ENABLING THE V2X ECONOMY REVOLUTION USING A BLOCKCHAIN-BASED VALUE TRANSACTION LAYER FOR VEHICULAR AD-HOC NETWORKS

Research full-length paper

Track: Blockchain Applications: issues, challenges and opportunities

Leiding, Benjamin, University of Göttingen, Göttingen, Germany,
benjamin.leiding@cs.uni-goettingen.de

Vorobev , William V., Chorus (Proof-of-Stake Inc.), New York, USA,
will@chorus.technology

Abstract

The next generation of tightly interconnected vehicles offers a variety of new technological as well as business opportunities. Those vehicles form so called vehicular ad-hoc networks (VANETs) in order to enable vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-human (V2H), or in general vehicle-to-everything (V2X) communication and interaction. A variety of manufacturers started implementing specific use cases, but limited to their own brands and products. However, a platform- and manufacturer-agnostic default standard for interactions and transaction within this new economy is still missing. This paper fills the gap in the state of the art by introducing a novel blockchain-based V2X platform that enables a transaction and interaction layer for goods and services required to kick-start the upcoming V2X economy. We present the general functions and features of the system, outline the requirements and goals as well as the architecture of the V2X platform. Moreover, we detail the system engagement processes of the identified stakeholders inside the V2X ecosystem and the theoretical foundations of those interactions and transactions.

Keywords: Blockchain, Autonomous Vehicles, V2X Economy, Self-Driving Cars, VANET, Smart Contract, Transportation-as-a-Service, TaaS.

1 Introduction

Despite steadily growing public transport networks and systems, especially in most first world countries, cars are still the default standard for urban transportation. In the US, "about 86 percent of all workers commuted to work by private vehicle, either driving alone or carpooling" (McKenzie, 2015), even though in recent years the numbers remained relatively stable after decades of consistent increase. Similar applies to other industrialized countries (Berends-Ballast et al., 2016)(Goodyear and Ralphs, 2009) though the overall percentage of vehicle commuters in Europe is lower than in the US (Cortright, 2016). While it is currently normal to own a vehicle and commute on a day-by-day basis, the future will bedifferent due to the progressing evolution of self-driving cars and autonomous vehicles. The car-sharing economy that developed in recent years in combination with autonomous cars results in a so called *Passenger economy* (Lanctot, 2017). However, the progressing automation and driverless transport that enables the passenger economy represents only a small aspect of the potential of these new technologies. In 2013, Mike Hearn described[1] a vision where most users do not own cars any more and instead use services provided by autonomous vehicles that own themselves. Those autonomous vehicles (AVs) offer services and goods to earn- and pay money to acquire services that they cannot provide on their own, e.g., cars renting a parking lot, paying for a charged battery, using toll roads, or simple service check ups. The idea of V2V and V2I or in general V2X (vehicle-to-everything) will fuel various new business fields.

Certainly, traditional payment systems such as paper money, or fiat currencies in general, are not suited to be part of this new economy. There are slow, depend on third parties, e.g., banks, and suffer from bureaucratic overhead. Blockchain technology and cryptocurrencies offer a promising alternative payment solution that comes with several additional technological advantages that we will discuss later on. The blockchain technology, also referred to as distributed ledger system, is most noticeably known for providing the foundation of the peer-to-peer (P2P) cryptocurrency and payment system Bitcoin (Nakamoto, 2008), but nowadays there are various different platforms out there, e.g., (Goodman, 2014)(Popov, 2018)(Wood, 2014). Several companies already started to prototype applications that combine vehicles and blockchains. Porsche is researching different payment-related applications for vehicles[2] whereas MacNeille et al. (2018) focuses on traffic marshalling. As expected in the early days of a new technology, companies focus on selective solutions for very specific problems or use cases and the resulting solutions are only compatible with their own products. What is currently missing is an industry standard for the V2X economy that can easily be integrated with self-driving and (semi)-autonomous cars or even nowadays cars.

This work addresses the detected gap by proposing a novel blockchain-based solution, thereby answering the question of how to implement a manufacturer- and blockchain-agnostic transaction layer that enables a V2X platform for goods and services? In order to answer this question with a separation of concerns, we pose the following sub-questions: What are the critical functional- and non-functional requirements? What is the corresponding architecture of the V2X platform? What are the system-engagement processes for the stakeholders?

The remainder of this paper is structured as follows: Section 2 introduces supplementary literature and related work. Section 3 analyses the requirements of the system and Section 4 outlines the resulting system architecture that we derive from the requirements. Afterwards, Section 5 expands on the system-engagement processes for the stakeholders. Finally, Section 6 concludes this work and provides an outlook on future work.

1 http://www.bbc.com/news/technology-30998361

2 https://newsroom.porsche.com/en/themes/porsche-digital/porsche-blockchain-panamera-xain-technology-app-bitcoin-ethereum-data-smart-contracts-porsche-innovationcontest-14906.html

2 State of the Art and Supplementary Literature

The following section provides background information and describes related work regarding previous ideas and concepts that focus on blockchain-based VANET platforms. First, Section 2.1 introduces the general concepts of blockchain technology, terms and frameworks. Afterwards, Section 2.2 focuses on the fundamentals of vehicular ad-hoc networks. Section 2.3 illustrates V2X introduces running cases and examples. Finally, Section 2.4 discusses related work.

2.1 Blockchain Technology

A blockchain consists of a chronologically ordered chain of blocks and every block consists of a certain number of validated transactions. Each of those blocks links to its predecessor by a hash reference. As a result, changing the content of one block also changes all succeeding blocks and hence breaks the chain. Blocks are stored on and verified by all participating nodes. While the initial Bitcoin blockchain only supported a very limited set of scripting instructions, the succeeding generation of blockchain platforms, e.g., Ethereum (Wood, 2014) or Tezos (Goodman, 2014), provide Turing-complete programming languages on the protocol-layer level in order to enable smart contract capabilities. Smart contracts are “orchestration- and choreography protocols that facilitate, verify and enact with computing means a negotiated agreement between consenting parties” (Dai et al., 2017). Hence, the entities participating in the enactment of a smart contract establish binding agreements and deploy applications using such smart contracts in order to provide blockchain-based applications. Those application are as versatile as smart contracts itself and enable a vast variety of services including applications within the financial sector (Nguyen, 2016)(Guo and Liang, 2016), authentication and identity solutions (Bochem and Leiding, 2018)(McCorry et al., 2015), reputation systems (Calcaterra et al., 2018) as well as platforms for Internet-of-Things (IoT) applications (Christidis and Devetsikiotis, 2016)(Ouaddah et al., 2017) and many more.

The blockchain concept is particularly interesting for the V2X economy for three reasons: First, it removes the need for trusted third parties and instead enables trust-less transaction enactment. Second, transactions that were agreed up on cannot be changed later on since the underlying blockchain can be assumed to be resistant to data manipulation. Third, no human interaction is required for any kind of transaction between vehicles or machines in general.

2.2 VANETs

Communication between vehicles, road infrastructure and Internet-based services is a key enabler for the upcoming generation of vehicles. So called vehicular ad-hoc networks provide an abstract concept that models the different components that are required for V2X communication. Figure 1 illustrates the main components of VANETs: road-side-units (RSUs), vehicles, on-board-units (OBUs) and application-units (AUs). RSUs are strategically placed along roads or in dedicated locations such as crossroads. Typically, RSUs provide short range communication based on IEEE 802.11p radio technology but can also be equipped with other network devices in order to provide communication within the infrastructural network (Al-Sultan et al., 2014). OBUs are mounted onto a vehicle and used for data exchange. To do so, short range wireless- or radio communication is used to exchange these information (Baldessari et al., 2007). Closely linked to the OBU is the AU, they might even reside in the same physical unit or as a mobile until that is regularly removed from the vehicle (e.g smartphones). The AU provides an execution environment for applications that utilize the OBU's communication capabilities (Al-Sultan et al., 2014)(Baldessari et al., 2007).

Communication in VANETs occurs either inside a vehicle between AUs and OBU, wirelessly between different vehicles (V2V), vehicles and infrastructure (V2I) or vehicles and the infrastructure via broadband (V2B) (Faezipour et al., 2012). For authentication purposes, each network participant is equipped with a unique public/private key pair that resides in a tamper-proof-device (TPD). In blockchain terms, the TPD is similar to an external hardware wallet.

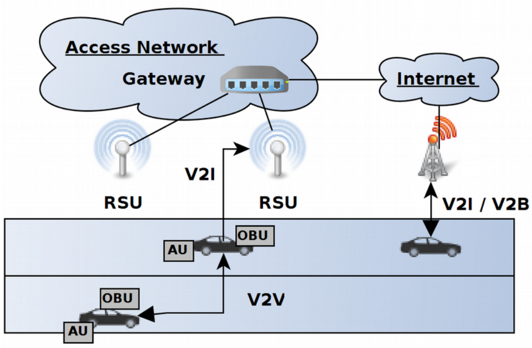

Figure 1. General VANET architecture (Based on Baldessari et al. (2007) and Leiding et al. (2016)).

2.3 Running Cases

In order to provide a better understanding of the vast variety of use cases and scenarios enabled by an universal V2X platform, we outline examples for each of the different main interaction and transaction categorizes: V2H, V2V and V2I. The running cases are used throughout the paper to illustrate certain aspects of the system.

2.3.1 V2H – Transportation as a Service (TaaS)

In the future most likely people will not poses their own vehicles any more. Instead, the vehicles may own themselves or they are owned by the government or private corporations (Pavone, 2015)(Chong et al, 2013)(Greenblatt and Shaheen, 2015). The self-owning vehicles are produced by a manufacturer and pay of their production cost by offering transportation services - transportation-as-a-service (TaaS). Users that are looking for a transport request the service via an application interface and trigger the service enactment. Such a TaaS concept provides several advantages: First, a vehicle-sharing economy reduces the amount of vehicles required to manage the general transportation of entities. Second, vehicles that own themselves can charge lower prices (compared to profit-oriented companies) since they only have cover their own expenses and not make a profit. In case a vehicle cannot find a new transportation task, it can search for an empty parking spot and idle for some time until there are new jobs. Finally, the TaaS concept is not limited to human transportation and applies to transportation of goods via drones, ships, planes and trains as well.

2.3.2 V2V – Road Space Negotiation and Mitigating Traffic Congestions

Traffic congestions are the result of a scarce resource – road space. V2V interaction and transaction offers opportunities to either mitigate traffic congestions via V2V collaboration, or to open up a market for road space negotiations. The first option utilizes the progressing interconnection and digitalization of vehicles that enables collaborative traffic flow management, e.g., using alternative routes, making optimal use of available road capacities, and so on (Lighthill and Whitham, 1955)(Wang and Jing, 2001).(Daganzo, 2002)(Kesting et al., 2008). Given the case that even perfect traffic management cannot provide sufficient throughput, network participants may start to trade road space as a good. Vehicles with a preference to arrive as soon as possible can pay another vehicle to switch place in a traffic jam in order to arrive faster at the final destination (Leiding et al., 2016)(MacNeille et al., 2018). Usage of priority lanes is another example but not always an option.

2.3.3 V2I – Automated Payment Services

In order to ensure proper maintenance of roadsides and the technological back-end of VANETs a minor fee has to be charged by the infrastructure providers. Toll road payments are already common in many countries, but still require human interaction. An automated payment execution based on a predefined usage model (travelled distance, time, data consumption, etc.) illustrates the most common example of V2I transaction and interaction services. As suggested by Leiding et al. (2016) further infrastructure enabled optional applications and services such as traffic jam notifications might also be paid in a similar manner. At the same time, those services represet a different type of V2I service provision.

2.4 Related Work

Leiding et al. (2016) envision a blockchain-based solution for services within self-managed vehicular ad-hoc networks (VANETs) such as traffic management, toll payment systems and traffic regulation enforcement. MacNeille et al. (2018) propose a solution for the specific use case of enabling traffic marshalling via a blockchain system that is similar to one of the ideas described by Leiding et al. (2016). Even though the proposals of both author teams overlap in some areas of the V2X ecosystem with our platform, both approaches focus on a rather limited number of specific use cases rather than following the idea of a holistic blockchain- and manufacturer agnostic solution.

Davidsen et al. (2018) present the concept of a global trading platform so that IoT devices can autonomously buy and sell data produced by those devices. Special focus is given on the truthfulness of traded data since the data manipulation may cause serious damage to the buyer. Sikorski et al. (2018) propose and implement a blockchain-based M2M electricity market for chemical industry where energy producers and consumers are trading electricity with each other via a blockchain platform, whereas Mengelkamp et al. (2018) a blockchain-based smart grid that facilitate a sustainable local energy markets. The research presented in these three papers is complementary to ours since several entities within a V2X ecosystem are either interested in buying/selling data or electricity, assuming that electric vehicles and other entities require these type of energy for operation purposes.

3 System Design and Architecture

In order to identify, structure and formalize the critical requirements and stakeholders on an abstract level, we use one part of an Agent-Oriented Modelling (AOM) method (Sterling and Taveter, 2009), i.e., goal models. The produced goal model is used in subsequent Section 4 to derive the system architecture. The resulting system architecture and specifications serve as implementation guidelines.

3.1 AOM Goal Modelling

In system development and software engineering, good requirements follow certain characteristics. According to (Davis,1993)(IEEE Computer Society et al., 1998) requirements address one issue only and are completely specified without missing information. Moreover, they have to be consistent and do not contradict itself, or in correlation with other requirements. Finally, a requirement must also be atomic and without conjunctions (Norta et al., 2014).

The AOM methodology is a socio-technical requirements-engineering approach used to model complex systems that consist of humans, devices, and software agents. An AOM goal model enables both, technical- and non-technical stakeholders, to capture and understand the functional- and non-functional requirements of a complex system. Figure 2 depicts the three main elements that an AOM goal model comprises in order to capture the system requirements and goals. Roles of involved entities are represented in form of sticky men, whereas functional requirements are depicted as parallelograms. Note that in the specific context of this work, a sticky man does not exclusively represent human entities but rather all kinds of entities, e.g., also vehicles or infrastructure. Functional requirements are referred to as goals. Non-functional requirements are depicted as clouds and refer to quality goals of the modelled software system. The AOM goal model follows a tree-like hierarchy with the root value proposition of the modelled system at the top. Subsequently, this main goal is decomposed into sub-goals where each sub-goal represents an aspect for achieving its parent goal (Marshall, 2014). The goals are further decomposed into multi-layered sub-goals until the lowest atomic level is reached. Additionally, roles and quality goal may be assigned to goals and are inherited to lower-level goals. The following Section 3.2 introduces the top-level goal model our system, followed by Section 3.3 focusing on the non-functional goals of the AOM goal model.

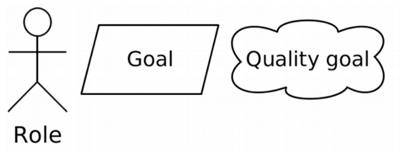

Figure 2. Selection of AOM notation elements.

3.2 Top-Level AOM Goal

Figure 3 presents the top-level AOM goal model of the system using the modelling method described above. The main value proposition is to provide a V2X platform and the corresponding interaction and transaction layer for (autonomous) vehicles, thereby representing the root of the goal model. The complex main value proposition is split into four sub-goals representing the four main components.

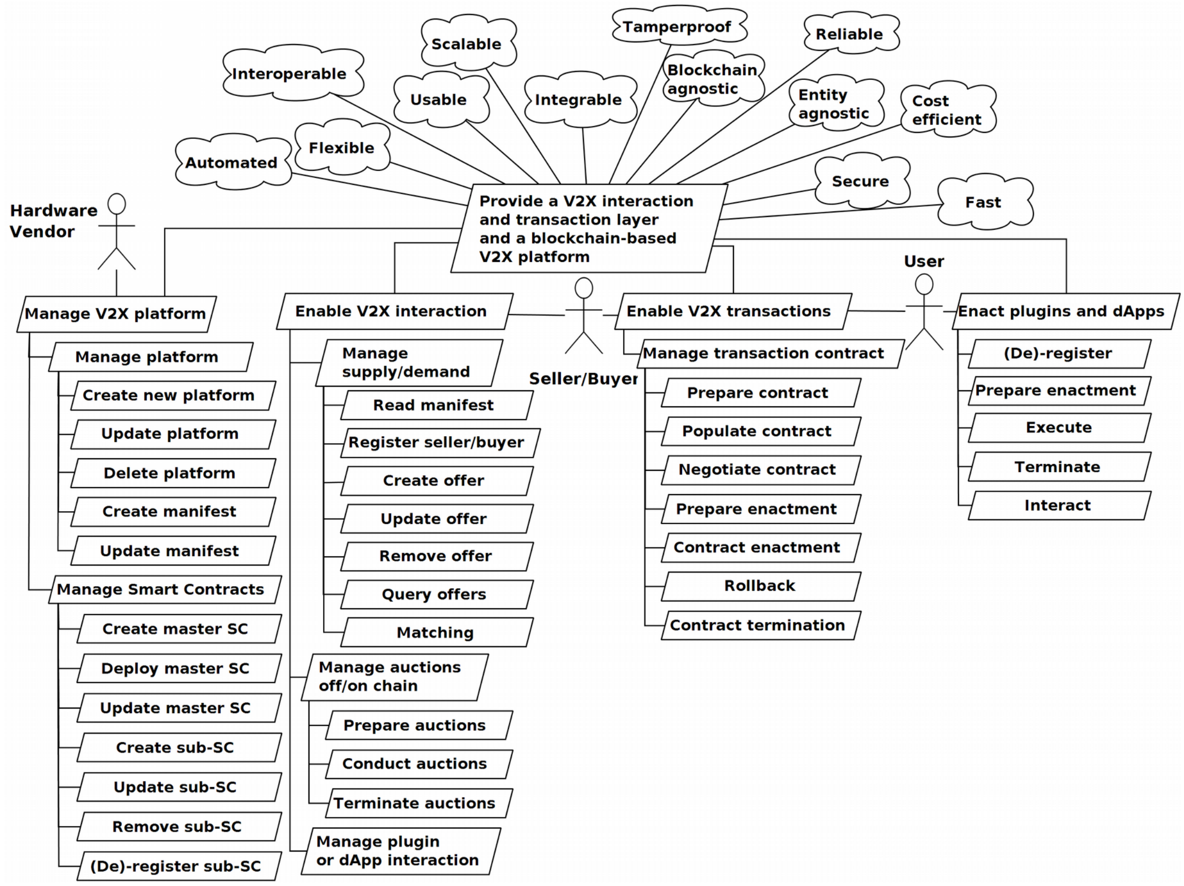

Figure 3. Top-level goal model representation.

First, a component for managing the V2X platform. This functional goal includes managing certain aspects of the platform itself, e.g., creating, updating, deleting a new platform, as well as the management of the underlying smart contracts. Each platform operates a master smart contract and several sub-smart contracts. While the master contract is in charge of platform management and controlled by the hardware vendor, the sub contracts each offer service provision for a specific service, interaction, transaction or application.

The second functional goal enables V2X interaction. That mostly covers on- and off-chain supply and demand administration. Entities may register offers or requests on-chain in order to attract business partners, but for other use cases a local supply demand management off-chain is more suitable, e.g., road-space negotiation. Supervising on- and off-chain auctions is basically equivalent to the on- and off-chain supply and demand management. Besides that, plug-ins and decentralized applications (dApps) of the ecosystem might use platform smart contracts for service enactment and have to be integrated as well in this context.

The third functional requirement, that represents the third main component, enables V2X transaction via the blockchain. The most important part here is the transaction management via a smart contract lifecycle (detailed later on in Section 5.1). Finally, the fourth functional requirement focuses on the enactment of various plug-ins and dApps. Applications and plug-ins have to be registered, prepared for enactment, executed and terminated. Moreover, they have to interact with various entities of the ecosystem depending on the use case. Since nowadays most blockchains offer Turing-complete smart contract support, the variety of applications and plug-ins in our ecosystem is quite vast.

3.3 Non-Functional Requirements

Besides the four sub-goals of the top-level AOM goal model, we further identify thirteen quality goals of the main value proposition that are inherited to all refining sub-goals. A *scalable* system design is necessary to provide services to a large quantity of users and customers. A further property that supports to achieve this scalability is the non-functional requirement *automated*, that refers to a high degree of process automation eliminating the need for human interaction, e.g., tedious and repetitive tasks. *Cost efficiency* is another important quality goal. *Flexible* digital collaboration is a highly dynamic process that involves the enactment of a multitude of variations of activities, participating partners as well as the exchange of diverse data (Norta, 2008). Thus, we must allow diverse collaboration scenarios and permit the inter-organizational harmonization of heterogeneous concepts and technologies between participating entities. Another key property of the system is being easy to use (*Usable*) for business collaboration. According to Norta et al. (2014), easy usability also includes the support of proper *error avoidance* in order to “anticipate and prevent common errors that occur during a collaboration configuration. Closely related is *error handling*, to help with system support a user to recover from errors. *Learnability* refers to how quickly users master using the system” (Norta et al., 2014).

Moreover, we assign two additional quality goals that ensure a *blockchain-agnostic* as well as *entity-agnostic* design. The solution should be neither limited to a specific blockchain nor vehicle hardware of a specific vendor. *Interoperable* hardware and software design is another consequence of the previous quality goals as well as easy integration (*integrable*). It is crucial to interoperate at runtime with information systems supporting other business functions. Furthermore, a *secure* service provision is crucial in terms of operational security, e.g., protect user accounts and personal data from unauthorized access, secure data transfer within the system between entities or preventing data- and information leaks as well as preventing accidents. A *reliable* enactment of all interactions and transaction facilitates the previous goals as well. Data communicated internally as well as externally has to be protected against unauthorized tampering (*tamperproof*) in order to protect business collaborations, but also ensure the safety of participating entities. Finally, since cars and similar vehicles move much faster than humans, a *fast* service provision is essential for most tasks.

The presented goal model is used in the following Section 4 to derive the system architecture. We do not list all details of the further refined AOM goal model in this paper due to space constraints and in order to focus on the most relevant system components and features.

4 System Architecture

The abstract system architecture is derived from the functional- and non-function requirements of the AOM goal model presented earlier. The services are powered by a service-oriented architecture (SOA) that is comprised of different designated components. Each of these components is self-contained, well-defined and provides a specific set of services (Erl, 2005)(Perrey and Lycett, 2003). Dedicated services and components may also consist of other underlying sub-services (Rosen et al., 2012).

In the following, a technology-agnostic UML-component-diagram representation is used to illustrate the system architecture (Booch et al., 1996)(Object Management Group, 2007). The UML notation elements used to model the architecture are presented in Figure 4. In UML, components are represented as rectangular boxes and labelled either with the keyword *component*, or with the component icon in the right-hand upper corner. A component may consists of further sub-components and is implemented by one, or more classes, or objects. Moreover, components are reusable and communicate via two types of interfaces as illustrated in Figure 4. Small squares depict ports that are attached to the border of components and expose required and provided interfaces. Ports may also specify inputs and outputs as they operate uni-, or bi-directionally (Booch et al., 1996)(Object Management Group, 2007). Once more, sticky men are used to depict entities and their interactions with the system.

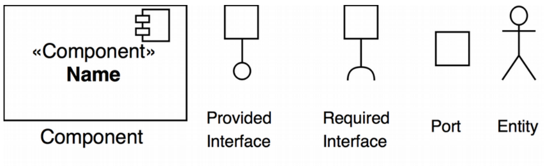

Figure 4. UML-component diagram notation elements.

The remainder of this section first introduces an abstract high-level overview of the system architecture and components. Further illustration present selected sub-components of our architecture.

4.1 High-Level Architecture

The highest architecture abstraction level of our system is depicted in Figure 5. The representation is divided into two distinct packages, e.g., the Blockchain package and the Vehicle-System package. In UML, packages are used "to group elements, and provide a namespace for the grouped elements" (Object Management Group, 2007). In the context of this architecture illustration, packages are used to provide a separation of concerns between the blockchain part and the vehicle-related system components, as well as the mobile smartphone application. The vehicle-system package consists of three main components, e.g., the firmware, the vehicles manufacturer OS and the component managing the underlying hardware of the vehicle, and several smaller components that are detailed in Section 4.2.

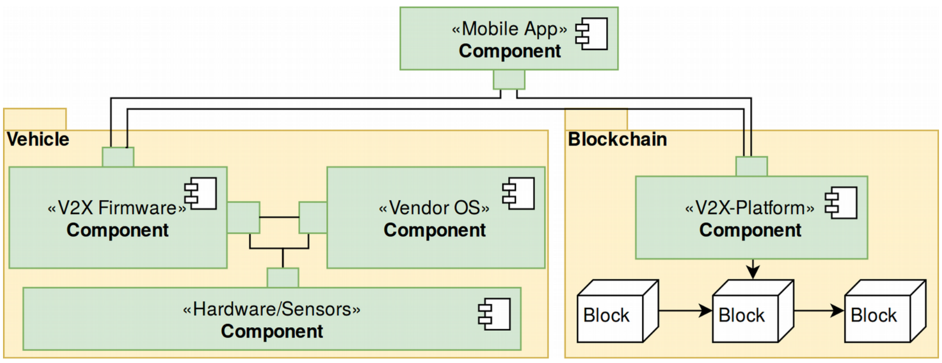

Figure 5. High-level architecture of the V2X system.

The blockchain package comprises the V2X platform itself and the blockchain utilized to enable service provision. Section 4.2 explains each of the units illustrated in Figure 5 in more detail.

4.2 Selected Architecture Refinements

The following section outlines some selected refinements of the high-level architecture presented in Figure 5. We simplified certain aspects due to space constraints and to reduce technical complexity. First, Figure 6 shows the different components of the *Mobile App* component, e.g., the user interface (UI) component, the settings/preferences component, the wallet component, the communication component and the application management component. The UI-component is the gatekeeper for the user and used to control all functionalities from the user side and also to interact with the system. The user can set preferences and change settings, visualize wallet balances, activate plug-ins or applications (we only listed two as an example) such as the “Traffic-Application”-plug-in. The wallet component holds the users public and private key pair that represent the wallet address. The user can transfer tokens from and to his/her wallet to use compatible services or applications. The user's smartphone is connected to the vehicle component and utilizes the communication component to interact with the vehicle component as well as the V2X platform.

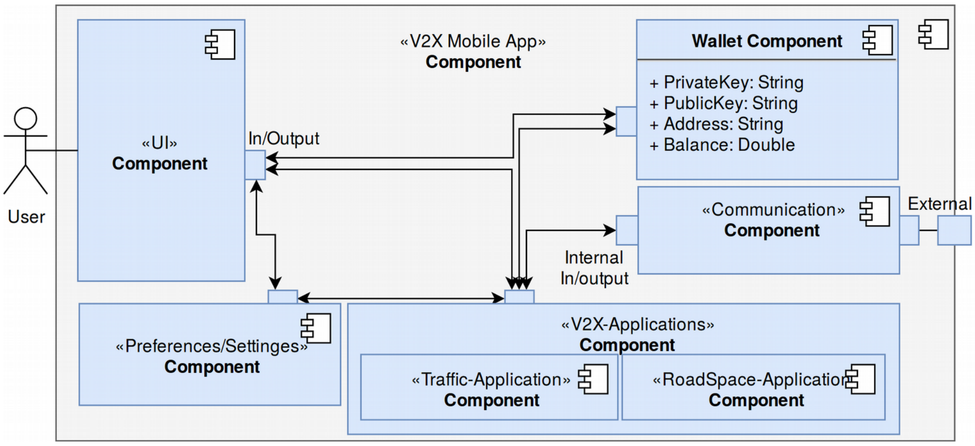

Figure 6. Refined illustration of the V2X Mobile Application component.

Next, Figure 7 presents a more detailed view of the *vehicle* sub-system. This sub-system is located in a dedicated box that is connected to the user's smartphone via Bluetooth or WIFI, the V2X platform via the Internet, to other vehicles via the WAVE protocol stack (Li, 2010)(Uzcátegui et al., 2009) as well as the vehicle via the CAN bus – hence we have a dedicated communication component on the left as well as the right for external- and in-vehicle communication. The CAN bus interface is used to query information from the car such as speed, steering, breaks and many more. The information are used by applications and plug-ins to provide their services. The logic of the applications mostly resides in the plug-in component of Figure 7 while the application component in Figure 6 is mostly used to control the applications and enable/disable them on the dedicated box. In the future, a dedicated box may not be necessary and manufacturers integrate all necessary functionalities into their own operation system or firmware.

Due to the speed of moving vehicles, most of the time on-chain auctions are not an option and instead auctions or negotiation on a local level between nearby vehicles are necessary. The auction component contains all functionalities to do so as well as settings that control the auction preferences of a vehicle. More details on the actual workflow of the off/on-chain auctions are available in Section 5.2.

In the future, when most people do not own cars themselves any more, users can transfer tokens to the vehicles wallet to pay for TaaS and the vehicle uses these earnings to pay for electricity or maintenance. Hence, the vehicle also has a separate wallet for this purpose.

Finally, Figure 8 presents a more detailed view of the *V2X platform* sub-system. As for all the other sub-system, the V2X platform contains a communication component managing the communication between the platform and the blockchain, or vehicles. In addition, the respective platform management entity (a vehicle manufacturer may operate their own compatible platform) has access to an administration interface. The administrator uses the interface to maintain the platform and the corresponding smart contracts as well as the user management. Similar to the auction component in the previous Figure 7, the V2X platform has a component that takes care of on-chain auctions using the same auction algorithms. Auctions may result based on the supply and demand management that is conducted in the corresponding component. Finally, similar to the application/plug-in components in the mobile application and the vehicle, we also have a pendant of these component in the V2X platform. Here, the component is used for application/plug-in related interaction and transaction enactment.

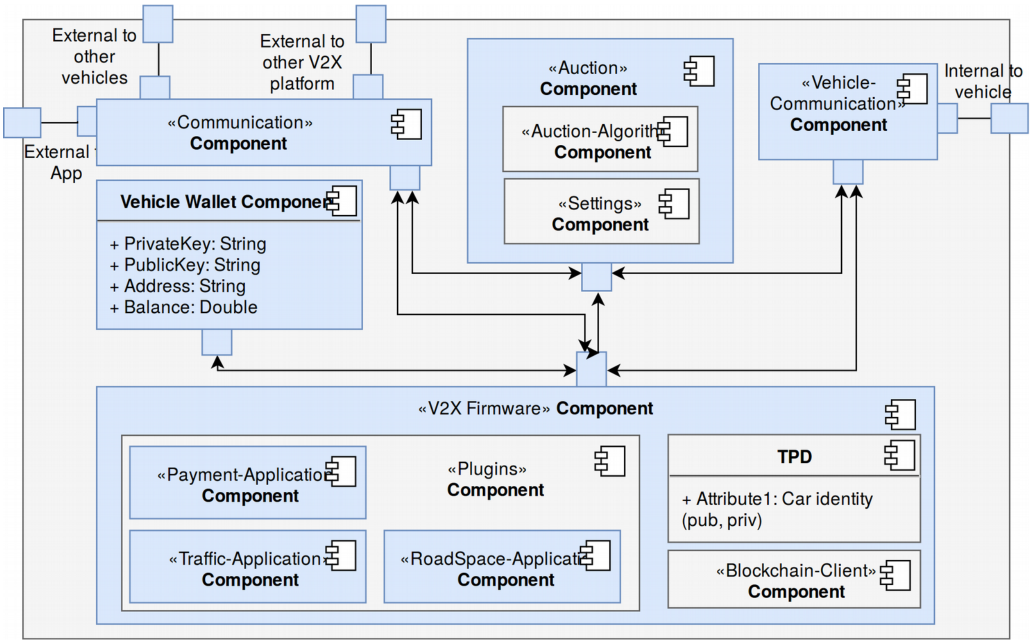

Figure 7. Refined illustration of the Vehicle sub-system.

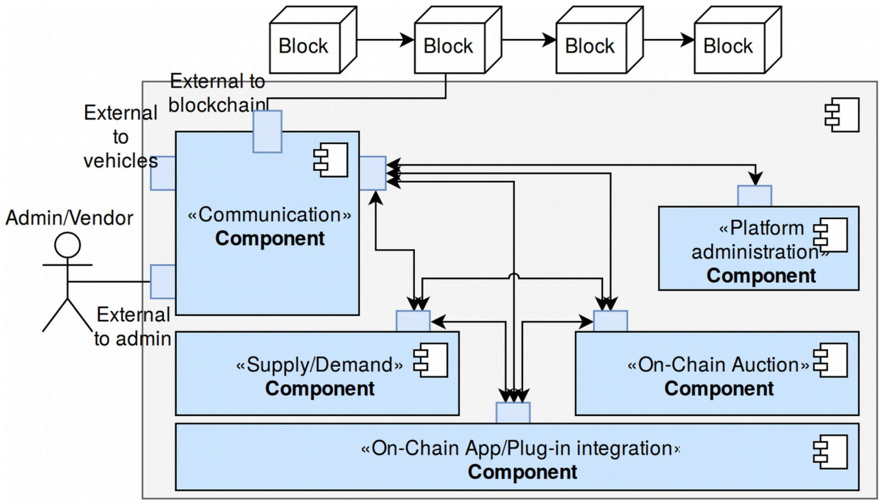

Figure 8. Refined illustration of the V2X-Platform sub-system.

Next, in Section 5 we present the system-engagement processes of the V2X system and outline the smart contract negotiation lifecycle, interaction workflow of the on/off-chain auction algorithms and the V2X platform integration.

5 System Engagement Processes

The transaction and interaction layer automates and simplifies VANET-based V2X service provision on several levels. A core element of many of the use cases is a smart contract-based negotiation and contract enactment between entities that are the result of collaborating tasks and sub-processes. For example, two vehicles conduct a road-space negotiation auction that results either in a change of positions or is aborted. This process potentially involves payment processing, further local as well as global communication and local match-making between vehicles. On an abstract level, most of the use cases presented earlier in this paper follow at some point a similar procedure on smart-contract level. Same applies for scenarios that involve a price negotiation or auction. In the following, we introduce these two abstract processes in more detail. The processes are represented using Business Process Model and Notation (BPMN) (Chinosi and Trombetta, 2012) and sequence diagrams. Consequently, Section 5.1 details the BPMN representation of the generalized contract negotiation lifecycle, followed by Section 5.2 that details the auction mechanism of our platform. Finally, Section 5.3 deals with platform integration.

5.1 Smart Contract Negotiation Lifecycle Management

The abstract smart contract negotiation lifecycle, as illustrated in Figure 9, is divided into the following stages: a) preparatory, b) negotiation, c) contract execution d) rollback and e) the contract expiry stage. During the preparatory stage, information regarding the involved entities, such as identifiers and wallet addresses are incorporated into the contract. In addition, the conditions of the requested contract are formally defined by specifying, e.g, the content and target of the contract. Following the example of the cab service for a human, this might include the start location, final destination and price. The conditions of the requested cab-ride mainly depend on information such as the travel distance and fuel/ energy consumption of the vehicle. In case the vehicle and the user agree on the negotiated conditions, both parties sign the contract and express their approval - if no agreement is reached, a contract rollback is triggered. After signing the agreement, the contract execution phase is triggered and the vehicle picks up the user.

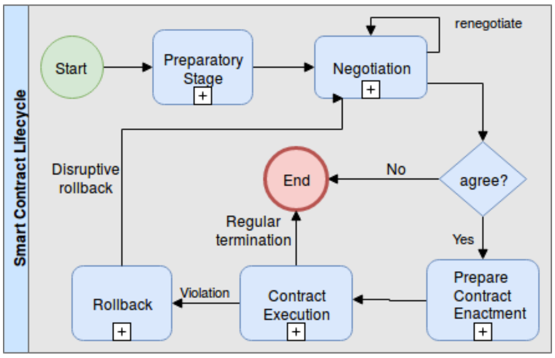

Figure 9. Smart contract negotiation lifecycle (Based on Dai et al., 2017).

The transportation contract terminates, or expires either after the user arrives at the final destination, or when the contract is prematurely terminated. Failing to transport the user to the agreed final destination might result in an immediate rollback of the smart contract or invokes some kind of a mediation process that is supervised by a conflict resolution escrow service that is not depicted in Figure 9.
The presented lifecycle not only covers trading negotiation but rather all kind of contract enactments. The user prepares and negotiates a contract with a collaboration partner and executes it in case that both parties agree on the specifications. That also includes incentives in case the user behaves correctly, e.g., reward, as well as punishment of bad behaviour, e.g., paying a penalty. A serious violation of the contract from any of the involved parties might result in an early termination of the contract or even a rollback.

5.2 Auction and Negotiation Algorithm

A further important core concept of our V2X system is to support the exchange and provision of goods on services between entities. When trading goods and services, the buying and the selling party usually have contrary goals in terms of pricing. The seller's goal is to maximize profits while the buyer tries to minimize the costs. Auctions are a common approach to reach a consensus on a certain price between buyer and seller. We designed an auction algorithm based on the concept of so called Vickrey Auction (Movdovanu and Tietzel, 1998)(Vickrey, 1961). During a Vickrey auction, participants exchange sealed bids. Each bidder submits a written and signed bid without having any knowledge of the bids of the other participants. After submitting all bids, the sealed bids are opened and the highest bidder wins. But instead of paying the price of this highest offer, the price paid is the second-highest bid. Due to space constraints and the technical nature of this paper we will not cover the economical and game theoretical implications concepts of Vickrey auctions and instead refer the reader to specific supplementary literature, e.g., (Ausubel and Milgrom, 2006)(Edelman et al., 2007)(Lucking-Reiley, 2007)(Movdovanu and Tietzel, 1998)(Vickrey, 1961).

Figure 10 presents the sequence diagram of the auction algorithm that is either run locally (off-chain) between auction participants that reside in close proximity to each other, or on-chain when interacting on a global scale. We assume a scenario with three buyers and one seller, but in general the auction algorithm works with multiple buyers and sellers – or only one buyer and seller. As mentioned in our AOM goal model (Figure 3), speed is one of the non-functional goals of our system - hence, only one auction round is conducted. In the given scenario buyer one is willing to pay a price of $1.80, buyer two offers a price of $3.20 and buyer three is offering $3.50. The seller is not selling for less than $2. We conduct a single auction round and the buyers as well as the seller all submit their bid in an encrypted and signed envelope that is distributed and send to all registered participants. As soon as all participants received the bids, the encryption keys are exchanged as well and the sealed bids are decrypted. Buyer three wins the auction and pays the seller the price of buyer two that offered $3.20.

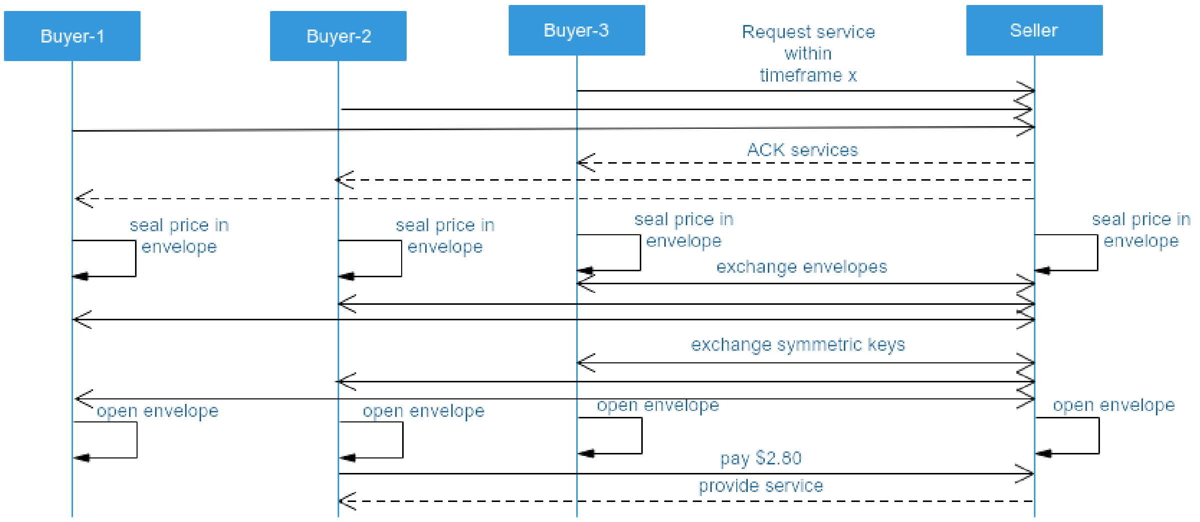

Figure 10. V2X on/off-chain auction algorithm.

In case we have multiple sellers, the sequence diagram is almost identical and the bidding process follows the same procedure. Except in the end, the highest bidder is paying the second highest price to the seller with the highest minimum price, and so on - as long as the paid price is higher than the matched seller's minimum price.

5.3 Platform Integration

Being blockchain- and manufacturer-agnostic are key requirements of our system and fundamental to the future of the V2X ecosystem. In order to interconnect different vendor-operated V2X platforms – that offer different services – among each other in a blockchain- and manufacturer-agnostic way, we propose integrate those different platforms via a heterogeneous multi-chain. Such a *relay-blockchain* is designed to provide no inherent application functionality at all and instead relay-chain functionalities "upon which a large number of validatable, globally-coherent dynamic data-structures may be hosted side-by-side. We call these data-structures parallelised chains or parachains, though there is no specific need for them to be blockchain in nature" (Wood, 2017). Hence, the heterogeneous multi-chain system connects specific chains of different vehicle manufacturers thereby enabling a blockchain- and manufacturer agnostic V2X platform hub. Each of the manufacturers may operates its own chain with their own tokens, e.g., specific utility tokens, as long as they ensure a certain level of compatibility necessary to be integrated into the V2X platform hub. The result is a globally usable platform that is not bound to a single manufacturer, while the platform operators profit from an open system that enables them offer their own services to vehicles of other brands.

6 Conclusion and Future Work

This work presents a novel blockchain-based, platform- and manufacturer-agnostic transaction and interaction layer that enables a V2X platform for goods and services. We outline and describe the technical foundations of this new economy as well as the different use cases and scenarios of V2X transactions and interactions, e.g., vehicle-to-vehicle (V2V), vehicle-to-human (V2H), or vehicle-to-infrastructure (V2I).

Based on the use cases and scenarios we identify the requirements and criteria that a blockchain-based V2X transaction and interaction layer protocol must satisfy. With respect to functional and non-functional requirements, we envision a blockchain- as well as manufacturer agnostic and interoperable V2X platform that enables interaction and transaction between participating entities and a plug-in interface for external applications. Subsequently, we derive the service-oriented architecture of the system based on the identified requirements and goals. We present the system architecture using technology-agnostic UML-component diagrams that detail the system's main components and communication interfaces. In order to ensure widespread adoption, special focus will be given in the future to the API design and library integration for car manufacturers.

A core element of many of the use cases is the smart contract-based negotiation and contract enactment between entities that are the result of collaborating tasks and sub-processes. On an abstract level, most of the use cases presented in this paper follow a similar workflow on the smart-contract level. Hence, we decided to integrate an abstract smart contract negotiation lifecycle that we describe. The lifecycle is divided into the different stages (preparatory, negotiation, contract execution, rollback and contract expiry stage) that we explain in detail. Furthermore, we propose an auction algorithms for the V2X economy that allow to reach an efficient consensus on a certain price between buyer and seller.

For future work, we plan to create an abstract ontology for the supply and demand management of the V2X platform. The goal is to facilitate category independent templates for offers and requests of services and goods that can be populated by autonomous agents (e.g., autonomous vehicles) as well as searched for offers that match their needs. Moreover, further research has to focus on scalability solutions concerning the underlying blockchain technology in order to ensure large-scale adoption. Finally, heterogeneous multi-chains currently lack in-depth research and need further improvements.

References

Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). "A comprehensive survey on vehicular ad hoc network." In: *Journal of network and computer applications*, *37*, 380-392.

Ausubel, L. M. and Milgrom, P. (2006). "The lovely but lonely Vickrey auction." *Combinatorial auctions*, *17*, 22-26.

Baldessari, R., Bödekker, B., Deegener, M., Festag, A., Franz, W., Kellum, C. C., Kosch, T., Kovacs, A., Lenardi, M., Menig, C. and others. (2007). "Car-2-car communication consortium-manifesto".

Berends-Ballast, M. and others (2016). *Transport and Mobility 2016.* URL: https://www.cbs.nl/en-gb/publication/2016/25/transport-and-mobility-2016 (visited on 04/26/2018).

Bochem, A. and Leiding, B. (2018). "Unchained Identities: Putting a Price on Sybil Nodes in Mobile Ad hoc Networks." In: *Security and Privacy in Communication Networks (SecureComm 2018)*. Springer, Singapore.

Booch, G., Jacobson, I., Rumbaugh, J.,and others (1996). "The Unified Modeling Language". *Unix Review*, *14*(13), 5.

Calcaterra, C., Kaal, W. A. and Vlad, A. (2018). *Semada Technical Whitepaper - Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125822 (visited on 04/18/2018).

Christidis, K. and Devetsikiotis, M. (2016). "Blockchains and smart contracts for the internet of things." In: *IEEE Access*, *4*, 2292-2303.

Chinosi, M. and Trombetta, A. (2012). "BPMN: An introduction to the standard." *Computer Standards & Interfaces*, *34*(1), 124-134.

Chong, Z. J., Qin, B., Bandyopadhyay, T., Wongpiromsarn, T., Rebsamen, B., Dai, P., and Ang, M. H. (2013). Autonomy for mobility on demand. In *Intelligent Autonomous Systems 12* (pp. 671-682). Springer, Berlin, Heidelberg.

Cortright, J (2016). *Sprawl Tax: How the US Stacks Up Internationally.* URL: http://cityobservatory.org/sprawl-tax-how-the-us-stacks-up-internationally/ (visited on 04/26/2018).

Daganzo, C. F. (2002). "A behavioral theory of multi-lane traffic flow. Part I: Long homogeneous freeway sections." In: *Transportation Research Part B: Methodological*, *36*(2), 131-158.

Dai, P., Mahi, N., Earls, J. and Norta, A. (2017). *Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform*. URL: https://qtum.org/uploads/files/a2772efe4dc8ed1100319c6480195fb1.pdf (visited on 05/18/2018).

Davidsen, M., Gajek, S., Kruse, M., Thomsen, S. (2018). *Empowering the Economy of Things – Whitepaper.* URL: https://assets.ctfassets.net/fo0rvac1gv8v/5Ui5mhVJKgGqYqe6O2OESm/4c66ff073a6510a8b4fe68e16ef2e48d/weeve_whitepaper.pdf (visited on 05/09/2018).

Davis, A. M. (1993). *Software requirements: objects, functions, and states*. Prentice-Hall, Inc..

Edelman, B., Ostrovsky, M. and Schwarz, M. (2007). Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *American economic review*, *97*(1), 242-259.

Erl, T. (2005). *Service-oriented architecture: concepts, technology, and design*. Pearson Education India.

Faezipour, M., Nourani, M., Saeed, A. and Addepalli, S. (2012). "Progress and Challenges in Intelligent Vehicle Area Networks." *Communications of the ACM* 55 (2), 90–100.

Greenblatt, J. B., and Shaheen, S. (2015). Automated vehicles, on-demand mobility, and environmental impacts. *Current sustainable/renewable energy reports*, *2*(3), 74-81.

Goodman, L. M. (2014). *Tezos – A Self-Amending Crypto-Ledger (White paper)*. URL: https://www.tezos.com/static/papers/white_paper.pdf (visited on 04/27/2018).

Goodyear, R. and Ralphs, M. (2009). *Commuting Patterns in New Zealand: 1996–2006.* URL: http://archive.stats.govt.nz/browse_for_stats/Maps_and_geography/Geographic-areas/commuting-patterns-in-nz-1996-2006.aspx (visited on 05/23/2018).

Guo, Y. and Liang, C. (2016). "Blockchain application and outlook in the banking industry." *Financial Innovation 2*(1), p. 24.

IEEE Computer Society. Software Engineering Standards Committee, and IEEE-SA Standards Board. (1998). *IEEE recommended practice for software requirements specifications.* Institute of Electrical and Electronics Engineers.

Kesting, A., Treiber, M., Schönhof, M. and Helbing, D. (2008). "Adaptive cruise control design for active congestion avoidance." In: *Transportation Research Part C: Emerging Technologies*, *16*(6), 668-683.

Lanctot, R. (2017). *Accelerating the Future: The Economic Impact of the Emerging Passenger Economy.* URL: https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf (visited on 04/27/2018).

Leiding, B., Memarmoshrefi, P. and Hogrefe, D. (2016). "Self-managed and blockchain-based vehicular ad-hoc networks." In: *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (pp. 137-140). ACM.

Li, Y. J. (2010). "An overview of the DSRC/WAVE technology." In: *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness* (pp. 544-558). Springer, Berlin, Heidelberg.

Lighthill, M. J. and Whitham, G. B. (1955). "On kinematic waves II. A theory of traffic flow on long crowded roads." In: *Proc. R. Soc. Lond. A*, *229*(1178), 317-345.

Lucking-Reiley, D. (2000). "Vickrey auctions in practice: From nineteenth-century philately to twenty-first-century e-commerce." *Journal of economic perspectives*, *14*(3), 183-192.

MacNeille, P. R., Wisniewski, J., & DeCia, N. (2018). *U.S. Patent No. 9,928,746*. Washington, DC: U.S. Patent and Trademark Office.

Marshall, J. (2014). "Agent-based modelling of emotional goals in digital media design projects." International Journal of People-Oriented Programming (IJPOP) 3(1), 44–59.

McCorry, P., Shahandashti, S. F., Clarke, D., & Hao, F. (2015). "Authenticated key exchange over bitcoin." In: *International Conference on Research in Security Standardisation* (pp. 3-20). Springer, Cham.

McKenzie, B. (2015). *Who Drives to Work? Commuting by Automobile in the United States: 2013.* URL: https://www.census.gov/library/publications/2015/acs/acs-32.html (visited on 05/23/2018).

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., & Weinhardt, C. (2018). "A blockchain-based smart grid: towards sustainable local energy markets." In: *Computer Science-Research and Development*, *33*(1-2), 207-214.

Moldovanu, B., & Tietzel, M. (1998). "Goethe's second-price auction." *Journal of Political Economy*, *106*(4), 854-859.

Nakamoto, T. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. URL: https://bitcoin.org/bitcoin.pdf (visited on 05/01/2018).

Nguyen, Q. K. (2016). "Blockchain - A Financial Technology for Future Sustainable Development." In: *Green Technology and Sustainable Development (GTSD), International Conference on* (pp. 51-54). IEEE.

Norta, A. (2008). *Exploring Dynamic Inter-Organizational Business Process Collaboration: Privacy Protecting Concepts for Choreographing eSourcing in B2B with Service-Oriented Computing.* VDM Verlag.

Norta, A., Grefen, P. and Narendra, N.C. (2014). "A Reference Architecture for Managing Dynamic Inter-Organizational Business Processes." *Data & Knowledge Engineering* 91, 52–89.

Object Management Group (2007). "OMG Unified Modeling Language (OMG UML) - Superstructure - Version 2.1.2." OMG Specification.

Ouaddah, A., Elkalam, A. A. and Ouahman, A. A. (2017). "Towards a novel privacy-preserving access control model based on blockchain technology in IoT." In: *Europe and MENA Cooperation Advances in Information and Communication Technologies* (pp. 523-533). Springer, Cham.

Pavone, M. (2015). Autonomous mobility-on-demand systems for future urban mobility. In A*utonomes Fahren* (pp. 399-416). Springer Vieweg, Berlin, Heidelberg.

Perrey, R. and Lycett, M. (2003). “Service-oriented architecture.” In: *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on* (pp. 116-119). IEEE.

Popov, S. (2018). *The Tangle - Version 1.4.3*. URL: https://iota.org/IOTA_Whitepaper.pdf (visited on 04/30/2018).

Rosen, M., Lublinsky, B., Smith, K. T. and Balcer, M. J. (2012). *Applied SOA: service-oriented architecture and design strategies*. John Wiley & Sons.

Sikorski, J. J., Haughton, J. and Kraft, M. (2017). “Blockchain technology in the chemical industry: Machine-to-machine electricity market.” *Applied Energy*, *195*, 234-246.

Sterling, L. and K. Taveter (2009). *The Art of Agent-Oriented Modeling.* MIT Press.

Uzcátegui, R. A., De Sucre, A. J. and Acosta-Marum, G. (2009). “Wave: A tutorial.” *IEEE Communications magazine*, *47*(5).

Vickrey, W. (1961). “Counterspeculation, auctions, and competitive sealed tenders.” *The Journal of finance*, *16*(1), 8-37.

Wang, D. and Jing, C. (2001). “Application of traffic-wave theory in urban traffic analysis.” In: *Vehicle Electronics Conference, 2001. IVEC 2001. Proceedings of the IEEE International* (pp. 143-147). IEEE.

Wood, G. (2014). *Ethereum: A Secure Decentralized Generalised Transaction Ledger*. URL: http://gavwood.com/paper.pdf (visited on 05/01/2018).

Wood, G. (2017). *Polkadot: Vision for a Heterogeneous Multi-Chain Framework.* URL: https://github.com/w3f/polkadot-white-paper/blob/master/PolkaDotPaper.pdf (visited on 05/10/2018).