Towards a Privacy-Preserving Way of Vehicle Data Sharing – A Case for Blockchain Technology?

Christian Kaiser, Marco Steger, Ali Dorri, Andreas Festl, Alexander Stocker, Michael Fellmann, Salil Kanhere

Virtual Vehicle Research Center, Graz, Austria <christian.kaiser@v2c2.at>,
Virtual Vehicle Research Center, Graz, Austria <marco.st1987@gmail.com>,
University of New South Wales, Sydney, Australia <ali.dorri@unsw.edu.au>,
Virtual Vehicle Research Center, Graz, Austria <andreas.festl@v2c2.at>,
Virtual Vehicle Research Center, Graz, Austria <alexander.stocker@v2c2.at>,
University of Rostock, Rostock, Germany <michael.fellmann@uni-rostock.de>,
University of New South Wales, Sydney, Australia <salil.kanhere@unsw.edu.au>

Abstract

Vehicle data is a valuable source for digital services, especially with a rising degree of driving automatization. Despite regulation on data protection has become stricter due to Europe's GDPR we argue that the exchange of vehicle and driving data will massively increase. We therefore raise the question on what would be a privacy-preserving way of vehicle data exploitation? Blockchain technology could be an enabler, as it is associated with privacy-friendly concepts including transparency, trust, and decentralization. Hence, we launch the discussion on unsolved technical and non-technical issues and provide a concept for an Open Vehicle Data Platform, respecting the privacy of both the vehicle owner and driver using Blockchain technology.

1 Introduction and Scope

1.1 Introduction and Motivation

Future smart vehicles will provide advanced autonomous driving functions and will be highly connected to other vehicles, roadside infrastructure and to various cloud services. The information gained through these wireless interconnections will be used by any smart vehicle to enrich its own information gathered by built-in sensors such as cameras and radar sensors to further increase the reliability of its autonomous driving functions. However, it will also assist to solve automotive research topics like detection of driver fatigue or driver distraction. These research topics will receive additional focus at the time autonomously driven vehicles will face real world problems on the street and will have to force the driver to takeover. However, the data collected within current vehicles of limited smartness can be used beyond assisting their drivers in driving. Moreover, vehicle data is valuable for third parties [1,2,3] including e.g. vehicle manufacturers (i.e., OEMs), suppliers, and traffic managers to name three stakeholders, although, there are still many open issues connected to the exchange of vehicle usage data. One dominant challenge for vehicle and driving data exploitation is how to safeguard the privacy of the driver. Despite the privacy regulation has gotten stricter in Europe with the General Data Protection Regulation (GDPR) [4], we argue that the exchange of vehicle usage data will increase a lot in the future due to two recent developments, tech startups pushing artificial intelligence technologies and the rising interest of the automotive industry to foster the automated driving paradigm.

Shortcomings of current vehicle data provisioning approaches are: Data, information, and services are mostly exchanged within *proprietary closed environments,* as collected vehicle usage data is usually directly sent from the smart vehicle to a single service provider (e.g., by a device connected to the OBD-II interface of the vehicle or via the drivers' smartphone). As a result, a vehicle owner willing to share data with multiple service providers will have to *provide the data multiple times* while collecting the data with different devices in parallel. This can be critical due to the large amount of data collected by smart vehicles (up to 4TB of data per day are expected [5]), and because a significant portion of current service providers (e.g., Automile and Zubie) is using dedicated OBD-II dongles to gather data from smart vehicles. Thus, it is currently not feasible or at least not practical to use several services at the same time. Finally, these closed systems certainly *disrespect the vehicle owner's privacy*, as they do not make it transparent how they further monetize the gathered

You can cite this paper as:
Kaiser, C., Steger, M., Dorri, A., Festl, A., Stocker, A., Fellmann, M., & Kanhere, S. (2018, September). Towards a Privacy-Preserving Way of Vehicle Data Sharing–A Case for Blockchain Technology?. In *International Forum on Advanced Microsystems for Automotive Applications* (pp. 111-122). Springer, Cham.

data nor with whom they share it. They typically do not allow the end user to control what data is transferred and shared. And most of them have a lock-in effect, i.e. they use the vehicle data for their own purposes. Finally, their *business models do not scale* yet as their user community is still composed mostly of early adopters [1].

1.2 Contributions and Structure

Sharing data always holds the risk of violating one's privacy. So, what is a privacy-preserving way of vehicle data exploitation? Can the Blockchain technology act as an enabler?

Blockchain technology is currently revolutionizing the way smart contracts between parties will be managed due to its outstanding advantages namely *decentralization* and *transparency* per design. The application of Blockchains as a solid basis for a secure data exchange platform seems to be promising to solve the challenge of monetizing vehicle usage data while protecting the data owner's privacy. In contrast to closed systems, a so-enabled *Open Vehicle Data Platform* for vehicle usage data based on smart contracts maintained within Blockchains would allow the user to choose which service providers can access certain vehicle data for which exploitation purpose. Thus, end users can make use of services from various service providers at the same time, while being in full control over the collected data, which will also be crucial for autonomous driving. Full control can be achieved by employing privacy settings for each authorized service provider. The user can decide whether to share only anonymized data (e.g., as required by traffic management systems), vehicle-specific data (e.g., for OEMs for continuous improvement), or even user-specific data (e.g., as required by insurance companies to provide flexible insurance rates in Pay-As-You-Drive (PAYD) models [6]). Such a platform will be able to support a wide range of service providers and allow different benefit/business models advantageous for both the users and the service providers.

Towards proposing a concept for an *Open Vehicle Data Platform*, in Section 1, we reviewed existing solutions for vehicle data sharing, highlight strengths and weaknesses, and particularly focused on potential privacy issues. Thereafter, in Section 2, we provide related work and background for Blockchain technology in the automotive domain and for connected vehicles. Consequently, we discuss the actors and roles of a vehicle data sharing ecosystem, the underlying privacy challenge and propose possible privacy setting schemes protecting the privacy of the involved users, followed by a concept for a Blockchain-based *Open Vehicle Data Platform* in Section 3. In the latter, Blockchain technology ensures a trustworthy data exchange between all involved entities and users. After providing a description of a conceptual workflow, we discuss open issues and related aspects required to realize the proposed data sharing platform and thereby conclude the paper with a discussion and outlook in Section 4.

2 Related Work and Background

2.1 Blockchain Technology (in automotive)

Blockchains were first introduced as underlying technology of Bitcoin in 2008 [7]. In this initial form, single transactions are used to describe a cash flow from one entity to another. Every new transaction is distributed to the entire Blockchain system and in a subsequent step a predefined amount of these transactions is compiled into a block, and finally this block is then stored in the Blockchain. The latter can be seen as a distributed database, where blocks are immutably chained to each other. The immutable property on block and on transaction level is ensured by using cryptographic hash functions and digital signatures. Every entity within the Blockchain system can easily verify a transaction as well as a block without requiring any trusted party within the system.

Newer versions of Blockchain allow, besides the exchange of simple transactions, also the creation of *smart contracts*. The latter can be seen as executable "if-then" condition which is stored on the Blockchain and can e.g. be used to trigger a cash flow by an event (e.g., transfer the flat rent to the landlord on the 1st day of each new month). Besides simple examples, smart contracts also allow describing more complex relations between companies, governmental bodies, etc. and

thus is a promising technology to realize a wide range of distributed services and applications in various industrial domains and especially w.r.t. IoT solutions.

Thus, Blockchains and especially smart contracts can potentially be used to solve certain open issues in the automotive industry due to its capability to preserve privacy; in particular w.r.t. long-term research topics like detection of driver attention/fatigue and current topics like utilizing vehicles as distributed comprehensive environmental sensors, thereby connecting vehicles more and more to each other (V2V) as well as to the surrounding infrastructure (V2I).

As a result of this, Blockchain technology raised enormous attention in research, academia and industry. Various projects and initiatives covering different industrial domains were started in the last months with the goal of identifying real business opportunities for the use of Blockchain in future products, or even to develop concrete (distributed) applications where the use of Blockchain technology can be beneficial, including the automotive industry which has identified potential areas for the use for Blockchains. Recently, automotive car manufacturers BMW, GM, Ford and Renault started the Mobility Open Blockchain Initiative (MOBI) together with other industrial and academic partners such as Bosch, Blockchain at Berkeley, Hyperledger, Fetch.ai, IBM and IOTA [8]. Also, other vehicle manufacturers are evaluating Blockchains or are already working on concrete projects: In 2017, Daimler started a project where Blockchain technology is used to manage financial transactions [9]. Furthermore, the automotive supplier ZF teamed up with IBM and UBS to work on a Blockchain-based automotive Platform called Car eWallet with the goal of paving the way for autonomous vehicles by allowing automatic payments and by providing other convenience features [10].

Hence, Blockchain definitely gained attention in the automotive industry. However, concrete ideas, products and services are needed to show that Blockchain is more than a hyped technology but rather allows the development of new business cases.

2.2 Connected Vehicles and Data Exploitation

Future vehicles will communicate with each other as well as with surrounding road infrastructure to collect valuable information about road conditions and to sense the current traffic situations (e.g., very relevant in traffic intersection scenarios). Furthermore, vehicles will increasingly be connected to the Internet to provide a wide range of convenience services to the users, to gather latest traffic and map information, the current city traffic strategy or even to report an accident (i.e., eCall).

This Internet connection could of course also be used to transfer environmental data collected by the vehicle itself (e.g., camera, Radar, or Lidar data) to the cloud. Intel recently released a statement saying that future (self-driving) vehicles will collect up to 4 TB of data each day [5]. A wide range of different service providers (not restricted to automotive) would be interested in using the collected data in various ways. Sharing the collected data could/should also be beneficial for the owner/driver of the vehicle (see Section 3.1) and, on the down side, will raise serious privacy issues, as the exchanged information could be used to e.g. track down the user's location or analyze the user's behavior (see also Section 3.2).

Several tech startups such as Automile, Dash, and Zendrive, as well as large initiatives driven by vehicle manufacturers such as AutoMat (coordinated by Volkswagen), started initiatives with the goal to collect and utilize data from single vehicles up to entire fleets following different purposes [1]:

i) Provide specific services in order to generate a benefit for the driver or the vehicle/fleet owner in return for sharing data.
ii) Create value by monetizing the collected data coming from a mass of vehicles to third parties, which in turn use it as input for algorithms.
iii) Further improve the business offerings of service providers and develop new services.

Furthermore, in times of a shift of the automotive industry towards digitalization, in times to manage different SAE levels of autonomous driving on the road simultaneously, and in times of the Internet of Things where sensors are increasingly connected to the Internet, the automotive industry still tries to solve many long-known phenomena. These phenomena in-

clude for example the detection of the drivers distraction, fatigue and trust or the vehicles security and safety, which will increasingly be done in the cloud, by feeding the algorithms with sensitive and privacy relevant data from vehicle usage.

Data ownership of vehicle sensor data seems to be yet unclear from a legal perspective. Driver, vehicle owner, passengers, and the vehicle manufacturer may claim their right on certain data. In the AutoMat project, coordinated by Volkswagen, it is argued that as usual in other domains, e.g. in the music show business, "the copyright is distributed proportionally among the members of the value chain" [11]. This copyright distribution would give vehicle manufacturers the right to use the data a driver produces without charge, and thus would bring vehicle manufacturers into the profitable data platform provider role (as they can integrate a data interface in their cars easily). However, from a driver's/vehicle owner's/passenger's perspective, copyright should not be distributed as there would not be any data without them driving the vehicle. This is usual in many domains e.g. digital camera manufacturers do not have a copyright on produced photos, and a competitive market with open data platforms will force innovative solutions and offer more benefits to the data owner to attract data provision.

3 Towards Privacy-Preserving Vehicle Data Sharing

3.1 A Vehicle Data Sharing Ecosystem

A series of stakeholders including vehicle developers, vehicle manufacturers, insurers, and even smart cities could benefit a lot from an open privacy-preserving vehicle data sharing platform, and thus participate in a vehicle data sharing ecosystem. The following Fig. 1, sketches such a vehicle data sharing ecosystem and highlights the connections between the different stakeholders. The figure illustrates stakeholders and advantages for their businesses (based on shared vehicle data), as well as advantages for vehicle owners (using the service the stakeholder provides based on their shared data). Thereby different connection types and privacy levels are envisaged, as different stakeholders are interested in different aspects of the data collected by connected vehicles.

As indicated in Fig. 1, certain service providers such as city planners or map providers are not interested in *who is driving* (i.e., do not need driver-specific information) or *what specific type of vehicle* (i.e., do not need vehicle-specific information such as brand, color, or model). Thus, these services can be satisfied by providing anonymized vehicle usage data. Other (automotive) services targeting on the vehicle development lifecycle (e.g., predictive maintenance or wearout of vehicle components), will only require vehicle-specific data, whereas other services will be mainly interested in user-specific information (i.e., who is/was driving).

The proposed Open Vehicle Data Platform will address the fact that different services require a different kind of data and allow specifying which components of the collected data is shared to enable services. Thereby, privacy is especially addressed as a connected vehicle will not necessarily have to share an entire dataset with a service provider but rather only the data which is really needed by the service provider to provide a specific service. In the simplified model of a vehicle data ecosystem four types of data sharing might be distinguished: sharing anonymous data, driver-specific data, vehicle specific data, or a combination of them.

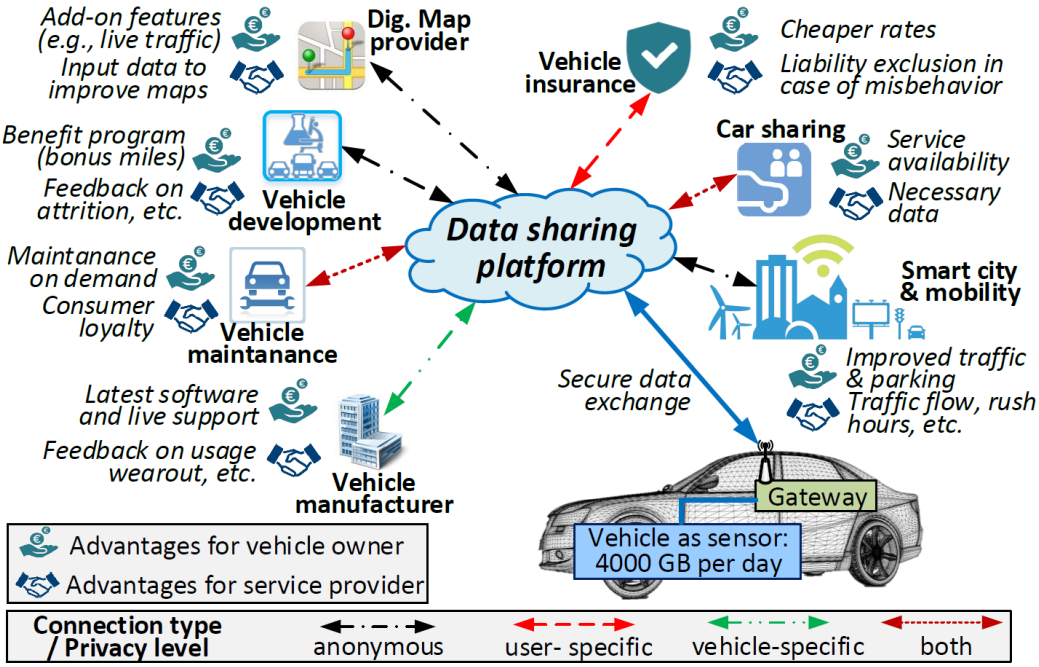

Fig. 1. Vehicle usage data can be used for various services and by different entities and bring advantages to both the vehicle owner/user as well as the service provider / data consumer.

From a more abstract point of view, a vehicle data sharing ecosystem can have several types of actors linked by value flows, as indicated in the e3value model in Fig. 2. For instance, a driver can share driving and vehicle data with a gateway provider who then forwards this data to a data platform provider. In return the driver may receive money but will probably have to mount a vehicle data gateway device in his vehicle. A service provider may use driving data from the data market/platform to establish a preventive maintenance service for drivers. While drivers may pay service providers a fee for consuming this service, the data market receives another fee from the service provider for providing the technical data, which is the baseline for this service.

Consequently, the ecosystem has mutual dependencies and thus allows scenarios where e.g. a driver uses an attractive service which is offered for free, because an organizational consumer (in current scenarios from the market usually without the knowledge of the driver) pays the service provider for the development and service provision in the background, in order to get the data or access to a valuable service based on this data.

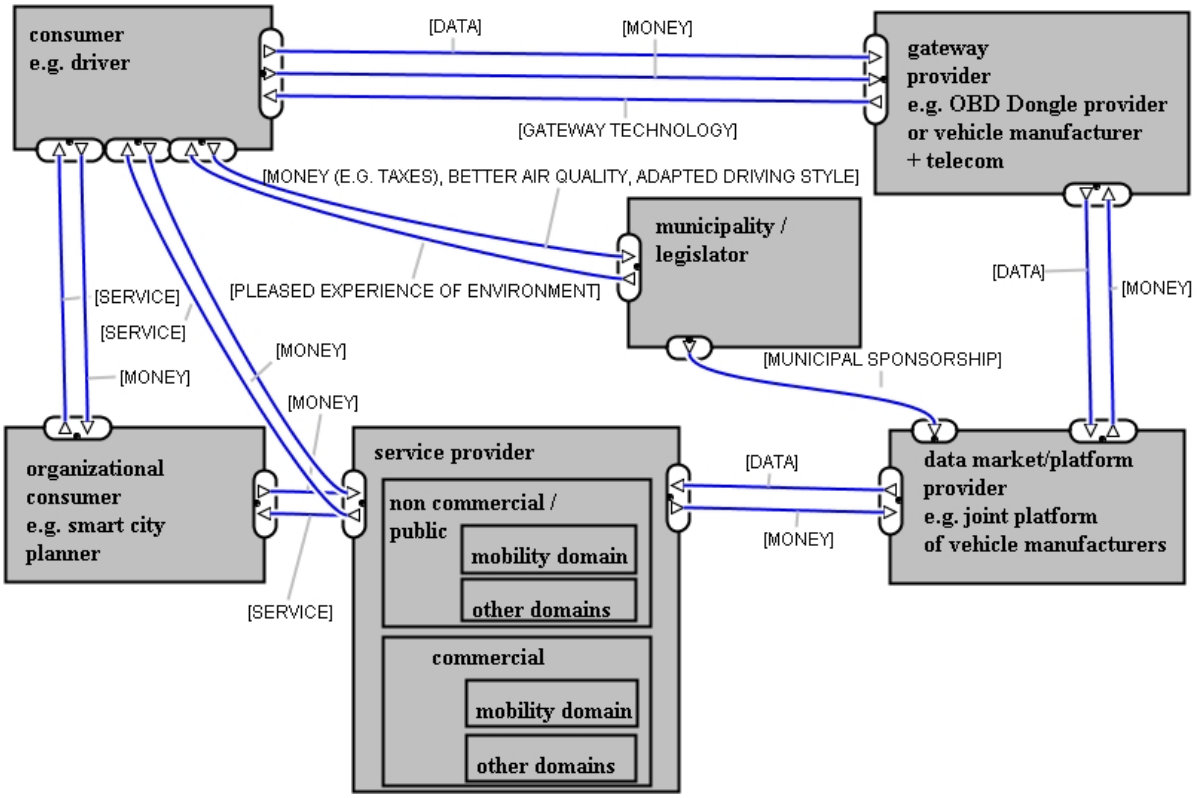

Fig. 2. Actors and value flows (e3value model) of a vehicle data sharing ecosystem.

3.2 The Privacy Challenge for Data Sharing

As discussed before, service providers will monetize data collected by connected vehicles and thus should reward drivers providing the data with certain benefits. In case that the exchange of data between the connected vehicle and the service provider is insecure [12] (or the service provider itself is compromised / acts malicious), privacy issues ranging from tracking down the user to stealing sensitive information can arise. Hence, security and privacy must be addressed when designing a vehicle usage data platform, and, as general rule, a service provider should only be allowed to access relevant (i.e., for providing a specific service) data collected by a connected vehicle.

The driver may conduct a driving behavior which could be interpreted in a negative way and might not be willing to share the so generated driving data with others as this would either imply legal, social or ethical consequences. For instance an aggressive driving behavior might cause social (if shared with friends while benchmarking) or even legal consequences (if captured by the police). Drivers becoming aware of this fact may not want to contribute to any data sharing platform at all if their shared vehicle data could allow to cause negative consequences for them. This fact is also reflected in current studies and surveys, where users are asked about trust and privacy w.r.t. connected vehicles. In one of these studies, Walter et al. [13] details the user concerns regarding connected vehicles and highlights the needs for a privacy-aware data sharing mechanism.

Defining a privacy configuration mechanism w.r.t usability and transparency brings up different opportunities:

One approach is a distinction between vehicle specific and driver specific data, where one can opt to share both of them either anonymized or not, just one or none.

Another approach would be to have four easy understandable levels with decreasing privacy: i) *don't share*, where simply no data is shared at all, ii) *private*, where data is provided e.g. to calculate some basic individual statistics, but cannot be

used for anything else, iii) *anonymized for public usage*, where data can be used like in private level and additionally is provided to public in an anonymized way, and iv) *public,* where all data is provided to public. However, this approach would raise awareness of drivers and service providers would have to adopt the concept, hence it limits possibilities and perhaps opens legal loopholes and at the end of the day it lacks transparency which specific data a service has access to.
Therefore, we argue that it is feasible to adopt the approach of Android smartphone applications, which clusters the access to certain data into topics (i.e. An app needs access to one's contacts and images). The level of detail is a decisive factor for such clusters: emission values can be clustered under a huge topic named *vehicle sensor data* or be seen as an individual *emission values* category, while using quite granular categories would require basic technical understanding of every user. The authors still see improvement potential as this solution has somehow a touch of too much information, comparable to terms and conditions no one really reads carefully.

3.3 A Concept for a Blockchain-based Open Vehicle Data Platform

The concept provided in this section sketches a privacy preserving *Open Vehicle Data Platform*. Instead of going into detail and arguing for certain tools and architectures, we'd rather spread our idea by describing the workflow.

A vehicle is capable of acquiring a lot of valuable data and the driver of the connected vehicle shall be able to decide if and how this data is shared with service providers, as discussed earlier. In the proposed concept and as indicated in Fig. 3, smart contracts based on Blockchain technology are used to specify whether a service is allowed to access data from a certain vehicle and also which kind of data will be shared.
Once an agreement between the connected vehicle and the service provider (i.e., smart contract) is signed, Blockchain technology is exploited to i) make sure that the smart contract cannot be tampered with, as well as ii) to make the smart contract available to so called *Brokers.* The latter provides an online storage, where data collected by connected vehicles is stored securely, and it is also responsible to handle the access of a specific service on data stored on its online storage according to existing smart contracts. Furthermore, the Broker will maintain secure data connections between its online storage and connected vehicles as well as service providers by using suitable protection mechanisms (e.g., TLS).

In the proposed concept, several Brokers will take over the aforementioned tasks, and thereby also allow connected vehicles to switch between different Brokers or even to store data on different locations. The Blockchain will thereby fulfill two essential tasks. Firstly, the Blockchain provides tamperproof storage for smart contracts as well as other transactions, and secondly also provides a way to ensure the authenticity of data collected by a connected vehicle and stored on an online storage, as the hash of a collected dataset is integrated in a transaction and then stored on the Blockchain. Such a transaction can also be seen as a trigger for service providers informing them about the latest available dataset.
Please note that storing data directly on the Blockchain is not advisable from technological point of view. Also note that existing contracts on the Blockchain can simply be revoked or changed by filing a new contract between the connected vehicle and the concerned service provider.

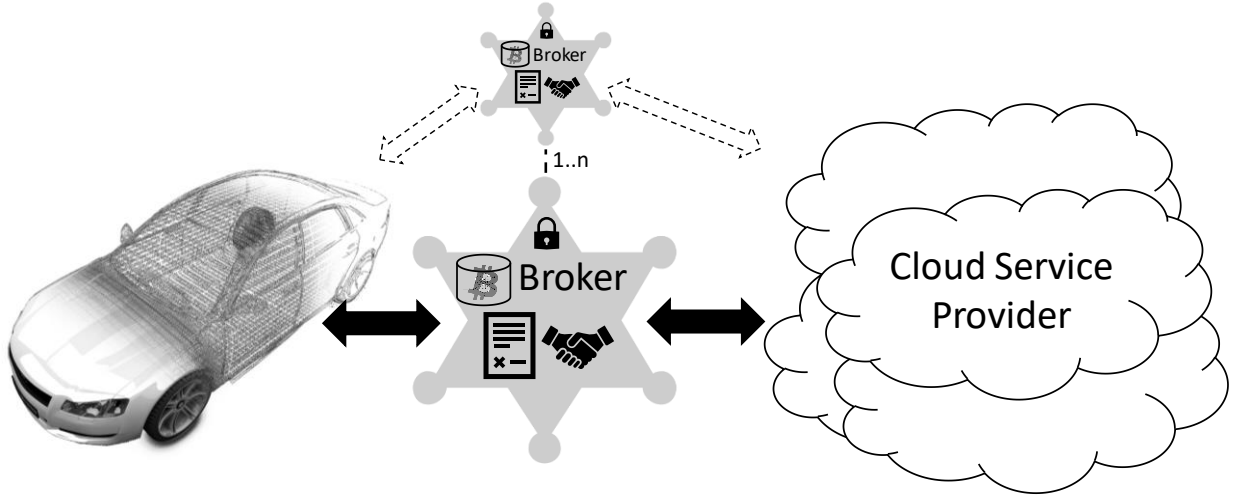

Fig. 3. Data exchange between origin (vehicle) and target (service providers) is managed by a broker using Blockchain technology for smart contracts.

The proposed concept will rely on two different entities which are stored on the Blockchain, namely

i) *Smart contracts*, describing which data is shared with a certain service provider and also specifies the corresponding reward. It will contain information about the Broker that is used to store the collected data, and the timespan in which a certain service is allowed to access the collected data. Each smart contract will be signed by the connected vehicle (is owner) and the service provider before it is stored on the Blockchain;

ii) *Dataset transactions*, containing the hash of a dataset stored on the online storage of a Broker. Every transaction is signed by the connected vehicle (or its owner), and also by the Broker once the dataset was successfully transferred (and verified) to its online storage.

The proposed concept is able to securely interconnect connected vehicles and services providers in a privacy-preserving way, by utilizing Blockchain as tamperproof, decentralized database, as well as by using dedicated Brokers providing a secure online storage and handling access control w.r.t. the stored data. In the following, we summarize seven steps required to share data between a connected vehicle and a service provider and use this example to highlight the benefits of the propose vehicle data sharing platform:

1. Initially, the owner of a connected vehicle wants to use a certain service and, in further consequence, will get into contact with the responsible service provider. In this initial step, the user will be informed about the type of the data the service provider requires to provide a specific service.
2. If the user agrees to this terms, a smart contract specifying the relation between the connected vehicle, its owner, and the service provider is created and signed by the vehicle owner (representing the connected vehicle) and the service provider.
3. Once the smart contract is finalized, it will be stored on the Blockchain.
4. While being used, the connected vehicle will continuously collect valuable data, which is divided into datasets (e.g., after a predefined time or once a certain amount of data is collected) and sent encrypted to the online storage of the Broker. Each transferred dataset is accompanied by a dataset transaction containing the hash of the dataset as well as the digital signature of the connected vehicle (its owner).
5. Hence, the Broker on the one hand can verify that the dataset was not altered while being transferred, and on the other is held from changing the dataset itself as this would invalidate the digital signature already included in the dataset transaction. Once the currently received dataset is verified, the Broker will add its signature (thus completes the transaction) to the transaction and broadcast it on the Blockchain network.
6. Service providers can monitor the Blockchain and will be directly notified about the latest available dataset by looking for relevant dataset transaction. In case such a transaction was found, the service provider requests the dataset by establishing a connection with the Broker.
7. Next, the latter looks for a suitable smart contract on the Blockchain and provides access to data as specified in the smart contract or declines the request in case no smart contract was found or it was revoked.

4 Conclusion, Discussion and Outlook

This paper was aimed to launch the discussion on how the Blockchain technology may help to establish an open vehicle data sharing platform, respecting the privacy of both the vehicle owner and the vehicle driver. Thereby smart contracts are introduced as a mode to fully digitize the data sharing relationship between a consumer (e.g. a driver, who provides his data with the purpose to use services) and a service provider (e.g. a provider of a preventive maintenance service). They describe what kind of data will be provided by whom and for what data exploitation purpose. While these smart contracts are stored on the Blockchain to increase the trust between the vehicle data sharing ecosystem stakeholders, the shared data itself will not be stored on the Blockchain, but for instance on a separate data platform and a data market.

However, a series of issues and research topics remain open and will be targeted in future work:

There are certain pre-requisites vehicles would need for the provided concept. For example, a standardized vehicle data interface across manufacturers, where in general all vehicle data can be provided to extern (to be stored on SD card or on a hard drive if used for private purposes, or to be sent to online destinations), would ease data acquisition. Only data which is marked to be stored/sent to somewhere should be captured, all other data should be deleted or continuously overwritten.

In order to participate, users need to be able to authorize themselves (e.g. to use their privacy settings in every vehicle they use) to the vehicle and the Broker, so they need to register and have an identity.

Using Blockchain technology ensures a privacy preserving way to securely share the data from the vehicle to the service provider. If a service provider gets access to one's data, then this indicates that he is not allowed to resell it unless this is explicitly mentioned in the contract. However, in praxis this can not be prevented with the presented concept, thus privacy can not fully be ensured.

As mentioned in Section 3.2, how to cluster data in useful groups and in which granularity is a topic for future research. An initial version could be as follows:

- Emission data
- Vehicle data (e.g. base weight, number of passengers, year of manufacture, type, brand)
- Environment data (e.g. road topography, temperature outside, rain)
- Traffic data (e.g. detected entities around the vehicle including humans and vehicles, information about the streets throughput rate)
- Driver data (e.g. Driver ID, music channel, mood, fatigue level, driving score, heart rate)
- Ride data (e.g. GPS position, temperature inside, start datetime, target)
- Other data

Acknowledgment

This work is partially funded by the SCOTT (http://www.scott-project.eu) project. SCOTT has received funding from the Electronic Component Systems for European Leadership (ECSEL) Joint Undertaking under grant agreement No 737422. This joint undertaking receives support from the European Unions Horizon 2020 research and innovation program and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway. SCOTT is also funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2017 and April 2020. The authors also acknowledge the financial support of the COMET K2 Program of the Austrian Federal Ministries BMVIT and BMWFW, the Province of Styria, and the Styrian Business Promotion Agency (SFG).

References

[1] Stocker, A., Kaiser, C., Fellmann, M., Quantified vehicles, Journal of Business & Information Systems Engineering, pp. 1–6, 2017.

[2] Stocker, A., Kaiser, C. Quantified car: potentials, business models and digital ecosystems, e & i Elektrotechnik und Informationstechnik, vol. 133, no. 7, pp. 334–340, 2016.

[3] Kaiser, C., Stocker, A., Festl, A., Lechner, G. & Fellmann, M., A Research Agenda for Vehicle Information Systems. In Proceedings of European Conference on Information Systems (ECIS) 2018 (will be published 2018).

[4] European Commission, Data protection in the EU. 2018 [Online], https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[5] Krzanich. B., Data is the new oil in the future of automated driving. 2016 [Online], https://newsroom.intel.com/editorials/krzanichthe-future-of-automated-driving/

[6] Husnjak, S., Perakovi, D., Forenbacher, I., Mumdziev, M. Telematics system in usage based motor insurance, vol. 100, no. January. Elsevier Ltd, 2015, pp. 816–825, conference of 25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014.

[7] Nakamoto, S., Bitcoin: a peer-to-peer electronic cash system, Whitepaper (URL: http://www.bitcoin.org/bitcoin.pdf), 2008.

[8] Russel, J., BMW, GM, Ford and Renault launch blockchain research group for automotive industry, Techcrunch, May, 2018.

[9] Dotson, K., Daimler and LBBW issue $114M corporate bond using blockchain, SiliconAngle, June, 2017.

[10] Kilbride, J., Secure Payments “On The Go” With Blockchain Technology From ZF, UBS and IBM, IBM, September, 2017.

[11] AutoMat-Project. Automat: Connected car data - the unexcavated treasure. Youtube. 2018 [Online], https://www.youtube.com/watch?v=uRjvnahJ-9o

[12] Valasek, C. Miller, C., Remote Exploitation of an Unaltered Passenger Vehicle, White Paper, p. 93, 2015.

[13] Walter, J., Abendroth, B., Losing a Private Sphere? A Glance on the User Perspective on Privacy in Connected Cars. 2018.

Full Authors’ Information

Christian Kaiser
Virtual Vehicle Research Center
Inffeldgasse 21/A,
8010 Graz, Austria
E-mail: Christian.Kaiser@v2c2.at

Marco Steger
Virtual Vehicle Research Center
Inffeldgasse 21/A,
8010 Graz, Austria
E-mail: marco.st1987@gmail.com

Ali Dorri
School of Computer Science and Engineering, University of New South Wales
K17, Barker St,
Kensington NSW 2052, Australia
E-mail: ali.dorri@unsw.edu.au

Andreas Festl
Virtual Vehicle Research Center
Inffeldgasse 21/A,

8010 Graz, Austria
E-mail: Andreas.Festl@v2c2.at

Alexander Stocker
Virtual Vehicle Research Center
Inffeldgasse 21/A,
8010 Graz, Austria
E-mail: Alexander.Stocker@v2c2.at

Michael Fellmann
University of Rostock
Albert-Einstein-Straße 22 (Konrad Zuse Haus),
18059 Rostock, Germany
E-mail: michael.fellmann@uni-rostock.de

Salil Kanhere
School of Computer Science and Engineering, University of New South Wales
K17, Barker St,
Kensington NSW 2052, Australia
E-mail: salil.kanhere@unsw.edu.au

Keywords

Blockchain Technology, Vehicle Data Sharing, Automotive Security and Privacy, Open Vehicle Data Platform, Privacy Settings, Quantified Vehicles;