava Rao Mukkamala [a,b,*]

[a] Center for Business Data Analytics, Department of Digitalization, Copenhagen Business School, Howitzvej 60, 2000 Frederiksberg, Denmark
[b] Department of Technology, Kristiania University College, Oslo, Norway

ARTICLE INFO

Keywords:
Blockchain
Car-sharing
Car-leasing
Distributed ledger technologies
Hyperledger fabric
Internet-of-things
Shared mobility

ABSTRACT

The shared mobility concept is seen as disruptive and transformative for the automotive industry. Shared mobility is changing the way we choose our travel mode, from just owning a car to e-hailing, car-sharing, and other relevant mobility solutions. There is a growing interest of car manufacturers (original equipment manufacturers or OEMs) in car-sharing as an expansion strategy. Similarly, blockchain technology is seen as another disruptive technology, which can potentially change how the data is stored and accessible via its immutable, transparent, and trustworthy features. Motivated by these two current trends, this paper aims to explore how blockchain and IoT technologies together can drive shared mobility forward. We have presented a high-level architecture for a blockchain-IoT-based platform for promoting shared mobility combining car-sharing and car-leasing. We also demonstrated a prototype implemented from the OEM's point of view by developing a blockchain-IoT-based platform streamlining car-sharing and leasing processes by taking into consideration of primary stakeholders (such as OEMs, a peer-to-peer car-sharing provider, leasing company and insurance provider as well as public authorities). This work also demonstrates that the design of such an integrated platform depends on the right balance between the key design principles (such as security and privacy, authenticity, traceability and reliability, scalability, and interoperability) in the context of car-sharing platforms.

1. Introduction

Nowadays, shared mobility (Burghard and Dütschke, 2019; Machado et al., 2018) is seen as an efficient, cost-effective alternative, and environment-friendly mode of transportation for traveling/commuting. However, many citizens owning multiple cars not only congest the roads but also pollute the environment. In particular, passenger cars are a significant polluter, accounting for almost 60.7% of total CO2 emissions from road transportation in Europe (EU Parliament News, 2019). In recent years, the concept of shared mobility is gaining momentum, reaching the market value of more than 60 billion US dollars and continuing to grow by about 20% in the coming years (McKinsey Center for Future Mobility, 2020). There is a growing voice to reduce the number of personal cars on the streets, freeing up parking space and streets to create green spaces and other infrastructure, thus enhancing citizens' quality of life, in general.

Car-sharing has gained powerful traction with its promise to satisfy individualized transportation demand more sustainably by decreasing the need for passenger cars leading to a potential reduction of emissions (Chen and Kockelman, 2016; Shaheen and Cohen, 2013). Furthermore, 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 et al., 2015). It is claimed that roughly ten cars could be replaced by one car-sharing.[1] Additionally, shared mobility offers new opportunities to the automotive sector, especially in the car manufacturing sector in terms of technology, both software, and hardware.

The car manufacturers, such as BMW and Volkswagen, etc., are hereafter referred to as Original Equipment Manufacturers (OEMs). The OEMs have started to invest in car-sharing due to their strategic shifts from the traditional business model to reduce the carbon footprint and become sustainable and more environmentally friendly. So naturally,

* Corresponding author at: Center for Business Data Analytics, Department of Digitalization, Copenhagen Business School, Howitzvej 60, 2000 Frederiksberg, Denmark.
E-mail addresses: sophia.auer@gmail.com (S. Auer), so.nagler@icloud.com (S. Nagler), sma.digi@cbs.dk (S. Mazumdar), rrm.digi@cbs.dk (R.R. Mukkamala).
URL: https://www.cbs.dk/en/staff/rrmdigi (R.R. Mukkamala).

[1] As indicated by a Product Manager from BMW.

https://doi.org/10.1016/j.jnca.2021.103316
Received 22 April 2021; Received in revised form 20 October 2021; Accepted 16 December 2021
Available online 6 January 2022

the OEMs are in a favorable position to contribute to the growing trend of shared mobility due to their resources and domain expertise. While still being able to give the customer the feeling of owning (i.e., psychological ownership) (Paundra et al., 2017; Peck and Shu, 2018), car leasing also gained importance due to support from the movement away from car ownership (Pfeifle et al., 2017). There is a growing awareness among OEMs to reduce their carbon footprint while earning profits. However, OEMs have to continue the innovation to take car-sharing to the next level (Deloitte, 2017).

With better traceability and transparency of information, blockchain technology is promised to strengthen trust and collaboration among businesses, consumers, and even vehicles (Gösele and Sandner, 2019) which can also help to move forward various mobility services in the automotive industry. Furthermore, blockchain is considered to be beneficial for IoT applications due to its ability to improve fault tolerance, secure data storage, and trusted authentication (Pavithran et al., 2020; Reyna et al., 2018). Today's cars are moving data centers with on-board Internet-of-Things (IoT) sensors and computing units that gather information about the vehicle (Dorri et al., 2019). These technological improvements make the cars a complex amalgamation of complex automobile hardware with software and complex IoT devices to provide various services. The current technological advancements (such as the built-in telematics[2]) makes car sharing/leasing easier, efficient as well as economical (offering a pay-as-you-go based billing model). Apart from that, travelers can also have preferences about the car models. In other words, shared mobility provides a new business/service model, improved user satisfaction, and environmental benefits.

However, there are specific challenges in the car-sharing and leasing platforms regarding both transparency and trust. For example, in the case of the private ownership of cars, the only stakeholder is the car owner. On the other hand, the car-sharing and leasing platform involves several stakeholders such as OEM, leasing company, insurance company, renter, and lessee. Of course, the roles of these stakeholders might vary based on the use cases. Still, whatever may be the use case, there will be several stakeholders involved in the transactions of the platform, which leads to a lot of transparency and trust issues among the stakeholders.

Furthermore, in the case of a centralized car-sharing and leasing platform, the data about car usage and other telematics data is collected and maintained by the stakeholder who maintains the platform, which leads to *information asymmetry* among the stakeholders. Due to this information asymmetry, there will be a lot of transparency and trust issues among the stakeholders, as not all the stakeholders will have the same access to information. Especially in the case of disputes, this lack of transparency of information may lead to many trust issues among the stakeholders, which could be detrimental to the success of car-sharing and leasing platforms. In such scenarios, a decentralized system like blockchain technology can solve many issues. The crucial information that needs to be shared among the partners is stored on a shared ledger that is available to all the stakeholders in a much more transparent and trustworthy way. Here, we have made a case for using blockchain and IoT, which can together be used to create such an ecosystem that goes into the leasing cars enabling keyless access without meeting the car owner.

However, blockchain-IoT integration is very complex (Dedeoglu et al., 2020) due to several challenges such as scalability and non-standardization of blockchain. The growing interest of OEMs in both car-sharing and blockchain serves us as a motivation to explore more in-depth how blockchain may advance the development of car-sharing in the future by designing an IoT-blockchain-based platform combining car-sharing and leasing. Not only in the industry but also the academia has shown interest in the cross-section of car-sharing and blockchain. An increasing amount of publications cover blockchain for the automotive industry (Dorri et al., 2019; Fraga-Lamas and Fernández-Caramés, 2019; Gösele and Sandner, 2019; Guhathakurta, 2018), general sharing economy (Hawlitschek et al., 2018), blockchain in the shared mobility (Shivers et al., 2019; Yuan and Wang, 2016) as well as specifically car-sharing (Bossauer et al., 2019; Madhusudan et al., 2019). However, the focus of existing research lies mainly in the technical implementation or socio-behavioral aspects of blockchain. Most of the works did not consider the interconnection between business and technical implications together with a significant impact on the car-sharing and automotive industry. However, bringing the technical requirements of an IoT-blockchain platform together with its industrial-specific business implications for car-sharing and leasing is missing. Our research work is focused on fulfilling this research gap by addressing the following two research questions.

1. *How can blockchain and IoT platform drive the advancement of car-sharing and leasing?*
2. *Which key design principles will be essential in facilitating such blockchain-IoT based car-sharing and leasing?*

To answer the above research questions, we first explore how blockchain interoperates with IoT to facilitate car-sharing and leasing with the help of a blockchain-based peer-to-peer (P2P) car-sharing platform as a case study. As part of the case study, we have selected a keyless vehicle access control system as a prototype to demonstrate the usefulness of the platform because keyless cars are rented out five times more.[3] The keyless vehicle access control system will emulate the behavior of providing access to a vehicle using a Raspberry Pi (version-3) and a Radio Frequency Identification (RFID) sensor together with Hyperledger Fabric (HLF). Secondly, we explore the role of the five key design principles in facilitating car-sharing using blockchain and IoT. They are security and privacy, authenticity, traceability and reliability, scalability, and interoperability. These principles serve as the foundation of the blockchain-IoT-based car-sharing platform for our work. Nevertheless, the design of the respective platform depends on the right balance between these key design principles. Finally, in this work, we advocate that a blockchain-IoT-based platform can advance car-sharing and car-leasing by facilitating inter-company collaboration and minimizing the need for trust among different stakeholders.

The rest of the paper is organized as follows. In the next section (Section 2), background concepts of our research will be presented, and in Section 3 we will present the related work. Then, in Section 4, we will present our conceptual design and high-level architecture for a blockchain-IoT-based platform and in Section 5 our prototype experimental setup and results will be presented. Next, in Section 6, we will provide a brief discussion on blockchain-based shared mobility and finally conclude in Section 7.

2. Preliminary concepts

In this section, we will describe the background concepts that lay the foundation for our research work.

2.1. Car-sharing and car-leasing

The concept of sharing exists already for quite some time and has its foundation in a sharing or collaborative consumption of resources. It is known as sharing economy or collaborative economy (Shaheen et al., 2020). It is termed shared mobility in the transportation sector. The primary difference between sharing and access to a resource is the perceived/shared sense of ownership. In sharing, ownership and possession of the car are jointly maintained. It is free for all of them

[2] Telematics represents the use of smartphones for data collection referring to services where telecommunications are employed to transmit information provided by sensors in vehicles (vehicle telematics).

[3] As indicated by an employee from https://gomore.dk/.

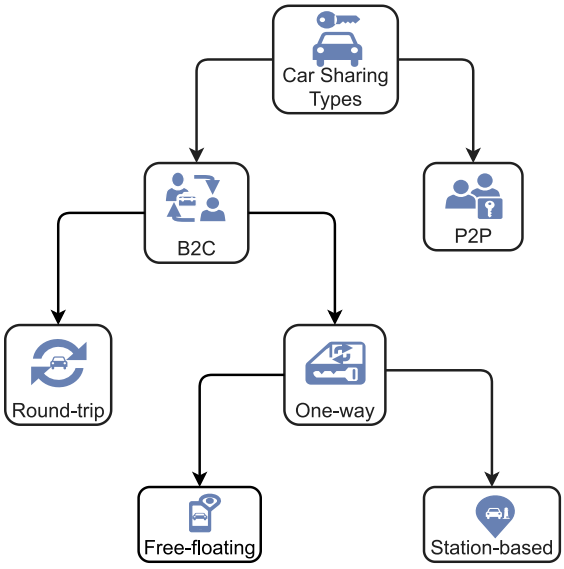

Fig. 1. The representation of two popular types of car-sharing: Business-to-Consumer (B2C) and Peer-to-Peer (P2P).

to use. Therefore, it does not require any monetary compensation, while the responsibilities for the car (e.g., maintenance) are shared jointly (Belk, 2010). In contrast to sharing, in the access mode, there is no transfer of ownership or joint ownership, but the user simply gains access to use the resource (such as a car) (Bardhi and Eckhardt, 2012).

As depicted in Fig. 1, car-sharing can be split broadly into Business-to-Consumer (B2C) and Peer-to-Peer (P2P) models (Münzel et al., 2020). Within B2C car-sharing, the earliest established model is round-trip (Le Vine et al., 2014). More recently, one-way models, including free-floating and station-based, emerged to address especially young adults who seem less interested in owning cars (Klein and Smart, 2017). Besides, the P2P model has been the most recent addition to the overall car-sharing concept. In a one-way system, the cars do not have to be returned to the initial pick-up location. Still, they 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). 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 made by the municipality to manage street space for parking. This challenge depends on the respective city 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 and Polak, 2019).

P2P car-sharing enables privately owned vehicles to be temporarily available for shared use, representing a decentralized car-sharing fleet (Le Vine et al., 2014). Thus, the car owner or lessee (host) can cover the high fixed costs or monthly leasing payment by profiting from the rental transactions with the renters (guests) (Shaheen et al., 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 (not centrally-managed), P2P car-sharing potentially offers a greater selection of pick-up/drop-off locations, vehicle types, and daily/hourly usage prices when compared to the B2C car-sharing (Ballús-Armet et al., 2014). Unlike B2C, 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 privately-owned cars (Shaheen et al., 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 et al., 2012).

However, P2P car-sharing is facing challenges such as insurance liability, lack of trust, expensive technological solutions, assurance of vehicle reliability as well as vehicle availability (Shaheen et al., 2012). For instance, personal vehicle insurances are commonly not valid[4] while a vehicle is rented out. Thus, a P2P car-sharing company has to provide secondary car insurance (Shaheen et al., 2012). A vehicle owner or lessee may still be exposed to some financial liability, especially concerning their insurance premium spikes (Lieber, 2012). Moreover, insurance providers often charge a higher premium (3x to 4x) for a car-sharing provider than the premium for a privately owned car (Le Vine et al., 2014). Thankfully, in-vehicle telematics can be used to assess the risk in a better manner as well as usage of the vehicle by tracking mileage, repairs, and others (Le Vine et al., 2014). User rating, thorough screening, and selection of users, as well as integration with social networks, are some solutions to address the lack of trust issues for a P2P car-sharing provider (Shaheen et al., 2012).

Car dealerships and fleet management firms that offer to lease 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 et al., 1998). Leasing gives the consumer (i.e., lessee) exclusive access to a car for a certain period by paying a fixed monthly rate while not obtaining the ownership of the car (Liao et al., 2019). According to Guyader and Piscicelli (2019), the primary motivation to promote leasing is to move away from ownership, which may lead to greater P2P car-sharing adoption where leasing costs can be shared.

2.2. Blockchain

The concept of blockchain originated in the development of digital currencies as a P2P version of electronic cash. Bitcoin was the first successful decentralized P2P cryptocurrency that bought the innovativeness and disruptiveness of Decentralized Ledger Technologies (DLT) into the limelight (Narayanan and Clark, 2017; Sun Yin et al., 2019). Built on the concept of decentralized and distributed storage systems, blockchain technology can be considered a decentralized data store with state machine replication using P2P protocol, where the transactions are the atomic changes to the stored data, which are grouped into blocks (Mamoshina et al., 2018). The integrity and tamper resistance of the transactional data is guaranteed through the linking of hash values among the blocks. Moreover, the consistency of the transactional states of different distributed nodes is achieved through agreement by the consensus of the majority nodes. 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 in decentralized systems are distributed among the participants, more specifically delegated to the underlying cryptographic protocols and thereby eliminating the need for a trusted intermediary (Klems et al., 2017; Sun Yin et al., 2019). As there are no real trustless systems in the sharing economy (Hawlitschek et al., 2018), a more accurate description could be "distributed trust" that can be seen as more trustful than a *central trust* (Klems et al., 2017). Smart contracts are automatically self-executable code, and they serve as a tool to deploy business logic over decentralized applications (Hawlitschek et al., 2018).

[4] Due to country/company-specific regulations.

The blockchain network is made up of a set of nodes, so-called peers. The access of each user to the network is based on permissions (for permissioned blockchain networks). Each node within the network holds a copy of the ledger, which consists of the world state (essentially the database) and the blockchain. 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. 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 centralized systems. 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. To address this challenge, there are several efficient and faster consensus mechanisms based on the type of requirements, such as public/private and other characteristics. The decentralization of the blockchain architecture can improve the fault tolerance and single point of failure by preventing network bottlenecks (Reyna et al., 2018).

2.3. IoT and blockchain

IoT is a network of things in a physical world. IoT devices are diverse in terms of 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). It has emerged as a set of technologies spanning from Wireless Sensors Networks (WSN) to RFID. IoT devices have limited computing power and capacity to sense, actuate and communicate over the internet with a backend application (Reyna et al., 2018). Current technological evolution results in a smaller size, energy-efficient, and cheaper IoT devices. The sensors or actuators can be placed within the device or attached to it. Smart vehicles are connected to roadside infrastructure (such as vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), vehicle-to-end users (V2P), and generally to everything connected to Internet (V2X)) (Dorri et al., 2019). In car-sharing, keyless authentication to unlock a car and to collect data with telematics (to track safety and driving behavior) can be attributed to the latest advancements in the IoT domain (Fraga-Lamas and Fernández-Caramés, 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 primarily centralized. It leads to limited scalability and imposes trust on a central entity, which raises the need for decentralization with the help of blockchain (Dedeoglu et al., 2020).

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). A blockchain network of interconnected IoT devices can eliminate the use of a central intermediary enabling real-time trustful data transfer. Distributed applications require the IoT devices to collect, process, and exchange an immense amount of privacy-sensitive user data that makes it very critical to protect from cyber-attacks. With current standard protocols used in IoT, it is possible to secure user data with a standard username, and password authentication, as well as encryption on the network (TLS/SSL) or application layer (payload encryption) (Peniak and Bubeníková, 2019). However, it adds significant network overhead resulting in high energy consumption.

In P2P car-sharing, only the rightful user who requested a specific car should be able to open that car. Participants can identify every single device by creating digital twins (i.e., digital copies of physical objects) in a blockchain-based platform while the provided data is immutably stored. Blockchain can also provide trusted distributed authentication as well as authorization for both devices and users using underlying cryptographic mechanisms. Even over time, participants of such a reliable system can verify the authenticity of the data. They can be certain that it has not been manipulated, ensuring the sensor data's traceability and accountability (Reyna et al., 2018).

It needs to be decided how and where the IoT interaction will take place (Reyna et al., 2018) prior to integrating IoT with blockchain. Three alternatives are: within the IoT (IoT-IoT), through the blockchain (IoT-Blockchain), or a hybrid design involving IoT and blockchain. The IoT-IoT approach is recommended if the use case has reliable IoT data with low latency during IoT interaction. Here, only a part of the IoT data is stored on the blockchain, but the IoT interaction itself happens independently. Next, the IoT-blockchain approach ensures that all interactions go through the blockchain, making them traceable but consuming the network bandwidth and delays processing the transactions. Lastly, the hybrid approach mixes 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 (Reyna et al., 2018). Although IoT-blockchain and hybrid approaches seem suited for some applications, the primary challenge remains in the adaptation of blockchain that is suited to embedded IoT devices and gateways with limited resources (Hang and Kim, 2019; Liu et al., 2020; Pavithran et al., 2020; Reyna et al., 2018). There is an increasing number of blockchain integrations (such as Rapsnode (for Bitcoin, Litecoin, and Ethereum) and EthEmbedded (for Ethereum) for Raspberry Pi). However, most embedded devices have too low computing power, limited data storage, and battery which could make them useless (Hang and Kim, 2019).

3. Related work

Car-sharing and blockchain usage have gained both academia as well as industry's research interest. An increasing amount of publications covers blockchain for the shared mobility (Shivers et al., 2019), specifically car-sharing (Bossauer et al., 2019; Madhusudan et al., 2019; Valaštín et al., 2019; Zhou et al., 2020) and car-leasing (Kwame et al., 2018), general sharing economy (Hawlitschek et al., 2018) and automotive industry (Dorri et al., 2019; Fraga-Lamas and Fernández-Caramés, 2019; Gösele and Sandner, 2019; Guhathakurta, 2018). In the industry, Toyota, together with Oaken innovation, has started working on prototypes of a car-sharing and leasing platform that offers a blockchain-enabled digital identity of vehicles and historical data storage (Oakeninnovations.com, 2020). As another example, a software development company[5] is working on an enterprise blockchain system supporting data integrity for the automotive supply chain, transparent vehicle maintenance, and streamlined car-sharing services.

Researchers in Zhou et al. (2020) propose a car-sharing control scheme using blockchain. In this work, many base stations of Internet-of-Vehicles are used to build the blockchain ecosystem (to replace any third-party server). It establishes a secure and tamper-proof car-sharing platform among service providers, vehicle owners, and tenants. It also shows that proposed control procedures can be performed with a delay of seconds using the Ethereum private chain. In Dmitrienko and Plappert (2017) authors present a concept of access control mechanism for the car-sharing system for free-floating cars without requiring an online connection. In this work, the authors deploy a two-factor authentication

[5] https://pixelplex.io/work/blockchain-car-sharing-and-automotive-supply-chain/.

mechanism and combine hardware (similar to RFID cards). The authentication tokens are stored on a mobile platform that also incorporated security features. Dorri et al. (2017) proposed a blockchain and IoT-based architecture to protect the privacy of users and to increase the security of the vehicular ecosystem. Yang et al. (2018) also proposed a blockchain-based trust management scheme for vehicular networks. In this work, the received messages from neighboring vehicles are validated by the Bayesian inference model. Finally, in Rowan et al. (2017), a blockchain-based inter-vehicle communication mechanism (via ultrasonic audio and visible light) was proposed. In this work, the primary use of blockchain was to secure inter-vehicular communication by securely establishing symmetric keys without using continuous radiofrequency or wireless infrastructure support.

Next, Xu et al. (2020) proposed a consortium blockchain-based data market for car-sharing. The proposed blockchain-based platform creates a trusted data trading environment without a centralized intermediary. Here, a smart contract is built-in for executing the pricing and trading logic. The model uses the Stackelberg game among data owners, service providers, and data buyers to obtain an optimal pricing strategy. In the area of round-trip B2B car-sharing, the researchers of Hassija et al. (2019) propose a blockchain-based car rental service with a focus on cost-optimization across multiple stakeholders, especially in case of an accident. Valaštín et al. (2019) developed a short-term car-sharing application based on blockchain. It uses the Ethereum platform to introduce P2P car-sharing services without a central authority. It also claims that replacing central authority costs is reduced, and data transparency has increased. The research work in Bossauer et al. (2019) also proposes blockchain-based P2P car-sharing with a primary focus on trust and privacy.

Similarly, a P2P platform-based solution was proposed in Madhusudan et al. (2019) for secure and private car booking and payments functionality for a car-sharing system. The developed smart contract was deployed in the Ethereum test net to register car-sharing offers, request matching, and settle the transactions. Another research work in Kwame et al. (2018) proposed a blockchain-based car-leasing platform that employs smart contracts to enforce decisions on all transactions and also penalizes the perpetrators. Unlike our work, IoT devices were not used in this work, while smart contracts are used to monitor participants' behavior. A private Ethereum network has been used to implement the car-leasing platform.

Our work tried to bridge the gap between car leasing and car-sharing with the help of blockchain and IoT. However, there is a lack of research integrating IoT with blockchain in the context of shared mobility, especially using Hyperledger Fabric (HLF),[6] while also placing its technical results into a more significant business perspective. Our contribution in this paper is to provide a secure blockchain-IoT platform among untrusted users and lessees combining car-sharing and car-leasing. The proposed blockchain-IoT ecosystem offers effective and efficient business monitoring and provenance of transactions. The HLF-based smart contracts ensure effective monitoring of various types of transactions in the sharing ecosystem.

4. Conceptual design and architecture

The high growth potential of P2P car-sharing due to its network effects and the increasing interest of OEMs in car-sharing leads to the idea of a P2P car-sharing platform initiated by OEMs. The commercial design of a blockchain-based car-sharing platform is complex and extensive. The proposed platform requires secure information sharing among multiple stakeholders (such as user, lessee, and service provider), leading to the decision to choose blockchain for its facilitation. IoT data generated by vehicles is of significant relevance to all involved stakeholders helping to streamline processes and features. However, this leads to the need for a robust and scalable platform that enables a suitable IoT infrastructure and network. According to several research works (Dedeoglu et al., 2020; Hang and Kim, 2019; Pavithran et al., 2020; Reyna et al., 2018), blockchain can address some of these IoT challenges.

In this section, we present the conceptual design and high-level architecture for the proposed case study of a blockchain-based P2P car-sharing and leasing platform. It brings together various stakeholders involved in the car-sharing and leasing process by integrating and streamlining their workflows. In the following, the problem identification and derived five key design principles are explained.

4.1. Requirements and use cases

Our research focuses on how blockchain, combined with IoT devices, can facilitate a seamless P2P car-sharing and leasing experience initiated by OEMs (which is commonly undertaken by a third party platform) (Münzel et al., 2020). 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 et al., 2019; Shaheen et al., 2012). At the same time, leasing in the automotive industry has been growing rapidly in the last few years and has become more attractive to the OEMs to manage the platform by themselves rather 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 and Piscicelli, 2019; Paundra et al., 2017; Peck and 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 and Fernández-Caramés, 2019; Guhathakurta, 2018). Thus, a unified platform-based approach that involves the entire process (such as leasing a car, getting insurance to P2P car-sharing, paying off the leasing fee) could move forward car-sharing as well as leasing.

Whenever a user is interacting with a different car-sharing business, a new digital persona is created, which is disconnected, leading to data silos that do not communicate with each other. There is a need to address the problem of data silos progressively caused by the growing amount of car-sharing providers. This raises costs in the form of reconciliations, lost time, and missing records, resulting in errors, waste of resources, and possible fraud and abuse (Ferdous et al., 2019). For instance, a deceptive user who committed fraud at one car-sharing platform may easily switch the platform and repeat the same behavior without the new platform knowing about their fraudulent history. Finally, the sharing of telematics data is crucial for streamlining the processes of car-sharing and leasing on one platform (Dorri et al., 2019; Gösele and Sandner, 2019). It results in a need for a persistent and scalable IoT infrastructure and network (Dedeoglu et al., 2020; Reyna et al., 2018). Unfortunately, there is a lack of a detailed demonstration integrating IoT with blockchain for such scenarios.

P2P car-sharing process incorporates stakeholders such as OEM, leasing company, insurance company, renter, and lessee. Our assumptions are:

1. the car-dealer role is taken over by the OEM (via direct sales)
2. one or more OEMs are willing to set up the permissioned network and become admin adding the different stakeholders with differed permissions

[6] https://www.hyperledger.org/use/fabric.

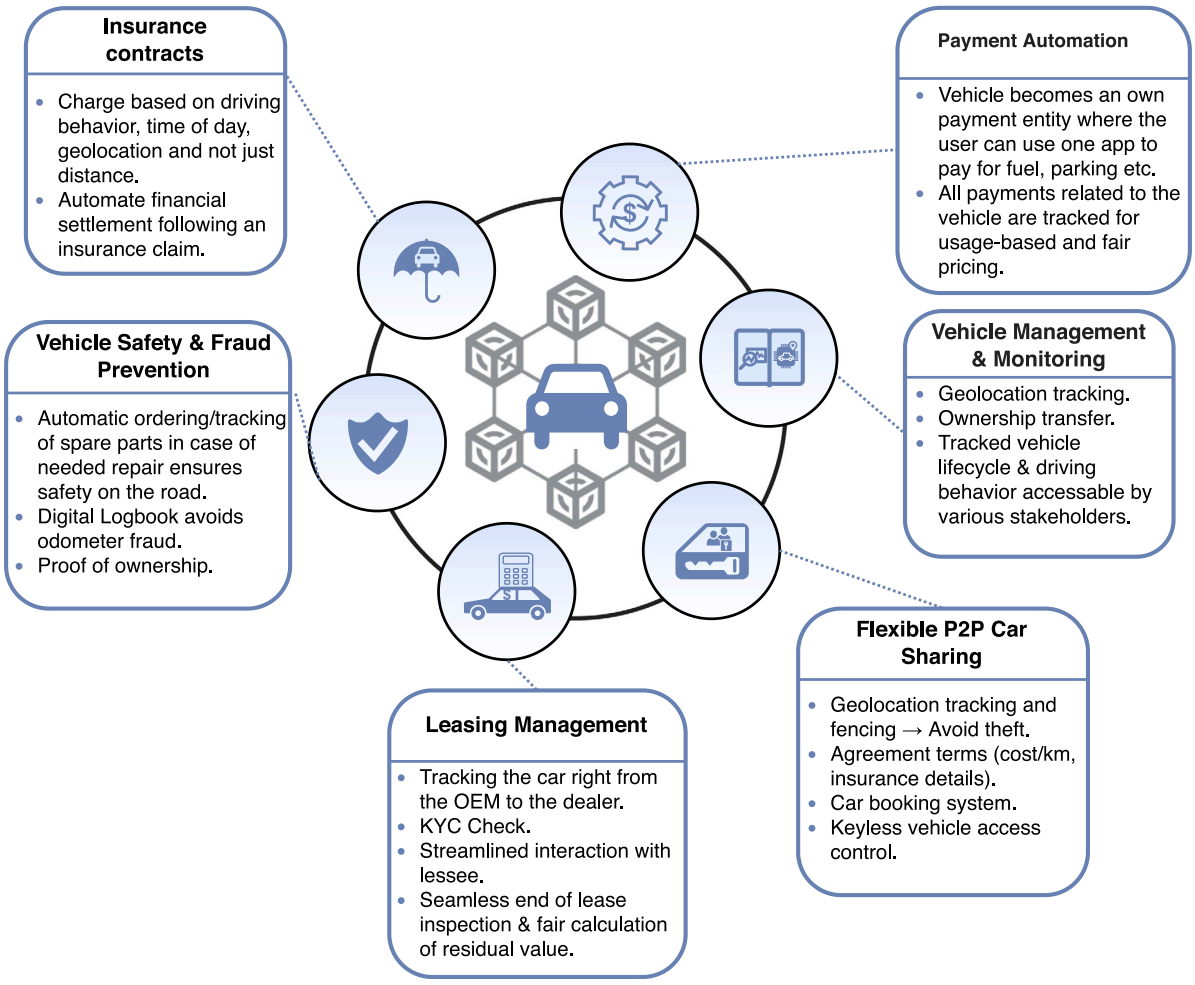

Fig. 2. Overview of use cases enabled by the conceptual design.

3. leasing contract (from leasing company) legally allows each lessee to rent out the respective car via a P2P car-sharing platform.
4. it is assumed that the leasing and insurance companies collaborate. Hence the leasing package includes insurance. Similarly, the leasing company can be both external and internal independent of the OEM.
5. each payment is made through cryptocurrencies.

As shown in Fig. 2, there are six main use cases of our conceptual design: P2P car-sharing, leasing management, vehicle management and monitoring, payment processing/automation, vehicle safety and fraud prevention and finally, insurance contracts. Each use case can be further split into sub-use cases, of which we use *keyless vehicle access control* sub-use case to demonstrate the blockchain-IoT interaction with its associated transactions as a proof-of-concept. To demonstrate the sub-use case, we use *unlock a car* transaction, which is implemented with a Raspberry Pi (representing a car) and RFID sensor (representing the door) based on the high-level architecture involving the Hyperledger Fabric platform.

4.2. Key design principles

The design principles are derived based on our literature review and then evaluated based on the interviews (refer to Section 5.3.2) conducted with respective industry experts from OEMs and other mobility companies.[7] The proposed solution requires meeting five design principles. They are *security* and *privacy*, *authenticity*, *traceability*, *reliability*, *scalability* and *interoperability*. We have used the main findings from the interviews to validate the main key design principles. Fig. 3 shows an overview of the derived key design principle (right) as opposed to its identified problem in car-sharing and leasing (left), as well as current technical problems (middle).

- *Security and Privacy:* Due to the tremendous amount of data exchanged among stakeholders, the platform has to handle private and sensitive user data 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. Besides, the immutability of the data needs to be ensured (Pavithran et al., 2020; Reyna et al., 2018). Finally, a permissioned network with a relevant byzantine-fault tolerant consensus mechanism is needed to ensure that only the participating organizations have access to

[7] Volkswagen (New Business Models & Technology researcher), GoMore (Product Designer & Head of Keyless Product), Bosch (Product Owner DLT Mobility), BMW (Manager Product Strategy Mobility Services), and Frederiksberg Municipality, Denmark (Smart City & Digitalization expert). This disclaimer informs that the views, thoughts, and opinions expressed by the interviewees solely belong to the interviewees and do not necessarily represent the views of the companies/organizations of the interviewees.

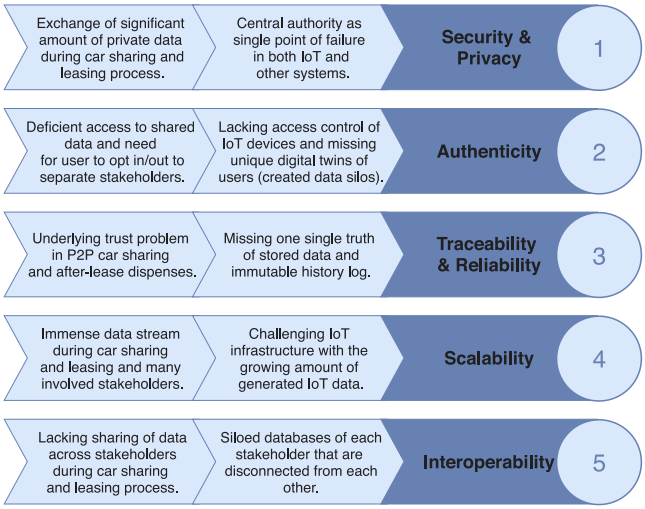

Fig. 3. Overview of problems and key design principles.

the data they need or the data owner is willing to give access to it.

- *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. Every system user needs to be securely identified (with a unique digital identity) by implementing a suitable digital identity management system for all the different services across the platform. Thus, the current problem of duplicate digital personas and data silos created across various platforms can be eliminated (Ferdous et al., 2019).
- *Traceability and 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 and 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). Data from different sources will be shared on the platform, 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 and Sandner, 2019). Furthermore, the recorded data's reliability 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, maintenance, and repairs). It is essential for each participant involved to be certain about the serviced car and its traceability in case of fraud, theft, or damages.
- *Scalability* As the platform aims to incorporate many different participants along with many IoT devices that generate large data streams; there is a need to assess to what extent the IoT interaction takes part within the blockchain to meet the criteria with regards to security, storage, and especially scalability. Consequently, the system and the IoT network have to be scalable even with a large number of participants in the network.
- *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 their own established business logic, which needs to be aligned with each other to be able to collaborate on one platform (Fraga-Lamas and Fernández-Caramés, 2019; Gösele and Sandner, 2019; Guhathakurta, 2018).

4.3. Proposed architecture

Fig. 4 represents our proposed high-level architecture for shared mobility based on blockchain-IoT based platform combining car-sharing and car-leasing. It consists of: *IoT-Physical Domain*, *Connectivity Domain*, *IoT-Blockchain Service Domain*, and *Application Domain*.

4.3.1. IoT Physical Domain

It encapsulates various embedded devices. Usually, vehicles are equipped with a unique digital identity, in-built telematics, storage, computing resources, and communication interfaces. However, in general, IoT devices do not hold strong computing ability and enough storage. Therefore, the IoT devices are unsuitable to be deployed as peer nodes of the blockchain. However, the generated vehicle and real-time data (e.g., driving behavior, telematics) can be securely recorded through the connectivity domain into the blockchain.

4.3.2. Connectivity Domain

The device data is generated and published as a payload to a relevant topic on the Message Queuing Telemetry Transport (MQTT) broker located in the Connectivity Domain. 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, is 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 event within the vehicle through IoT Physical Domain (e.g., unlocking the car after authentication). This time the vehicle subscribes to the registered control topic to receive the message. Overall, the purpose of the Connectivity Domain is to facilitate communication with the blockchain. Since the IoT devices can generate a large stream of data at frequent intervals, the IoT data and events can be aggregated within this domain. In that case, only aggregated results can be sent to the IoT-Blockchain Service Domain as indicated in Zheng et al. (2019) and Christidis and Devetsikiotis (2016).

Moreover, IoT devices and sensors can sometimes malfunction and produce faulty or out-of-sync data. In such cases, advanced machine learning techniques can be used to make sure that the data produced by the IoT devices is valid according to certain validation patterns or checks (Gaddam et al., 2020; Zheng et al., 2018). In such a scenario, the Connectivity Domain will also contain data validation algorithms to validate the input received from various IoT devices and sensors from the IoT Physical Domain.

4.3.3. IoT-Blockchain Service Domain

As the core of the system, the IoT-Blockchain Service Domain exposes Representational State Transfer (REST) APIs to access for users (e.g., short-term renter or lessee) in the Application Domain and for the message brokers in the Connectivity Domain. In other words, all the product-specific services provided by the blockchain network are accessible through RESTful APIs, which can be invoked by either web clients (via Application Domain) or IoT devices (via Connectivity Domain). The IoT-Blockchain Service Domain consists of four sub-domains, namely *Data*, *Network*, *Consensus*, and *Smart Contract*. As a possible scenario, a candidate block is created from transactional data such as IoT sensor data and other relevant information to ensure immutability and security with the appropriate encryption mechanism, time stamping, and suitable hash pointers to the data from the Data sub-domain. Afterwards, the block is broadcasted to the P2P network (in the Network sub-domain). The network consists of all the stakeholders. Each of them gets different permissions and access rights to smart contracts, especially to the ability only to read or write. Even the read permissions are limited to some of the stakeholders. For instance, the short-term renter should not have access to anything related to

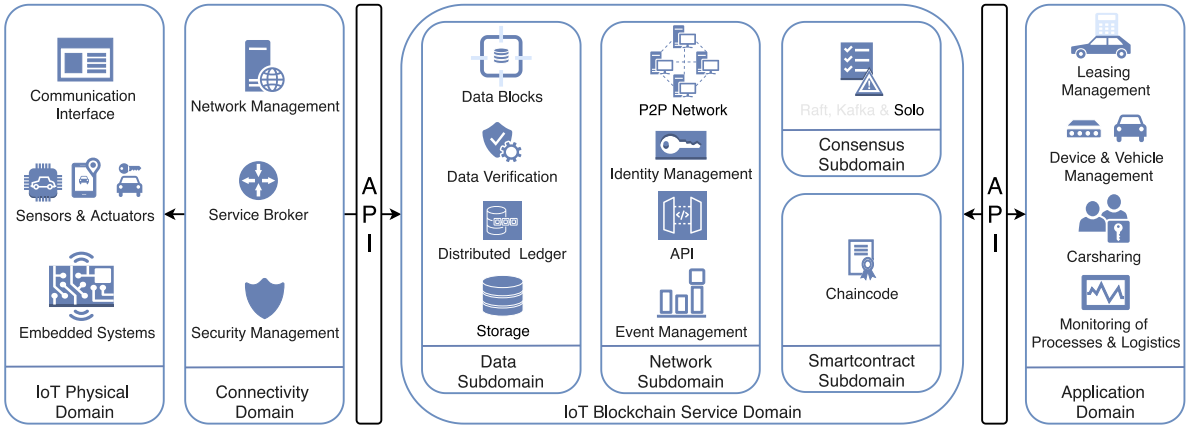

Fig. 4. High-level view of the proposed architecture.

the leasing contract between the lessee and the leasing party. These permissions are defined in the identity management of the network sub-domain 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 blockchain nodes reach a consensus-based on a defined consensus mechanism (in our system, Solo). Once consensus has been reached, the block is ready to be appended to the blockchain and distributed to every node's immutable ledger. The smart contracts are self-verifying, self-executing, and self-enforcing state-response rules that are stored 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. In the proposed architecture, smart contracts are used for different scenarios, from managing vehicles and their real-time data to authorizing the unlocking of a car based on an existing rental request, as shown in Fig. 5. Besides verifying transactions that are triggered by the IoT network, another REST API can expose access to the blockchain coming from the Application Domain.

4.3.4. Application Domain

Application Domain contains all potential scenarios and use cases of the conceptual design. Administrators can add and upgrade smart contracts as well as manage the overall blockchain system. In the proposed architecture, an OEM or a group of OEMs initiate and administer the network. Nevertheless, other stakeholders can receive similar permissions through respective certificates handed out by the OEM. On the other side, the end-user (such as the short-term renter) can send attribute-based authorization requests to the blockchain to register, make a car-sharing request and handle the insurance. Here, we adopted a lightweight solution where the blockchain is used as an external service to provide reliable, immutable, and secure storage and trustful and seamless identity management that may drive the collaboration between different stakeholders of the conceptual design. Thus, the architecture brings a flexible integration between the blockchain layer and the IoT network, including the devices and the gateways. The architecture represents how blockchain can bring together different stakeholders streamlining the leasing and car-sharing processes by recording and executing agreements and financial transactions in an immutable secure, and reliable manner. 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.

4.4. Car-sharing and leasing workflow

Now, we will describe the car-sharing and leasing workflow. It shows how a lessee orders a car via the leasing party and rents out the leased car to a short-term renter to help pay off the leasing fees using our proposed blockchain-IoT platform. As shown in Fig. 5, the workflow presents four main stakeholders together with steps and processes involved in the workflow, including the required registrations and smart contracts. They are a short-term renter (representing the car-sharing renter), lessee, OEM, and leasing party (also the insurance company).

- First, OEMs set up the blockchain network and allow stakeholders to be added. Next, OEM lists all available car models with relevant details (such as car color, model, transmission, motor, extra features, e.g., roadside assistance). Every entity receives a unique digital identity from the certificate authority of the network. 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's licenses).
- A potential lessee can browse the different models and eventually choose a car from other preferences and customizations (refer to step 2 of Fig. 5). The lessee also needs to choose a suited leasing and insurance plan. Securely stored data in the blockchain is made available to only 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 this scenario, the car is listed tentatively and automatically turned into a confirmed listing as soon as the lessee receives the car.
- The smart contract (chaincode in HLF) between the lessee and the leasing entity is triggering a leasing request event on which basis the leasing entity can perform suitable checks (such as Know Your Customer (KYC) check/customer verification) efficiently within the platform. In addition, it requires that the potential lessee provide suitable access to bank history by linking their digital identity with their bank. Once the lease is approved (refer to step 3 of Fig. 5), 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 (refer to step 4a of Fig. 5), 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.

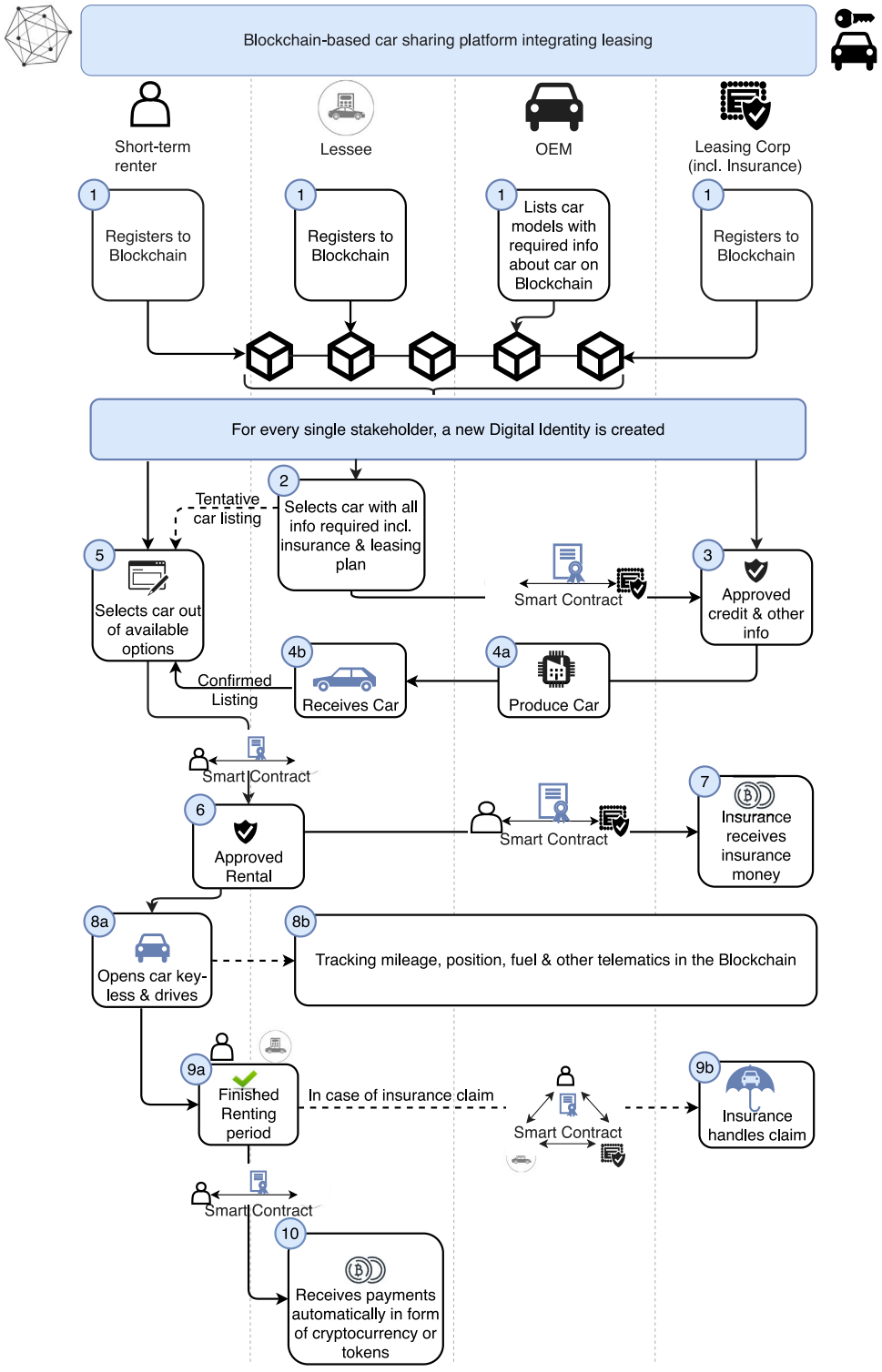

Fig. 5. Detailed architectural workflow of blockchain-based car-sharing platform integrating leasing.

- After a successful background check and production of the respective car, the lessee receives the car (refer to step 4b of Fig. 5). 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 chooses this option). In this case, the lessee can adjust the availability of the car for short-term rental by providing a suitable schedule in which the car is automatically made available for rent. To ensure trust in the platform, the car's mileage, fuel, and other IoT telematics data 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 (refer to step 8b of Fig. 5), it applies to the entire period of the car usage (both leasing and short-term rental (hence as soon as (refer to step 4b of Fig. 5) starts)).
- The short-term renter can now select a car nearby from available options varying in type and time availability (refer to step 5 of

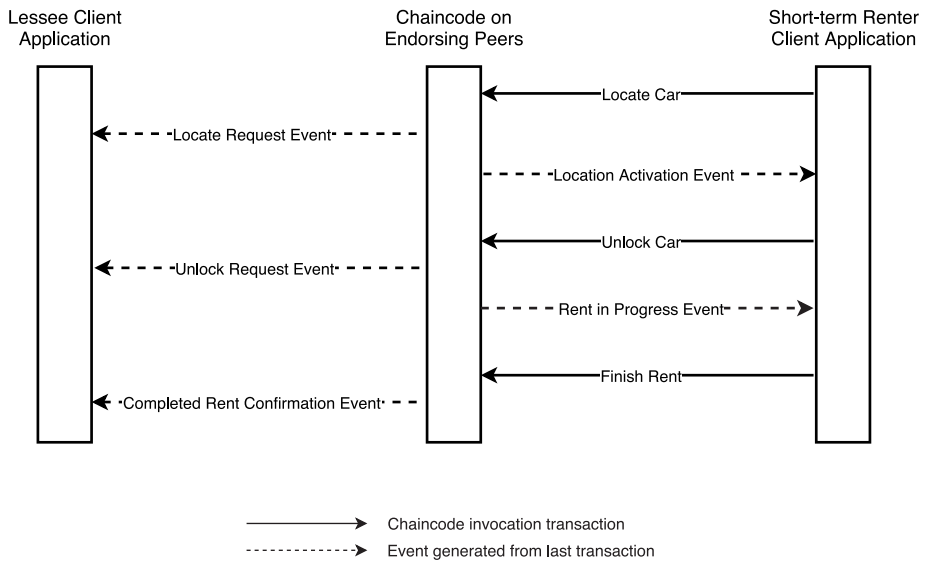

Fig. 6. Transaction flow of keyless vehicle access control.

Fig. 5). The short-term rental includes usage-based insurance, ensuring that both the lessee and short-term renter can be sure of an all-time insured car. Next, a smart contract between the short-term renter and lessee provides the necessary background check to driver licenses and the validity of both parties with the help of their digital identities. Finally, it leads to an approved rental (refer to step 6 of Fig. 5) 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 (refer to step 7 of Fig. 5).

- After the approved rental request, the short-term renter can open the keyless car with a smartphone at the requested time, entering the unique private key and the license number of the respective car (refer to step 8a of Fig. 5). 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 (refer to step 8b of Fig. 5). Beyond the rental duration, the platform will automatically charge the short-term renter a fee for extended driving time.
- After the short-term use renter closes the car with the smartphone, which triggers an event in the blockchain that changes the car's status as being securely closed (refer to step 9a of Fig. 5). All information regarding possible damages 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 an accident, the insurance is automatically notified. It 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 (refer to step 9b of Fig. 5).
- Finally, lessees receive the appropriate payment (as cryptocurrency) for renting out their cars (refer to step 10 of Fig. 5). Payment is also 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 car's status is automatically changed back to available so that it is listed for a new rental.

4.5. Smart contract support

All the relevant business logic and/or rules related to car-sharing and leasing can be incorporated into the smart contracts. The selected scenario between lessee client and short-term renter client is described to demonstrate how smart contracts can facilitate the execution of reusable and pre-defined business logic. The transaction starts after the short-term renter client has sent the rental request and is accepted by the lessee client. We outline the use case, where the smart contract logic is activated by each entity involved and the subsequent events. Three classes are defined, namely *car*, *lessee*, and *short-term renter*. The class car defines the attributes (such as car license number, lessee as well as a renter identification number, renter start and finish time, car location together with car's current status (e.g., whether in use or not)) related to each car registered on the blockchain-IoT network as shown in Table 1.

Table 1
Overview of required attributes of class car.

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

Similarly, 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. The transaction process, shown in Fig. 6, 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 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 smart contracts (or 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 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. Thus, 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. Afterwards, the *car* object is updated to include the location coordinates. 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.
- *Unlock Car*: it is called when the short-term renter physically unlocks the car. 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 rental *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*: it is called when the short-term renter physically ends the rental and the attribute status is changed from *unlocked* to *completed*. The attribute rental end time 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 is 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. Simulation

In this section, we present some of the insights collected from our prototype simulation, which represents a smaller version of blockchain-IoT-based peer-to-peer (P2P) car-sharing platform. We model the transactions of the use case *keyless vehicle access control system* in the car-sharing and leasing processes by duly taking into consideration of all the primary stakeholders.

5.1. Environment setup

We simulate the unlocking of a car by having a Raspberry Pi3 representing the computational unit of the car, an RFID sensor as the car lock, and the RFID tag as the keyless option (which could be a smartphone application as well, refer to Fig. 7). The primary focus is to model the interaction between an IoT device (RFID with RPi3) and the Hyperledger Fabric (HLF). The implementation consists of two main components, a virtual machine (VM) for the HLF network and an RPi3[8] for the connection of the IoT device and broker. The chosen programming language is Python[9] to read the data from the RFID sensor[10] and handle the communication with Message Queuing Telemetry Transport (MQTT) which is a lightweight publish–subscribe

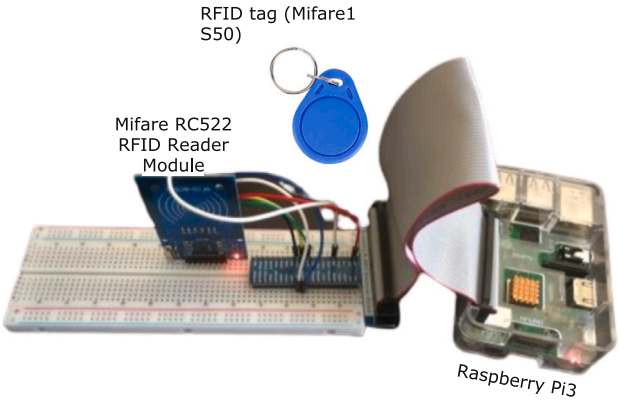

Fig. 7. IoT device setup for experiment.

communication protocol. The RFID reader (with Philips MFRC522 chip) sensor is connected to the RPi3 by using a breadboard (general purpose input/output (GPIO) extension) and jumper wires. Simulating a smartphone, we use an RFID tag (Mifare1 S50 non-standard) held against the sensor.

MQTT is used to facilitate the communication between the IoT device server and the blockchain. For simplicity, the same RPi3 has been used as both the publishing client and the MQTT broker[11] instead of shifting the broker into a cloud service. MQTT is a well-accepted protocol that supports publish/subscribe model. We have deployed the HLF network (v1.4.4 with Node.js fabric-client) on a single VM instance[12] following standard installation procedure. The default ordering service Solo is deployed on the orderer node with CouchDB as the default world state database. We create two users (admin and short-term renter) for the application. Admin is responsible for registering short-term renter as the user who triggers the smart contracts by unlocking the door. The lessee is not implemented since, in our case, they would solely receive event notifications tracking the rental period.

5.2. Application deployment

Application user can invoke a smart contract which queries (reading data) and updates (writing data) the ledger through the smart contract API (e.g., *queryCar* and *openCar*). After deployment, the application can initiate interaction with the ledger by submitting a transaction as shown in Fig. 8. An MQTT broker client is installed on both the RPi3 and the HLF node. The RPi3 as the IoT server publishes the data to the MQTT broker client with topic name as *rfidData* (refer to step 3 of Fig. 8) and the HLF node subscribes to the same topic (refer to step 4 of Fig. 8). Besides, the same RPi3 device serves as the MQTT broker as the bridge between two clients. 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 (refer to Fig. 9) in the blockchain network. Besides the incorporated MQTT client, the *invoke* program also contains the *submitTransaction* API. Once *invoke* is run, the client connects to the broker on the RPi3 and subscribes to the topic *rfidData* listening to an incoming message (refer to step 4 of Fig. 8). So far, there is the only action regarding the car-sharing MQTT client, but the transaction process (refer to step 6 of Fig. 8) has not been triggered yet.

Now we can turn on RPi3 which represents a car to start the actual IoT data transmission. As the RFID tag represents a mobile app, a user would type in its *renterID* and the reservation confirmation number representing the *carKey*. The *carKey* is written on the RFID tag with

[8] Model B+ (Rev-1.3) with ARM Cortex-A53@1.4 GHz core, 1024 MB memory, and Raspbian 10 operating system.

[9] Version-3.7.3.

[10] The SimpleMFRC522 library is used to read the data coming from the RFID sensor on the RPi3.

[11] Libraries Paho MQTT for the client and Mosquitto for the broker are used.

[12] Ubuntu Linux 18.04.4 LTS with 4 GB memory and Intel i7-8565U model with clock speed 1.80 GHz.

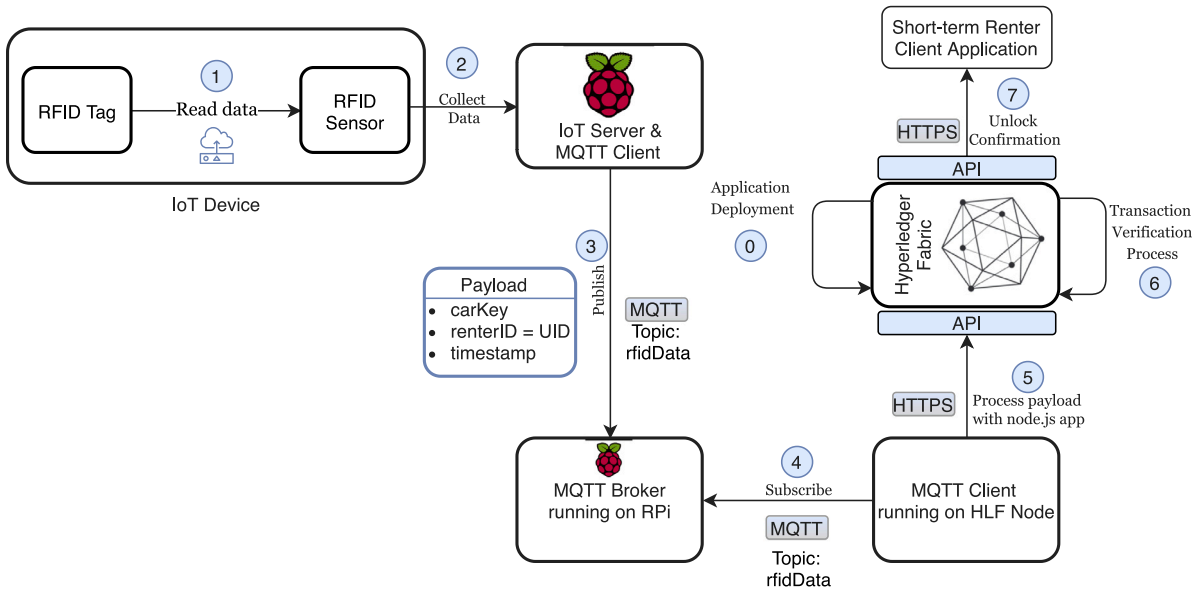

Fig. 8. Workflow of transaction deployment.

Algorithm 1: Invoke Program: Connect to MQTT Broker and Submit transaction

Result: Pass on Data to smartcontract submitting a transaction
Data: rfidData (JSON object from RPi3)

```
/* Check correct user                          */
wallet is walletPath;
if Renter is not in wallet then
    return "Renter does not exist in wallet";
end
/* Initialize HLF network, contract,
   MQTT broker                                 */
network is carLeaseChannel;
contract of network is leasecar;
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
```

Fig. 9. Pseudocode of Invoke Node.js program.

Algorithm 2: RPi3 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
```

Fig. 10. Pseudocode of reading and publishing program on RPi3.

a simple *write* script using the SimpleMFRC522 library. 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 running that collects the data from the RFID sensor (refer to step 2 of Fig. 8) reading the *UID* and the written *carKey* from the RFID tag (refer to step 1 of Fig. 8). The *UID* corresponds with the *renterID* stored in *carKey*. 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 (refer to step 3 of Fig. 8). MQTT client on the RPi3 is demonstrated as pseudocode in Fig. 10.

At the HLF network, the published payload with the JSON object has arrived and has been used in the *invoke.js* to trigger the *chaincode* (*smartcode*) function *openCar()* by using the *submitTransaction* API (refer to step 5 of Fig. 8). In this way, the received values *carKey*, *renterID*, and *timestamp* are passed on to the *openCar* transaction function, which is demonstrated as pseudocode in Fig. 11. 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

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
```

Fig. 11. Pseudocode of our main transaction function openCar().

car object to *unlock* and *startTime* to the *timestamp*. The set event can be used in further development to trigger a new message published back to the RPi3 to actuate a light or sound simulating the physical opening of a car door. Eventually, the ledger is updated accordingly. In a nutshell, the application submits the particular transaction to the blockchain network. Once it has been validated and committed (refer to step 6 of Fig. 8), the application receives a notification that the transaction has been successful (refer to step 7 of Fig. 8).

5.3. Results and analysis

In Section 1, we already mentioned that our proposed architecture answers two research questions. In this sub-section, first, we will present the results from our simulation (refer to sub-Section 5.3.1). Next, we will briefly analyze five primary design principles (refer to sub-Section 5.3.2).

5.3.1. Simulation results

Table 2 shows the changes occurred where the empty *startTime* is replaced with the *timestamp* received from the RPi3, and the status is changed from *located* to *unlocked* which represents a successful transaction.

Besides the updated world state, we can look at the specific block created. As a first comparison, we checked the blockchain before and after the submitted transaction. As seen in Table 2, the height of the blockchain changed from five to six. The already higher number of the initial blockchain means that all the setup activities to the network and the application (such as 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*. 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 (refer to Figs. 12 and 13). There are two main details in the block that are of particular relevance, while most of the information is encrypted. 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 (refer to Fig. 12). Second, the proposal response payload contains the information about the set event *TransferConfirmed* mentioned before, as seen in the left side image of Fig. 13 and the write request on the ledger for the key *CARxxx* with the respective encrypted value, which is visible in the right side image of Fig. 13.


```
"payload": {
        "action": {
                "endorsements": [
                {
                 "endorser": "CgdPcmcxTVNQEqoGLS0tLS1CRUdJTi.....",
                 "signature": "MEUCIQC2g948R2IfCH0A+/2xj6wp....."
                 },
                 {
                  "endorser": "CgdPcmcyTVNQEqoGLS0tLS1CRUdJT.....",
                  "signature": "MEUCIQDF+BBUjsIRgn+vVRhMex6....."
                  }
                 ],
```


Fig. 12. Snippet of the block in regard to endorsement.

5.3.2. Qualitative analysis

We have conducted five expert interviews to evaluate both the technical and business implication of the prototype and overall designed artifact. Thus, we can eventually discuss the designed artifact not only based on theoretical deduction (literature review) and technical feasibility (prototype) but also in terms of pragmatic and real-world insights, which are reported below:

- *Security and Privacy* Surprisingly, it is notable that privacy and security regarding 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, addressed in the next section. After all, it still can be confirmed that using a permissioned blockchain is recommended while finding the right balance between centralization and decentralization is necessary. Finally, the interviews show that the need for security and trust requires an assessment for every use case and transaction within our proposed architecture resulting in the questions of what should run on- or off-chain.
- *Authenticity* Based on the interviews with experts, we can argue 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.
- *Traceability and Reliability* Based on interviewees, 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. Thus, even the demonstrated use case of our architecture needs a certain level of security for the authentication and reliability of the data. In addition, whether the actual transaction process could be shifted to off-chain is discussable.

Table 2
Output of query and blockchain info before and after the submitted transaction.

	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”:
	“5b83ekkxlFWY4hPevxu1UeWW3AkuGtC8 Wr4HVzDnFfE=”
	“previousBlockHash”:
	“zbO1gojMGkCk662Ue+3P7g9GSyEkBzmR
	IRpqrzeXzuw=”
	}
		Block 5:
		{
		“height”: 6,
		“currentBlockHash”:
		“CwAJAIOL9mVrCzej+Zl7kbFxz36hemY8F
		A+jRM24Lew=”
		“previousBlockHash”: “5b83ekkxlFWY4hPevxu1UeWW3AkuGtC8
		Wr4HVzDnFfE=”
		}


```
"_response_payload": {
                    "extension": {
                     "chaincode_id": {
                      "name": "fabcar",
                      "path": "",
                      "version": "1.0"
                      },
                      "events": {
                       "chaincode_id": "fabcar",
                       "event_name": "TransferConfirmed",
                       "payload": "eyJzdGF0dXNDYXIiOiJvcGV.....",
                       "tx_id": "20602bfcab2ecc951991435f3....."
                      },
                      "response": {
                       "message": "",
                       "payload": null,
                       "status": 200
                       },
```

```
"writes": [
        {
        "is_delete": false,
        "key": "CARxxx",
        "value": "eyJjdXJyZW50T3duZXIiOiI0NTZh"
        }...
```


Fig. 13. Snippets of the block in regard to event submission and ledger update.

- *Scalability* 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, blockchain alone will not be the only technology that provides the scalability of such a system. Still, it will also rely on public network and communication technology (such as 5G/6G). Nevertheless, it is highly relevant to carefully consider which transactions should run on- or off-chain and select a blockchain platform that supports scalability.
- *Interoperability* We can confirm from the interviews that the interoperability and seamless integration of the OEMs and leasing companies to set up a more attractive blockchain-based car-sharing platform is an important principle to consider in our designed high-level architecture. 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 and the allocation of administrative and operational efforts over several companies. New features can be offered based on regulating and executing the full leasing and car-sharing process on one platform while sharing data securely. 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 is required as incentives for other companies to join the network. The modular architecture of HLF eases the integration of each organization’s system. In conclusion, providing the right incentives can further enable people to develop and apply our high-level architecture. At the same time, first, a profitable and scalable business model has to be identified.

6. Discussion

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). 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 societycite (Chen and Kockelman, 2016). 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, or carpooling in how the renters themselves drive the shared car. Additionally, it also differs from the traditional car rental since cars are available nearby,

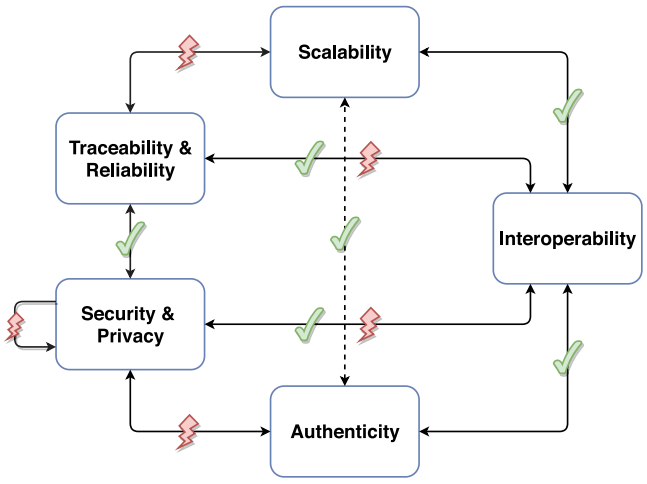

Fig. 14. Interconnections between key design principles.

and the rent is more flexible regarding the duration and pick-up/drop-off location (Münzel et al., 2020). As the main asset of car-sharing, cars are moving data centers that need to be connected securely to a reliable system (Dorri et al., 2019). Blockchain, as one possible technology, has the potential to drive car sharing by enabling secure and trustful data sharing between both the cars and the participating stakeholders during the car-sharing and leasing (Gösele and Sandner, 2019; Bossauer et al., 2019).

6.1. Design principles

A visible trade-off between traceability (including reliability), security (including privacy), and scalability is presented in Fig. 14. 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, along with the desired V2X communication making every single vehicle part of the blockchain network. On the other hand, however, it suffers from scaling problems. Currently, the lack of lightweight consensus mechanisms and powerful IoT devices hinders the ultimate scalability of our proposed blockchain-based platform. However, the IoT domain's technological advancements are happening in a rapid phase, so soon, these obstacles can be addressed. Overall, finding an adequate level of traceability, security, scalability, and authenticity can positively affect the interoperability of the entire proposed architecture, as further discussed below.

- *Security and Privacy* Gaining trust among rational actors is complex, and sharing a valuable asset such as a car in a P2P car-sharing involves a lot of trust issues among the stakeholders. Collecting privacy-sensitive data via telematic data may build trust, but lack of secure processing, access, and unreliable traceability could defeat the gained trust. 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 (Dedeoglu et al., 2020). Therefore, a blockchain-based decentralized trust mechanism eliminates the single point of failure by distributing trust on several nodes. The degree of decentralization and respective choice of a secure, privacy-preserving blockchain platform with a suitable consensus mechanism must be further investigated.
- *Authenticity* Authentication with diverse levels of access control to IoT devices is of significant importance. In the car-sharing process, every interaction with a new business entails newly created digital personas that are disconnected from each other. Bringing everyone together on one platform enabling secure data sharing with blockchain, one unique and universal identity can be created that allows the user to access the services provided by all businesses. Finally, there is a need to employ digital identity management (e.g., self-sovereign identity) for permissioned blockchain to ensure authenticity for the car-sharing and leasing process and avoid data silos.
- *Traceability and Reliability* Blockchain offers immutability of data, which enhances further trust in the systems as data can be verified and validated at any point in time. For example, by storing the telematics data of a leasing car on the blockchain, accessible to both the lessee and leasing company, disputes at the end of a leasing period are minimized. Furthermore, our proposed architecture ensures that each transaction is logged, right from ordering a leasing car over selecting an insurance package in renting a car. Combined with the blockchain, stored IoT data ensures reliability and traceability, leading to the reproducible history of the car's data, which is especially useful during fraud or damages. As one of the possible applications of such data, the price of insurance and rental could be set fairly according to the actual usage of the car and the driving behavior of the lessee. Furthermore, each car's status and telemetric data are stored on the blockchain in our proposed architecture, which leads to an immutable history log, allowing the query of the car's status at all times by the stakeholders.
- *Scalability* Scalability is one of the critical issues that are crucial for any real-time application. Blockchain can handle the IoT data, but the real-time applicability entirely depends on the data storage locations (such as on or off-chain), reliability, modularity, distributed application type together with other functions/libraries/technologies. Our implemented prototype is on-chain-focused, where all the data is stored on the blockchain. However, such an approach is not scalable for larger production-ready applications, results in significant resource consumption, limited throughput, and response delay. One of the solutions could be to use a hybrid approach where off-chain storage is used for storing the data of car renting/leasing events and a hash pointer (to the off-chain storage data location) on the blockchain (Faber et al., 2019). In comparison, this hybrid approach will ensure data integrity and immutability of the off-chain data location through the hash pointer and, at the same time, scalable, as only hash pointers are stored on the blockchain.
- *Interoperability* is crucial for shared mobility, which essentially is an inter-company platform accessible by multiple stakeholders via multiple (micro)-services. Interoperability brings multiple advantages: better automation, shared operation costs via integration, and improved features/services. However, the literature lacks comparable studies about which blockchain or combination of different technologies could be suitable for car-sharing or shared mobility. After all, HLF has the potential to provide the feasibility of implementing different business logic.

In summary, we see interoperability as relevant to open innovation, inter-company collaboration, and competition. Moreover, scalability is more crucial and challenging to fulfill in a blockchain-based ecosystem than we initially assessed. Finally, 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.

6.2. Discussion on technological aspects

Apart from the above design principles, other factors can influence our blockchain-based car-sharing platform and its implementation. These factors are: (i) smart contracts; (ii) immutable chains; (iii) shared database; (iv) decentralization and (v) consortium creations.

While the smart contract addresses more on the interoperability side of blockchain, data immutability also supports record traceability and reliability. The decentralization enhances scalability as well as reliability. Consortiums also tried to address the issues on authenticity, interoperability, security, and privacy, while shared databases can improve the scalability and network throughput. Below we are discussing all these factors in brief:

- *Smart Contracts:* They can ease the interoperability of different stakeholders and also increase trust in the system (Dedeoglu et al., 2020; Yuan and Wang, 2016). Once the smart contract is deployed, it cannot be modified thus the logic design, interpretation, and legal status[13] must be considered beforehand taking into consideration all the aspects of use covering the relevant stakeholders. However, smart contracts' technological and legal development will have a far-reaching impact on the applicability of blockchain-based shared mobility platforms and needs to be elaborated in further research.
- *Immutable Chains and GDPR Compliance:* The data immutability on the blockchain is achieved through hash pointers and a suitable consensus mechanism. However, the applicability and usefulness of applying immutability to data storage need to be evaluated from multiple aspects, case by case. For example, the data gathered for the proposed blockchain-based car-sharing platform might include individuals' privacy-sensitive information. Furthermore, as individuals have the right to demand the erasure of their data (i.e. "Right to be Forgotten" (GDPR)), the tracking of information on an immutable ledger poses the challenge of deleting the records/data from the blockchain, which will leave the blockchain in an inconsistent state. Alternatively, if the information is not deleted, it will make the blockchain non-compliant with GDPR. In such situations, storage of personal information on the off-chain repositories and storing a hash pointer on the blockchain, pointing to the personal data storage location off-chain repository, can make the information both GDPR compliant and at the same time immutable as indicated in Faber et al. (2019). Having a hash pointer on the blockchain to the personal data location on the off-chain repository can achieve the immutability nature of the blockchain as the personal information on the off-chain repository can be verified using the hash value stored in the hash pointer. In addition, when someone exercises their "Right to be Forgotten", then respective personal information on the off-chain repository can be removed to be GDPR compliant. Still, the hash pointer stored on the blockchain can stay as it is, as the hash pointer without any personal information on the off-chain repository reveals nothing. In this way, the challenge of storing user information on the blockchain can be addressed.
- *Decentralization and Power Imbalance:* There is a trade-off between higher security and less control over the data and/or system, which could be optimized using the access rights (such as using permissioned blockchain). The permissioned blockchain divides the responsibility of managing the consensus mechanism and maintenance by a group of equally powerful participants (Dedeoglu et al., 2020). 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 a consensus to set up and adapt the network, leading to an abuse of power by certain consortium members. They could make their agreement dependable on self-beneficial factors (such as economic benefits). These aspects need to be considered carefully while implementing the proposed high-level architecture.
- *Consortium Types:* Blockchain-based shared mobility still lacks commercial adaptation. We advocate that the advancement of car-sharing and other mobility services with blockchain is suitable for the consortium of several companies. The consortium for mobility services should be scalable and sustainable, and it should add value to all the stakeholders.[14] The automotive industry's transformation through blockchain and related technologies will undoubtedly be significant in the coming years, but which type of consortium will lead the way is future dependent. There are benefits and drawbacks for both small and large consortiums, including small or big companies. Still, it depends on the geographical location, existing infrastructures, technological developments within the blockchain, and supportive network.
- *Sharing of Data and Resources* The potential of blockchain to aggregate car-sharing services and other mobility services on one platform in the fashion of Mobility as a Service (MaaS) will be the ultimate goal. The benefits of streamlining the car-sharing and leasing process based on the sharing of data and resources will lead to higher efficiency and performance. Such an approach also reduces the data silos in the shared platforms (Ferdous et al., 2019).

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 autonomous vehicles become roadworthy, car-sharing may reach a new level of relevance in combination with advanced IoT and digital twin, self-sovereign identity (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 solution needs to be extended with a detailed consideration of cryptocurrencies and SSI to understand the feasibility of acting autonomously service-wise entirely. Finally, 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.

7. Conclusion

Motivated by the growing interest in shared mobility, this research work investigates how blockchain and IoT technologies can drive the advancement of shared mobility, specifically for car-sharing and leasing. This research proposed a conceptual design and architecture of a blockchain-IoT-based car-sharing platform based on key design principles. Furthermore, we also developed a prototype for a keyless vehicle access control to demonstrate the feasibility of a blockchain-IoT-based car-sharing platform and experiment with streamlining car-sharing and leasing processes. Our findings reveal that blockchain, as one possible technology, can advance car-sharing by facilitating inter-company collaboration between several stakeholders within car-sharing and leasing and eliminating the need for trust to some extent. However, the design of the underlying blockchain-based platform relies on the appropriate balance between five design principles, namely security and privacy, authenticity, traceability and reliability, scalability, and interoperability, as discussed in the previous sections. 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

[13] 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. 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.

[14] Toyota with Oaken Innovation created a consortium with a car-sharing and leasing platform that offers a blockchain-enabled digital identity of vehicles and historical data storage (Oakeninnovations.com, 2020).

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.

The proposed car-sharing platform, involving an immense amount of IoT data collected by a large number of vehicles, faces the challenge of integrating IoT with blockchain scalably. Our findings also confirm the interoperability of such an IoT and blockchain integration. Eventually, it is inevitable to make IoT devices part of the blockchain network to address the need for connectivity between vehicles, users, and the surrounding (V2X). Thus, Car-sharing is expected to remain of significant relevance for the environment and society. Nevertheless, its economic growth relies on developing innovative concepts concerning technology and business models in which OEMs will play a significant role. Therefore, blockchain as one possible technology can be seen as one cause of thought for OEMs to collaborate with other stakeholders to advance car-sharing and support the transformation of the entire automotive industry to shift from the car as a product to the 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*.

7.1. Future work

We would like to work along the following lines as part of our future work.

- *Authenticity* of accessing the IoT device could be improved by replacing the RFID with an NFC14 sensor and the RFID tag with a mobile app. Thus, users need to authenticate themselves by actually using their private keys instead of the pre-defined ID of the RFID tag. Finally, to truly complete the "unlock car" transaction, an actuator would be necessary to show the entire workflow from sending data into the blockchain and back to the IoT device to trigger an action (such as a LED lamp or sound-based indication or alert).
- *Scalability* The implementation has to be scaled up to represent a real-world usage scenario with an increase in the number of nodes, users, and transactions. In addition, combining different blockchain platforms to achieve better compatibility with the key design principles should also be assessed.
- *Perspective* The problem has been formulated from OEM's point of view. Furthermore, it is necessary to test and evaluate the proposed architecture from other perspectives, such as the end user's viewpoint (such as sharing willingness, incentives for leasing, the flexibility of using offered services).
- *Leasing and Insurance processes* In the current research work, the leasing and insurance processes are not analyzed in-depth, based on the assumption that streamlining of these processes is possible. Our research indicates that there is great potential for further research in this direction. It also showcases the need for researching these areas separately more in-depth, especially concerning blockchain's feasibility to comply with KYC checks.

CRediT authorship contribution statement

Sophia Auer: Conceptualization, Methodology, Writing – original draft, Software. **Sophia Nagler:** Conceptualization, Methodology, Writing – original draft. **Somnath Mazumdar:** Resources, Visualization, Data curation. **Raghava Rao Mukkamala:** Formal analysis, Supervision, Writing – review & editing, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Ballús-Armet, I., Shaheen, S.A., Clonts, K., Weinzimmer, D., 2014. Peer-to-peer carsharing: Exploring public perception and market characteristics in the San Francisco bay area, California. Transp. Res. Rec. 2416, 27–36.

Bardhi, F., Eckhardt, G.M., 2012. Access-based consumption: The case of car sharing. J. Consum. Res. 39, 881–898.

Belk, R., 2010. Sharing. J. Consum. Res. 36, 715–734.

Bossauer, P., Neifer, T., Pakusch, C., Staskiewicz, P., 2019. Using blockchain in peer-to-peer carsharing to build trust in the sharing economy. In: Track 3: Unternehmensmodellierung & Informationssystemgestaltung (Enterprise Modelling & Information Systems Design). pp. 274–278.

Burghard, U., Dütschke, E., 2019. Who wants shared mobility? Lessons from early adopters and mainstream drivers on electric carsharing in Germany. Transp. Res. D 71, 96–109.

Chen, T.D., Kockelman, K.M., 2016. Carsharing's life-cycle impacts on energy use and greenhouse gas emissions. Transp. Res. D 47, 276–284.

Christidis, K., Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303.

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R., Michelin, R., Zorzo, A., Kanhere, S., 2020. Blockchain technologies for IoT. In: Advanced Applications of Blockchain Technology. Springer, pp. 55–89.

Deloitte, M., 2017. Car sharing in europe business models, national variations and upcoming disruptions. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/consumer-industrial-products/CIP-Automotive-Car-Sharing-in-Europe.pdf.

Dmitrienko, A., Plappert, C., 2017. Secure free-floating car sharing for offline cars. In: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy. pp. 349–360.

Dorri, A., Steger, M., Kanhere, S.S., Jurdak, R., 2017. Blockchain: A distributed solution to automotive security and privacy. IEEE Commun. Mag. 55, 119–125.

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.

EU Parliament News, 2019. Co2 emissions from cars: facts and figures. https://www.europarl.europa.eu/news/en/headlines/society/20190313STO31218/co2-emissions-from-cars-facts-and-figures-infographics.

Faber, B., Michelet, G.C., Weidmann, N., Mukkamala, R.R., Vatrapu, R., 2019. Bpdims: A blockchain-based personal data and identity management system. In: Proceedings of the 52nd Hawaii International Conference on System Sciences. pp. 6855–6864.

Ferdous, M.S., Chowdhury, F., Alassafi, M.O., 2019. In search of self-sovereign identity leveraging blockchain technology. IEEE Access 7, 103059–103079.

Fraga-Lamas, P., Fernández-Caramés, T.M., 2019. A review on blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE Access 7, 17578–17598.

Fraiberger, S.P., Sundararajan, A., et al., 2015. Peer-to-Peer Rental Markets in the Sharing Economy. NYU Stern School of Business Research Paper 6.

Gaddam, A., Wilkin, T., Angelova, M., Gaddam, J., 2020. Detecting sensor faults, anomalies and outliers in the internet of things: A survey on the challenges and solutions. Electronics 9, 511.

Gösele, M., Sandner, P., 2019. Analysis of blockchain technology in the mobility sector. Forsch. Ing. 83, 809–816.

Guhathakurta, R., 2018. Blockchain in automotive domain. In: The Age of Blockchain: A Collection of Articles. p. 17.

Guyader, H., Piscicelli, L., 2019. Business model diversification in the sharing economy: The case of gomore. J. Cleaner Prod. 215, 1059–1069.

Hang, L., Kim, D.H., 2019. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. Sensors 19, 2228.

Hassija, V., Zaid, M., Singh, G., Srivastava, A., Saxena, V., 2019. Cryptober: A blockchain-based secure and cost-optimal car rental platform. In: 2019 Twelfth International Conference on Contemporary Computing (IC3). IEEE, pp. 1–6.

Hawlitschek, F., Notheisen, B., Teubner, T., 2018. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. 29, 50–63.

Johnson, M.D., Herrmann, A., Huber, F., 1998. Growth through product-sharing services. J. Serv. Res. 1, 167–177.

Ke, H., Chai, S., Cheng, R., 2019. Does car sharing help reduce the total number of vehicles? Soft Comput. 23, 12461–12474.

Klein, N.J., Smart, M.J., 2017. Millennials and car ownership: Less money, fewer cars. Transp. Policy 53, 20–29.

Klems, M., Eberhardt, J., Tai, S., Härtlein, S., Buchholz, S., Tidjani, A., 2017. Trustless intermediation in blockchain-based decentralized service marketplaces. In: International Conference on Service-Oriented Computing. Springer, pp. 731–739.

Kwame, O.B., Xia, Q., Sifah, E.B., Amofa, S., Acheampong, K.N., Gao, J., Chen, R., Xia, H., Gee, J.C., Du, X., et al., 2018. V-chain: A blockchain-based car lease platform. In: 2018 IEEE 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). IEEE, pp. 1317–1325.

Le Vine, S., Polak, J., 2019. The impact of free-floating carsharing on car ownership: Early-stage findings from London. Transp. Policy 75, 119–127.
Le Vine, S., Zolfaghari, A., Polak, J., 2014. Carsharing: Evolution, Challenges and Opportunities-22th Acea Scientific Advisory Group Report. European Automobile Manufacturers Association, Brussels.
Liao, F., Molin, E., Timmermans, H., van Wee, B., 2019. Consumer preferences for business models in electric vehicle adoption. Transp. Policy 73, 12–24.
Lieber, R., 2012. Share a car, risk your insurance. N.Y. Times.
Liu, H., Han, D., Li, D., 2020. Fabric-iot: A blockchain-based access control system in IoT. IEEE Access 8, 18207–18218.
Machado, C.A.S., de Salles Hue, N.P.M., Berssaneti, F.T., Quintanilha, J.A., 2018. An overview of shared mobility. Sustainability 10, 4342.
Madhusudan, A., Symeonidis, I., Mustafa, M.A., Zhang, R., Preneel, B., 2019. Sc2share: Smart contract for secure car sharing. In: ICISSP. pp. 163–171.
Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., Izumchenko, E., Aliper, A., Romantsov, K., Zhebrak, A., et al., 2018. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 9, 5665.
McKinsey Center for Future Mobility, 2020. Shared mobility. https://www.mckinsey.com/features/mckinsey-center-for-future-mobility/overview/shared-mobility.
Münzel, K., Boon, W., Frenken, K., Blomme, J., van der Linden, D., 2020. Explaining carsharing supply across western European cities. Int. J. Sustain. Transp. 14, 243–254.
Narayanan, A., Clark, J., 2017. Bitcoin's academic pedigree. Commun. ACM 60, 36–45.
Oakeninnovations.com, 2020. Oaken innovation verticals. URL: 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. J. Environ. Psychol. 53, 121–130.
Pavithran, D., Shaalan, K., Al-Karaki, J.N., Gawanmeh, A., 2020. Towards building a blockchain framework for IoT. Cluster Comput. 1–15.
Peck, J., Shu, S.B., 2018. Psychological Ownership and Consumer Behavior. Springer.
Peniak, P., Bubeníková, E., 2019. Validation of IoT secure communication gateway for constrained devices. In: 2019 International Conference on Applied Electronics (AE). IEEE, pp. 1–5.
Pfeifle, S., Ley, C., Tauschek, F., Enderle, P., 2017. Fleet Management in Europe - Growing Importance in a World of Changing Mobility. Technical Report, Deloitte Consulting GmbH.
Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M., 2018. On blockchain and its integration with IoT, challenges and opportunities. Future Gener. Comput. Syst. 88, 173–190.
Rowan, S., Clear, M., Gerla, M., Huggard, M., Goldrick, C.M., 2017. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. arXiv:1704.02553.
Shaheen, S.A., Cohen, A.P., 2013. Carsharing and personal vehicle services: worldwide market developments and emerging trends. Int. J. Sustain. Transp. 7, 5–34.
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. Elsevier, pp. 237–262.
Shaheen, S.A., Mallery, M.A., Kingsley, K.J., 2012. Personal vehicle sharing services in north America. Res. Transp. Bus. Manage. 3, 71–81.
Shaheen, S., Martin, E., Bansal, A., et al., 2018. Peer-to-Peer (P2P) Carsharing: Understanding Early Markets, Social Dynamics, and Behavioral Impacts. Technical Report, Institute of Transportation Studies at UC Berkeley.
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. J. Urban Des. 1–18.
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.
Sultan, A., 2016. Leasing in the automobile industry: Who lease cars. Int. J. Appl. Econ. Financ. 10, 14–20.
Sun Yin, H.H., Langenheldt, K., Harlev, M., Mukkamala, R.R., Vatrapu, R., 2019. Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain. J. Manage. Inf. Syst. 36, 37–73.
Valaštín, V., Košt'ál, K., Bencel, R., Kotuliak, I., 2019. Blockchain based car-sharing platform. In: 2019 International Symposium ELMAR. IEEE, pp. 5–8.
Xu, C., Zhu, K., Yi, C., Wang, R., 2020. Data pricing for blockchain-based car sharing: A stackelberg game approach. In: GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, pp. 1–5.
Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C., 2018. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet Things J. 6, 1495–1505.
Yuan, Y., Wang, F.Y., 2016. Towards blockchain-based intelligent transportation systems. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, pp. 2663–2668.
Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J., 2018. Blockchain-based personal health data sharing system using cloud storage. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE, pp. 1–6.
Zheng, X., Sun, S., Mukkamala, R.R., Vatrapu, R., Ordieres-Meré, J., 2019. Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies. J. Med. Int. Res. 21, e13583.
Zhou, Q., Yang, Z., Zhang, K., Zheng, K., Liu, J., 2020. A decentralized car-sharing control scheme based on smart contract in internet-of-vehicles. In: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring). IEEE, pp. 1–5.

Sophia Auer was born in Munich, Germany in 1995. She received the B.Sc. degree in Management & Technology with major in Mechanical Engineering and Finance from the Technical University of Munich, Germany in 2017. In 2020 she completed her M.Sc. degree in Business Administration and Information Systems — E-Business from Copenhagen Business School, Denmark. Her research focus during her Master was on Mobility, IoT, Robotics and Big Data infrastructure technologies. Professionally, she works on her career path as a Software Engineer.

Sophia Nagler was born in Karlsruhe, Germany in 1993. She received the B.Sc. degree in Business Administration with major in Management, Marketing and Innovation from the Ludwig-Maximilians University, Munich, Germany in 2018. She received the M.Sc. degree in Business Administration and Information Systems — E-Business from Copenhagen Business School, Copenhagen, Denmark in July 2020. She focused her research during her Master on Data Analytics, Data Science and Big Data infrastructure technologies. Professionally, she works on her career path in Data Analytics.

Somnath Mazumdar is a Postdoctoral Researcher at the Department of Digitalization. His research interests focuses on Distributed Ledger Technology/Blockchain, Machine Learning, Big Data, and High-Performance Computing. He holds a PhD in Computing Systems from University of Siena, Italy, as well as a MS in Distributed Computing from Polytech Nice Sophia Antipolis, France. Somnath also has worked on multiple EU/International research projects.

Raghava Rao Mukkamala is the director of the Centre for Business Data Analytics (https://cbsbda.github.io/), an associate professor at the Department of Digitalization, Copenhagen Business School, Denmark. Raghava holds a PhD in Theoretical Computer Science and his current research focusses on Big Data Analytics, Data Science, Blockchain Technologies and Cyber Security. Combining formal/mathematical modeling approaches with machine learning techniques, his current research program seeks to develop new algorithms for big data analytics. He is also the Programme Director for the Masters in Data Science programme at CBS and teaches several courses on machine learning. Before moving to research, Raghava has many years of programming and IT development experience from the Danish IT industry.