A Blockchain architecture for a Mobility as a Service system with the adoption of Autonomous Vehicles.

G. Vega
Delft University of Technology
The Netherlands

ABSTRACT: Autonomous vehicles have the potential to introduce numerous changes, opportunities, and innovations in mobility services, environment, data, value networks, and economy, among others. These automated vehicles are expected to impulse a disruptive change in society, especially within transport technology economics, travel behavior, and network performance. This introduces new challenges and opportunities for the automotive industry and society. Mobility as a Service could take a significant role in the utilization of autonomous vehicles, especially with the current downwards tendency of car ownership in Europe and North America. The scientific literature and consultancy firms reinforce this by providing analysis and predicting a decline of car ownership in the global markets. Nevertheless, there is a need for trust and more secure and tamper-resilient processes within Autonomous Vehicles and Mobility as a Service ecosystems. Because of this, the idea of this research is to explore what a Blockchain-based Mobility-as-a-Service concept design operated by Autonomous Vehicles requirements and Blockchain architecture would look like. This research is conducted from a complex socio-technical point of view that considers a Design Science Research methodology. By doing so, a set of requirements are developed to create a Blockchain architecture. In this regards, it is found that the dominants requirements are about trust, security and privacy. Lastly, it is found that the issue of latency is one of the most decisive elements to consider when designing a BC architecture for a system that uses Mobility as a Service with Autonomous Vehicles.

KEYWORDS: Blockchain, Autonomous Vehicles, Mobility as a Service, Design Science Research, Architecture.

1. INTRODUCTION

Autonomous vehicles (AVs) are the next generation of cars that are enabled by advanced sensors, navigation, and computer vision technologies that allow them to drive autonomously with the complete or partial assistance of humans (Mehedi Hasan et al., 2018). The work of Monios & Bergqvist, (2020) emphasizes that AVs will introduce a significant reduction in operation costs and acting at the same time as a driver for non-ownership business models. In addition to this, they state that there is a strong trend of decreasing the ownership of personal vehicles on the way to the utilization of Mobility as a Service (MaaS).

The idea of MaaS is regularly treated as a one-stop, digital platform Intelligent Transportation System (ITS) that offers travel management regarding their distribution, acquisition, and journey creation (Wong et al., 2020). These types of services propose an on-demand use of vehicles which translate into a change from the fixed cost of buying a car to a variable cost depending on the amount of time and distance that the user needs. In addition to this, the internet of things, big data analytics, and AVs are working together to optimize transport networks, improve effective vehicle utilization while refining the usage of infrastructure and providing a better customer experience. Nevertheless, these connectivity-based vehicles rely on networked software that is susceptible to issues like privacy and security of AVs ecosystems which can make them vulnerable to cyberattacks and hacks (Kim, 2018).

There are multiple issues regarding the trust, transparency, privacy, and security of AV ecosystems, from secure V2X communication, data breach, tight control, decision and diagnosis units, privacy, integrated embedded security, and more. Additionally, the vast majority of critical operations of AVs require a real-time response making latency a big concern for the secure design of an AV (Mitra et al., 2019). In regards to data privacy, security, and trust, technologies like Blockchain (BC) can be useful due to its tamper-resilient and verifiable record of transactions, which enables a provenance of data, the validity of data and immutability of data (Mitra et al., 2019).

BC is a distributed technology that includes a hash function, cryptography with digital signatures, and time sequence (Yang et al., 2019). Additionally, BC is composed of two types of elements, Transaction: Which are the activities created by the participants in the system. Blocks: Which are the transactions recorded to make sure they are not tampered with and stay in the correct arrangement (Mehedi Hasan et al., 2018). This distributed ledger technology (DLT) poses many benefits, especially in modern data privacy and real-time automation with the use of smart-contracts.

One of the main advantages of technologies like BC is their ability to provide a safe and tamper-resilient within a shared state, especially useful for AV ecosystems and grids (Mitra et al., 2019). In this sense could be interesting to use these properties to solve the needs for trust, secure and tamper-resilient data aggregation of AVs by using BC technologies in the MaaS industry.

These new mobility services and technologies like AVs are complementing each other towards services and promoting a shift in paradigm regarding mobility. The private ownership of cars is not used as an asset nowadays and is going into a transition towards access on-demand services (Wong et al., 2020). These new mobility services are already operating in different countries around the world. MaaS is continuously growing, and probably it will continue to grow in the upcoming years. Nevertheless, there are numerous uncertainties on how they will operate with AVs and the current issues or difficulties that this automatization technology is experiencing.

The main issues of security, privacy, and trust are also the market and technology drivers in the mobility industry (Romanski & Daim, 2019). In this regard, BC can be used to set a decentralized, secure, and trusted autonomous ITS ecosystem but there is a critical need for creating an ecosystem architecture that enables a free flow of data, assets, and money withing an ITS ecosystem (Yuan & Wang, 2016). Moreover, the existing models that use BC technologies in MaaS environments are variated and do not provide a complete overview of the whole ecosystem (Karinsalo & Halunen, 2018).

There are no scientific articles that describe a BC architecture for a BC-based MaaS system with the adoption of AVs. Moreover, there are lots of opportunities from the capabilities of these different technologies and their interactions. Because of this, the objective of this research is focused on build and evaluate an artefact that aims to the following:

Design a Blockchain-based Mobility-as-a-Service concept with the adoption of Autonomous Vehicles Blockchain architecture would look like.

According to the relevance and future possibilities of BC, MaaS, and AVs, this research will provide a first insight into how the BC architecture of such a system would look like.

BC is an interesting solution for this work because of its fundamental principles of transparency, decentralization, privacy, and security (Aste et al., 2017). Additionally, BC can be used to develop a secure, trusted, and decentralized autonomous ITS ecosystem (Yuan & Wang, 2016). In regards to decentralized architecture, BC can help to protect users privacy from global surveillance of corporations and states (De Filippi, 2016). Furthermore, BC enables new ways of distributed software architectures where decentralized and transactional data can be established to untrusted members eliminating the need to rely on a single integration point (Xu et al., 2017).

For this research, a future scenario is considered were AVs will operate on Level 5 of autonomy. This means that there will be no need for the users of the vehicle to drive the vehicle or even have a driver's license. Moreover, one of the requirements for future AVs is the implementation of the fifth-generation

networks (5G). In this regard, 5G can introduce new capabilities like lower latency, edgeless connectivity, increased capacity, and fundamental changes of connection paradigms (Zheng et al., 2017). Due to this, the assumption that these technologies will be fully implemented in the future is taken for this research.

2. RESEARCH APPROACH

This research follows a Design Science Research (DRS) approach and phases proposed by Johannesson & Perjons, (2014). Furthermore, a systems engineering perspective is also taken due to the high complexity and socio-technical characteristics of the previously mentioned research objective. DSR is a combination of two different paradigms; behavioral science and design science (Hevner et al., 2004). Behavioral science comes from natural science, and its objective is to justify theories to clarify the human and organizational phenomena in regards to its design, analysis, and implementation of Information Systems (IS) (Hevner et al., 2004). On the other hand, the design science paradigm is a problem-solving paradigm. This paradigm has the objective of developing artefacts that can help to design, analyses, implement, and manage solutions for IS (Denning, 1997). Moreover, the creation of these artefacts is based on kernel theories that provide help to the researchers in their journey for solving problems (Markus et al., 2008).

The artefact proposed for this research are design choices to consider for the design of a BC-enabled MaaS with the adoption of AVs BC architecture. Being the proposed design an IS, DSR provides a good fit for design, development, demonstration, and evaluation of such artefact (Johannesson & Perjons, 2014). Furthermore, this approach proposes five distinctive phases; *Explicate Problem, Define Requirements, Design and Develop Artefact, Demonstrate Artefact, Evaluate Artefact.*

To systematically analyze the problem mentioned above a complex socio-technical system perspective is taken. To design in a complex socio-technical system, the study of other systems that form part of the first system, often called sub-systems, is conducted. Furthermore, a TIP (Technology, Institutional, and Process) design approach is taken into account. This TIP design approach means that technical and institutional components are studied to produce functional processes (Bots & Els Van Daalen, 2012).

3. RESULTS FROM THE RESEARCH APPROACH

By utilizing the explicated research approach a system, institutional, and stakeholder analysis are elaborated and discussed. Moreover, by utilizing requirements engineering a set of requirements is presented in this section.

3.1. Socio-technical System analysis

For the first phase a system analysis is conducted where the system of interest is decomposed into three sub-systems. These are the technical, institutional, and stakeholder sub-systems. Generally, IS are not just their technical part but also about the user trust, behavior, rules, and regulations. Because of this, a socio-technical point of view is taken to analyze these sub-systems.

Technical analysis

In general, MaaS is a user-centric, personalized, and on-demand intermodal or multimodal transport solution to optimize transport mobility. Moreover, these transport solutions are offered in a single digital platform in an intelligent way with the support of Information and Communications Technology (ICT) infrastructure for the correct functioning of a MaaS ecosystem (Kamargianni & Matyas, 2017).

While there are multiple definitions in the literature about what a MaaS in this article the definition of Kamargianni & Matyas, (2017,) is used. They state that a MaaS is defined as follow:

> *"Mobility as a Service is a user-centric, intelligent mobility distribution model in which all mobility service providers offerings are aggregated by a sole mobility provider, the MaaS provider, and supplied to users through a single digital platform."* Kamargianni & Matyas, (2017, P.4)

MaaS possess some interesting characteristic that defines how this subsystem would look like and are useful to identify to elicit technical requirements later. These characteristics are also relevant to identify what elements form part of a MaaS concept and its implication in such a concept. To look into these core characteristics the work of Jittrapirom et al., (2017) is studied. They propose 9 core characteristics that are based on a literature review of 12 MaaS schemes from different authors: *Integration of transport modes, Tariff option, One platform, Multiple actors, Use of technologies, Demand orientation, Registration requirement, Personalization, Personalization, and Customization (*Jittrapirom et al., 2017).

After analyzing the core characteristic of a MaaS system some key functionalities are needed to support these core characteristics. Furthermore, these key functionalities will correlate with a variety of transactions that are needed to support such a system. These take the form of tools and services that the users need to take a trip; Planning, Booking, Access to real-time information, Payment, and Ticketing (Kamargianni & Matyas, 2017). Moreover, the key functionalities that are considered for this research are *User identification, Planning, Booking, Access to real-time information, Payment, and Ticketing.*

These key functionalities are the basics that are needed to develop a MaaS system (Kamargianni & Matyas, 2017). Moreover, these will take the form of transactions that are needed to be performed by the system.

Institutional analysis

MaaS systems rely on personal data and regulations like the General Data Protection Regulation (GDPR) can possibly impact the implementation of a MaaS system. Elements like location data and online identifiers are relevant for a MaaS ecosystem and form part of their core characteristics. Furthermore, MaaS systems need to process user data to enable the key functionalities which needs to be aligned with the GDPR regulations. Complying with these regulations is

essential for the development of a MaaS system, by analyzing the GDPR articles some elements are considered as needed for a MaaS system: Privacy by Design, Data minimization and purpose limitation, Breach notification, Data protection Officers, Obligation to conduct data protection impact assessments, Right of Access, Right to erasure ('right to be forgotten'), Affirmative Consent and Use of Cookies (GDPR, 2016).

For the proposed BC-based MaaS system with the adoption of AVs, it is fundamental that these types of vehicles can circulate in every road. Because of this, it is needed to assume that laws and regulations in the future will permit the use of fully AVs. Overall, the need for policy frameworks and recommendations for passenger rights, privacy, safety, security, social inclusion, sustainable development, and fair competition of the market (Kamargianni & Matyas, 2017) are taken as assumptions for this research.

Stakeholders analysis

In such a complex system, several actors will be directly involved in the AVs data ecosystem. These actors will probably participate directly in a MaaS system and will share some data. Furthermore, other actors could be involved in the MaaS ecosystem. By conducting desk research, the following actors are considered as the main participants in a MaaS ecosystem: *MaaS provider, Transport provider, Data provider, Insurance provider, and User.* Furthermore, their main roles are identified and illustrated in *Table 1*.

Table 1: Stakeholders roles.

Stakeholder	Role
User	Use the MaaS system.
MaaS provider	Provide journey planning, payment options, data analtytics, and a platform.
Transport provider	Provide transport means (AVs), provide data.
Data provider	Provide data and analytics to the MaaS ecosystem.
Insurance provider	Provide insurance to the vehicle, users, and third parties.

3.2. Requirement engineering

For the second phase desk research is conducted based on a System Engineer and Requirement Engineering approach. The requirements are an attribute of an artifact that is wanted by stakeholders and are used as a guide for the development of such artifact (Johannesson & Perjons, 2014). Moreover, requirements are an assessment of the needs of such systems and what the system should. For this work, the requirements represent a description of the services and processes that the MaaS system will provide. These requirements could be high-level user requirements and system requirements that are a detailed description of what is expected of the system. To further support this process and supplement this information, a user scenario is proposed. Scenarios are a description of a particular task to have an idea of how the system can be used. These scenarios are useful to discover what people do, what system they use, and what information they use and generate (Sommerville, 2016). For this scenario, an Uber general trip is used as a reference guide to come up with the most basic processes that need to be enabled by the system. In addition to this, some examples of things that could go wrong are proposed for such a scenario. While it is impossible to consider all the things that can go wrong on a trip the proposed examples are just a couple that focusses on usability issues. To further illustrate this scenario, a high-level overview of the user AV trip scenario of the processes of creating an account, booking, and using an AV in a MaaS platform is illustrated in *Figure 1* utilizing a Business Process Model Notation tool that can be found in the *Appendices*. By doing so, user requirements and system requirements are formulated in *Table 2* and *Table 3* which can also be found in the *Appendices*.

4. SYSTEM DESIGN

The third phase of this design is about fulfilling the defined requirements in a design that is intended to solve a problem. With the objective of exploring what a BC-based MaaS concept design with the adoption of AVs BC architecture would look like the work of Tasca et al., (2017) is used as guidance. They identify and classify the main blockchain components and their relationships; this helps to explain how blockchain works and design or model a blockchain concept. These main components are *Consensus mechanism, Transaction capabilities, Native currency/tokenization, Extensibility, Security & Privacy, Identity Management, Charging, and Rewarding system (*Tasca et al., 2017). These main components are assessed and selected according the requirements of the system.

4.1. Consensus mechanism

This is a group of procedures and rules that preserves and updates the ledger with the idea of ensuring the trustworthiness, accuracy, authenticity, and reliability of the records in the ledger (Tasca et al., 2017). This group of procedures and rules have other components and sub-components that are assessed to identify what layout offers the best fit for the requirements. Some of the requirements for the proposed system are related to latency and trust, (U4, U8, and S4.1). Moreover, these requirements demand a low latency system to reach real-time operations and a system that the users can trust. These requirements are relevant for considering the network topology of a BC system and demand a fast consensus mechanism for the system. In contrast, permissions-less or public network topologies are one of the most secure ones but with inherent latency issues (Casino et al., 2019; Tasca et al., 2017). This leaves out with two other topology choices; private and consortium topologies. Private and consortium topologies possess comparable scalability and privacy protection but consortium topologies select a group of nodes instead of a single one with access to transaction processes as used in the private topology (Casino et al., 2019).

The proposed system in this work is formed with a group of stakeholders that will need access for different transactions (U8, U9, U10, and U11). This entails that the only feasible option that can fit the requirements for multiple nodes or stakeholders is a Consortium or Federated network topology. By doing so, this selection locks some of the other options when considering the consensus mechanism of the BC architecture. The Consensus Immutability and Failure Tolerance list of choices is predetermined by the network topology previously chosen. This

entails that only a limited number of nodes will have reading and approval rights. Moreover, only a Practical Byzantine Fault Tolerance (pBFT) mechanism can perform in network topologies with a handful of identified nodes with permission to authenticate transactions and offers low latency capabilities (Castro & Liskov, 2002). This is relevant because an important element to consider when using AVs are latency issues.

The design choices of a Consortium network topology with a pBFT mechanism are reinforced with requirements regarding the real-time operations needed for the system. Furthermore, the system needs a shared or global truth for all the nodes to agree up, this is called Agreement and defines the probability of reaching consensus (Tasca et al., 2017). In this regard, the pBFT is a deterministic consensus mechanism (Castro & Liskov, 2002) thus, the type of agreement for reaching consensus should be a deterministic one. This consensus mechanism work by allowing the replicated system to tolerate faults if 1/3 of the replicas turn faulty inside a window of vulnerability (Castro & Liskov, 2002). Moreover, pBFT enables high transaction throughput in the case that consortium nodes are functioning as ordering nodes.

4.2. Transaction capabilities

The transaction capabilities relate to the scalability of transactions and the possible use in applications and platforms (Tasca et al., 2017). The proposed system has some requirements regarding the transaction capabilities of this design. Moreover, requirements U4 and U8 specify a low tolerance for latency and demands high transaction capabilities. Furthermore, requirements U5, U8, S5.1, S5.2, S8.1, and S8.2 introduce a demand for additional services and online cashless payment solutions for such services. In addition to this, scalability requirements (S13) also form part of the system design to enable the system for future expansions.

The transaction capability demands of this system are low latency in transactions with a high transaction throughput. Additionally, online cashless payment options that can support the key functionalities offered by the platform. Furthermore, only a couple of design alternatives are available that fit with the previous network topology choices and the requirements previously mentioned. This is the case of the data structure in the block-header which describes the ability of the system to store transaction information (Tasca et al., 2017). In this case, the only available option to consider that works with a Consortium topology is the Patricia Merkle Tree. This type of data structure allows to insert, delete, or edit information in the balance of the accounts and allows faster and flexible transactions (Tasca et al., 2017). This design decision is also reinforced with the latency requirement of the proposed system. With the same argumentation, the only server storage layout that is compatible with a Consortium topology is the Thin Nodes Capabilities (Tasca et al., 2017). With this design choice, only some of the connected nodes in the network contain a part of the information stored in the BC (Tasca et al., 2017). This layout for the server storage also creates a more scalable system (Tasca et al., 2017) which is also aligned with requirements U8 and S13.

Another relevant requirement regarding the transactions is the ability of the system to process these transactions automatically (S14). For this smart contracts could be useful, because there is no need for human interaction, confirmation, or mediation (Tasca et al., 2017). Smart contracts offer several automation properties that fit with the requirements of this design, such properties as self-enforceable, self-executable, self-verifiable, and self-constraint (Clack et al., 2016).

4.3. Native currency/tokenization

The use of native currency and tokenization allows the use of asset-transfers for different use cases with BC technology, this technology has underlying native assets or tokens that enable activities on platforms or communities (Tsukerman, 2016). Tokenization could be used as a digital bearer bond and its ownership is resolved by the data rooted in the BC, they can be transferred between holders and do not require the approval of authorities (Tasca et al., 2017).

The proposed system has requirements to support a diversity of actors (S12). To fulfill this requirement a convertible multiple asset layout is needed because this allows exchanging assets with others outside the platform with a diversity of currencies (Tasca et al., 2017). This could reduce the entry barrier for the users in the system while satisfying requirement S12. In addition to this, the proposed system has several requirements for access, book/ticketing and payment options (U1, U8, S1.4, S6.4, S6.5, U3, U6, S3.1, U5, U9, S5.1, S5.1, S8.3). This entails that the system could use tokenization as a means of payment. Regarding this, the work of Oliveira et al., (2018) identifies three classes of tokens; Coin/Cryptocurrency, Utility Token, and Tokenized Security. Moreover, cryptocurrencies are asset-based token used as digital money. Tokenized Security is used as a digital share that possesses entitlement to profit or dividends. Moreover, Utility Tokens are meant to pay a fee for access or pay-per-use platforms as well as reward user behavior and experience in such platforms (Oliveira et al., 2018). Among these, the only class of tokens that has the purpose needed for this system is the Utility Token. Mainly because these tokens will be used to access the vehicle and its additional services.

4.4. Extensibility

Elements like interoperability, intraoperability, and governance can help to take a look at the future ecosystem of the BC network and its integration potential (Tasca et al., 2017). The interoperability shows the capability of BC to exchange information with other systems that might or not be blockchain-based systems (Tasca et al., 2017). Next, intraoperability shows the capability of the BC to trade information with other BCs systems (Tasca et al., 2017).

The proposed system has multiple requirements that illustrate the need for the system to exchange information with other systems and technologies like IoT and infrastructure (U8, U9, U10, U11). In addition to this, other system requirements demand the exchange of information inside the system like access to services, devices, data, and transactions (S1.4, S6.2, S6.3, S8.1-S8.4, and S11). These extensibility components for the architecture of the BC are explicitly illustrated in the requirements. Consequently, the only possible layout for the proposed system is to consider Explicit Intraoperability and

Explicit Interoperability components.

Another relevant component to consider for the system extensibility is governance rules. These are decisive elements for its successful implementation, adaptation, change, and interaction (Tasca et al., 2017). The work of Tasca et al.,(2017) identifies two types of governance rules; the Technical Rules of self-governance, this is formed by protocols, procedures, software, supporting facilities among others. In addition to this, Regulatory Rules are defined by external entities and formed by industry policies, regulatory frameworks among others. Moreover, this research identifies multiple system technical requirements, this entails that the consortium of stakeholders in the ecosystem must satisfy these technical requirements and rules. For this, a layout of the governance would need to be composed of different stakeholders that work together to develop commercially and technologically for common profit. In this regard, the only option that considers this is an Alliance Mode were only nodes that meet certain criteria (like permission to write or read in the BC) are approved to collaborate to set the technical rules of the BC (Tasca et al., 2017).

4.5. Security and Privacy

A way to secure data is to use data encryption which is a cryptographic tool that is used to hash and validate information, making the system more or less versatile (Tasca et al., 2017). Whereas security is inherent to BC technologies because there is no single point of failure, some research shows that BC transactions can be susceptible to information extraction and even identification of the participants (Tasca & Liu, 2016). Similarly, multiple solutions exist to encrypt data and keep this data obfuscated, this is by making a program into a “black box”, intending to deny access to data and processes (Tasca et al., 2017). In this regard, components like security and privacy are closely related. The privacy of information is the ability to control the use and procurement of people personal information (Westin, 1967). BC does not fully secure user privacy because most BCs transactions are pseudonymous and the identity of the origination and recipient can be exposed (Rossi et al., 2019).

There are multiple requirements identified in this work that relates to the need for data security and privacy for the system (U7, S7.1-S7.6, U10, and S10.2). While BC does not fully solve these issues, some design considerations can help to mitigate them. For this purpose, privacy concerns can be satisfied by the inclusion of smart contracts that can automatize transactions thus reinforcing this decision by satisfying requirement S14. Nevertheless, these smart contracts could include personal information of passengers in the case of MaaS systems (Nguyen et al., 2019). For this reason, a Zero-Knowledge - Succinct Non-interactive Argument of Knowledge (ZK-SNARKS) can be used to validate terms without revealing private information in the smart contracts (Nguyen et al., 2019).

The previous design decision of using a pBFT consensus mechanism is reinforced regarding the need for security of the system. This is due to the properties of the pBFT regarding security. According to Castro & Liskov, (2002) this consensus mechanism poses a good performance, it is safe to use in an asynchronous environment like the Internet, has defensive mechanisms for Byzantine-faulty clients and it is proactive to recover replicas.

Another way to mitigate privacy vulnerabilities of the system is the practice of not including private data on the BC. This entails that the system would need to use a digital identity that does not track back to personal data or a tokenization mechanism. This is already discussed before and reinforces the design decisions of using tokenization and also a digital identity that is aligned with requirement U1. Similarly, one of the requirements regarding privacy is to comply with GDPR regulations (U7). Specifically, BC does not fully comply with GDPR regulations due to the property of immutability of the data in the BC and according to GDPR, personal data must be able to be forgotten. For this reason, the need of not storing personal data in the BC is further strengthened and validated to satisfy system requirements and regulatory rules.

4.6. Identity Management

The identity management component is formed by two layers; the Access and Control layer and the Identity layer. They ensure access to sensitive data and determine the governance model of the BC (Tasca et al., 2017). Regarding the access and control layer, it is relevant to establish an adequate governance structure while considering the ledger construct (Tasca et al., 2017). In this regard, the governance structure regulates control policies management and authorizations which are rules that manage users, systems, and node permissions on the BC (Tasca et al., 2017). This is represented in rules that determine who has read and write access and who can manage the consensus in the ledger.

Several requirements that relate to access and control demands are detected (U3, U8, U10, and U11), these requirements demand that some stakeholders have control and access to information on the BC. For instance, the data provider should have read and write access to process and send new data to other stakeholders in the ecosystem while complying with requirement S7.1. Therefore, the system demands specific access and control for each of the stakeholders or nodes that participate in the system.

Multiple requirements relate to identity management, there is the need for a unique ID (U1) and use of this ID to gain access to different systems and services (U2, U3, U5, and U6). In addition to this, other system requirements demand to use this ID (S1.1-S1.4) for payments (S5.4), user identification (S6.1 and S6.2), and exchange of information with different stakeholders in the ecosystem (S8.x-S11). In addition to this, user requirements demand a system that can be trusted (U12). By doing so, digital identities can provide security, data integrity, and anonymity without the need to rely on third parties (Yli-Huumo et al., 2016). In this regard, digital identities have become a fundamental security measure (Rivera et al., 2017).

The requirements listed above demand a need for the identity layer where information can be trusted and verified. Therefore, when looking at the identity layer of the BC, onboarding and

offboarding of nodes are key aspects that need consideration (Tasca et al., 2017). These can be achieved by implementing identity verification processes, like Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) that can increase transparency and verify user information (Tasca et al., 2017).

4.7. Charging and Rewarding System

Operational and maintenance costs of the BC systems are usually covered by the members of the network and it is done by different models depending on the architectural configuration, governance, data structure, and computation required on the chain (Tasca et al., 2017). To cover these potential financial costs of running a BC platform an incentive scheme could be used to maintain the cost structure for different stakeholders (Tasca et al., 2017).

A Reward System is a rewarding mechanism that functions automatically and generated by BC systems to retribute for verifications, validations, or data storage in the network (Tasca et al., 2017). In a BC network, various computing elements can act as nodes in the network, BC could be used to include all the available computing elements or nodes in the ecosystem (Yuan & Wang, 2016). In particular, the AVs could be used as nodes to validate route information and transactions. It is possible to already see examples of this in the case of the BC model Block-VN proposed by Sharma et al., (2017), where they allow vehicles to realize and use their resources to develop a vehicular network to produce services. In addition to this, IoT devices in the infrastructure and smart devices from the users could also be used as nodes. By doing so, the system could increase further participation of the nodes and fulfilling requirement S12 by proposing a reward scheme that compensates participants with a token that could be used to buy services in the ecosystem. The user or AVs that opt to participate in the network by providing their computer power could be rewarded with these tokens. In addition to this, some BC networks introduce a fee system when users make use of the BC, nevertheless, this is not necessary (Tasca et al., 2017). Moreover, this is aligned with requirements S12 and the intention to reduce the entry barrier for the users.

5. EVALUATION

The fifth phase of this design is about evaluating the process to determine if the proposed artefact is useful and live up to the expectation of exploring how a BC-based MaaS system with the adoption of AVs BC architecture would look like. For this, a formative evaluation is conducted that assesses the design process of the proposed artefact (Johannesson & Perjons, 2014). The means for doing this are a set of semi-structured interviews that are formed by a group of experts via flexible open questions that can be discussed and allows the interviewers to respond to them in their own words (Johannesson & Perjons, 2014). In this regard, the design requirements are treated as sub-objective needed to achieve the design objective, which is reflected in the structural specifications of this design (Verschuren & Hartog, 2005). This is an ex-ante evaluation; this means that the evaluation is conducted to assure that the design process is correct and the resulting design will not fail (Verschuren & Hartog, 2005). Moreover, an ex-ante evaluation can be done faster, does not require a large number of resources, users, or organizations and it is ideal to evaluate an initial design or prototype (Johannesson & Perjons, 2014).

The expert validation was conducted with a semi-structured interview by a walk-through with experts in Blockchain, ICT architectures, and autonomous systems. A walk-through is an evaluation instrument similar to a peer review were the designer leads the expert's trough a method or artefacts (Johannesson & Perjons, 2014). In this style of interviews, the experts are allowed to ask questions, identify problems, suggest other solutions, or give any other kind of feedback (Johannesson & Perjons, 2014).

The interviews resulted in various improvements regarding the fulfillment of the requirements of this research. While the feedback provided by a group of experts is relevant and important for the design of a BC-based MaaS concept with the utilization of AVs it is not possible to include them all due to time and scope limitation of this article. Moreover, some of the feedback gave great insight into possible future research topics and improvements. In general, the group of experts was pleased about the design methodology used for this research as well as the designed artefact and the accomplishment of the research objective.

The fourth phase of this design consider the BC components, sub-component of experts a BC architecture for a BC-based MaaS system with the adoption of AVs which is presented in *Figure 2* that can be found in the *Appendices*. In this figure, the top part represents the main components followed by the sub-components. In the bottom are the selected design choices, in green, that are used to design the BC architecture of the proposed system in this research.

6. CONCLUSION AND FUTURE RESEARCH

The objective of this research was to design what a BC-based MaaS concept design with the adoption of AVs BC architecture would look like. From using a TIP analysis, the key functionalities, main regulations and most relevant stakeholders for the design of such system are found. Furthermore, by performing system analysis and requirement engineering it is possible to elicitate a set of user and system requirements needed for the design of an artefact. In this regard, it is found that the most dominant requirements are related to trust, security and privacy issues. Moreover, transaction capabilities and specially latency, play a major role when deciding the BC architecture components and sub-components for this system.

While this research proposes positive results, some limitations can be found. Regarding the methodology, limitations can be found in the DSR approach. Creating novel innovations by relying on existing scientific theories could make this research difficult and could lead to delays and deficiencies. Besides, the lack of knowledge base in the creation of the proposed artefact could lead to issues of practicality for their users and the researcher have to use their intuition or experiences while designing such a system. In addition to this, the designed system

remains at an abstract level which means that is it not possible to go into all the details of the system in this research. Furthermore, the researcher does not possess a juridical background or experience that could provide a detailed insight into the GDPR regulations. Nevertheless, this research remains at a high-level and scape the scope and intentions. The requirements gathered in this research could also induce limitations, this is particularly true in this case were the requirements were gathered through observation studies, desk research, and literature reviews. This research is focused on a futuristic scenario which entails a high level of uncertainties regarding the development of the technologies needed for the feasibility of a system like the one proposed in this research. The system design is based on the Ontology of Blockchain technologies developed by Tasca et al., (2017). This could create a tunnel vision of the design alternatives and decisions assessed to develop the BC architecture of this research. There is also some limitation in the evaluation of the system. Additionally, the number of interviews and the type of interviews could also affect the evaluation of the system. While an ex-ante type of evaluation is faster, does not require a large number of resources, users or organizations and it is ideal to evaluate an initial design or porotype (Johannesson & Perjons, 2014), an evaluation with a greater number of stakeholders could also be useful.

With the intention to address these limitations some possible future research topics are explored. For instance, it is interesting to implement a similar system with current AVs technology with the objective to see how the user interacts with such a system. In addition to this, a real-life test could be useful to gain insight into the implementation process of a system like the one proposed in this research. By doing so, it can help to identify requirements of the system and design criteria in a lower-level detail that could be useful to future implementation. This research only focuses on the MaaS system that uses AVs. In this sense, it is interesting to explore if the proposed BC architecture could be applied to a MaaS system that does not use AVs. For instance, it could be applied to multi-modal means of transportation that use public and private transportation means. In this regard, it is also interesting to research if a BC-based MaaS system will be sufficient enough to handle a higher transaction throughput when is designed for a large-scale real-world implementation environment.

References

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer*, *50*(9), 18–28. https://doi.org/10.1109/MC.2017.3571064

Bots, P. W. G., & Els Van Daalen, C. (2012). Designing socio-technical systems: Structures and processes. In *CESUN 2012: 3rd International Engineering Systems Symposium, Delft University of Technology, The Netherlands, 18-20 June 2012*.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. In *Telematics and Informatics* (Vol. 36, pp. 55–81). Pergamon. https://doi.org/10.1016/j.tele.2018.11.006

Castro, M., & Liskov, B. (2002). Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems*, *20*(4), 398–461. https://doi.org/10.1145/571637.571640

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). *Smart Contract Templates: essential requirements and design options*. http://arxiv.org/abs/1612.04496

De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production*, *7*. https://ssrn.com/abstract=2852689

Denning, P. J. (1997). A New Social Contract for Research. *Communications of the ACM*, *40*(2), 132–134. https://doi.org/10.1145/253671.253755

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Jittrapirom, P., Caiati, V., Feneri, A. M., Ebrahimigharehbaghi, S., Alonso-González, M. J., & Narayan, J. (2017). Mobility as a service: A critical review of definitions, assessments of schemes, and key challenges. *Urban Planning*, *2*(2), 13–25. https://doi.org/10.17645/up.v2i2.931

Johannesson, P., & Perjons, E. (2014). An Introduction to Design Science. In *The Design Method*. Springer International Publishing. https://doi.org/10.1007/978-3-319-10632-8

Kamargianni, M., & Matyas, M. (2017). The Business Ecosystem of Mobility-as-a-Service. *96th Transportation Research Board (TRB) Annual Meeting, Washington DC, 8-12 January 2017*, *January*, 8–12. http://discovery.ucl.ac.uk/10037890/1/a2135d_445259f704474f0f8116ccb625bdf7f8.pdf

Karinsalo, A., & Halunen, K. (2018). Smart Contracts for a Mobility-as-a-Service Ecosystem. *Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security Companion, QRS-C 2018*, 135–138. https://doi.org/10.1109/QRS-C.2018.00036

Kim, S. (2018). Blockchain for a Trust Network Among Intelligent Vehicles. In *Advances in Computers* (Vol. 111, pp. 43–68). Elsevier. https://doi.org/10.1016/bs.adcom.2018.03.010

Markus, M. L., Majchrzak, A., & Gasser, L. (2008). A design theory for systems that support emergent knowledge processes. *Design Science Theories and Research Practices*.

Mehedi Hasan, M. G. M., Datta, A., Ashiqur Rahman, M., & Shahriar, H. (2018). Chained of Things: A Secure and Dependable Design of Autonomous Vehicle Services. *Proceedings - International Computer Software and Applications Conference*, *2*, 498–503. https://doi.org/10.1109/COMPSAC.2018.10283

Mitra, S., Bose, S., Gupta, S. Sen, & Chattopadhyay, A. (2019). Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles. *2018 IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2018*, 548–551.

https://doi.org/10.1109/APCCAS.2018.8605625

Monios, J., & Bergqvist, R. (2020). Logistics and the networked society: A conceptual framework for smart network business models using electric autonomous vehicles (EAVs). *Technological Forecasting and Social Change*, *151*. https://doi.org/10.1016/j.techfore.2019.119824

Nguyen, T. H., Partala, J., & Pirttikangas, S. (2019). Blockchain-based mobility-as-a-service. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2019-July*(section II), 1–6. https://doi.org/10.1109/ICCCN.2019.8847027

Oliveira, L., Bauer, I., Zavolokina, L., Bauer, I., & Schwabe, G. (2018). To Token or not to Token : Tools for Understanding Blockchain Tokens. *International Conference on Information Systems 2018, ICIS 2018*, *October*, 1–17. https://doi.org/10.5167/UZH-157908

Rivera, R., Robledo, J. G., Larios, V. M., & Avalos, J. M. (2017). How digital identity on blockchain can contribute in a smart city environment. *2017 International Smart Cities Conference, ISC2 2017*, *00*(c), 17–20. https://doi.org/10.1109/ISC2.2017.8090839

Romanski, B., & Daim, T. (2019). A Technology Roadmap to Uncontested Market Space Using Autonomous Vehicles in the Transportation Industry. *IEEE Engineering Management Review*, *47*(1), 67–76. https://doi.org/10.1109/EMR.2019.2900435

Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda. *Journal of the Association for Information Systems*, *09*, 1390–1405. https://doi.org/10.17705/1jais.00571

Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of Information Processing Systems*, *13*(1), 184–195. https://doi.org/10.3745/JIPS.03.0065

Sommerville, I. (2016). *Software Engineering: Global Edition, Tenth Edition*. https://doi.org/10.1136/bmj.1.5802.756-b

Tasca, P., & Liu, S. (2016). The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment Relationships. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2808762

Tasca, P., Thanabalasingham, T., & Tessone, C. J. (2017). *Ontology of Blockchain Technologies. Principles of Identification and Classification*.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union 1 (2016). https://doi.org/10.5771/9783845266190-974

Tsukerman, M. (2016). The Block is hot: A Survey of the State of Bitcoin Regulation and Suggestions for the Future. *Berkeley Technology Law Journal*, *30*, 1127–1169. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2587421

Verschuren, P., & Hartog, R. (2005). Evaluation in design-oriented research. *Quality and Quantity*, *39*(6), 733–762. https://doi.org/10.1007/s11135-005-3150-6

Westin, A. F. (1967). Privacy and Freedom annotated. In *Privacy and Freedom* (Vol. 22). American Bar Association. https://doi.org/10.2307/40708684

Wong, Y. Z., Hensher, D. A., & Mulley, C. (2020). Mobility as a service (MaaS): Charting a future context. *Transportation Research Part A: Policy and Practice*, *131*(October 2019), 5–19. https://doi.org/10.1016/j.tra.2019.09.030

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., & Rimba, P. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. *Proceedings - 2017 IEEE International Conference on Software Architecture, ICSA 2017*, 243–252. https://doi.org/10.1109/ICSA.2017.33

Yang, Y.-T., Chou, L.-D., Tseng, C.-W., Tseng, F.-H., & Liu, C.-C. (2019). Blockchain-based Traffic Event Validation and Trust Verification for VANETs. *IEEE Access*, *7*, 1–1. https://doi.org/10.1109/access.2019.2903202

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLOS ONE*, *11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Yuan, Y., & Wang, F. Y. (2016). Towards blockchain-based intelligent transportation systems. *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*, 2663–2668. https://doi.org/10.1109/ITSC.2016.7795984

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Appendices

Figure 1: AV trip scenario process model.

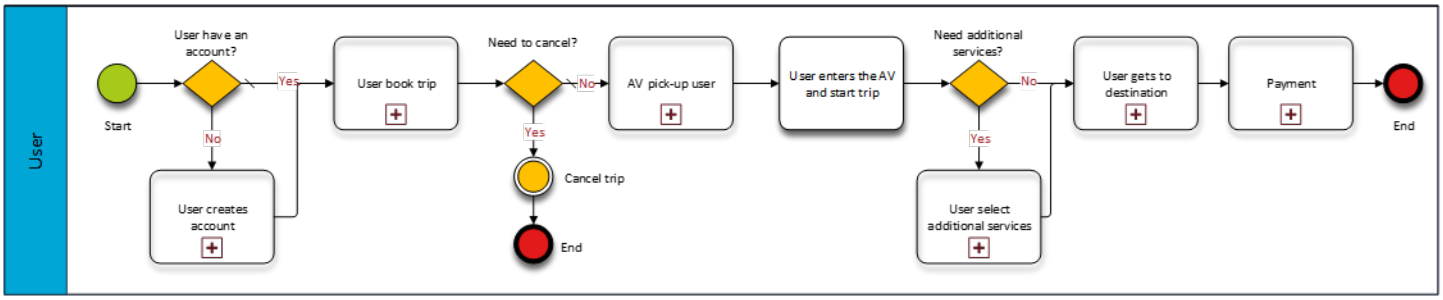

Table 2: User requirements.

ID	Source	Requirement	Justification
U1	*Technical*	The system shall provide the user with the ability to create a unique account to enable access to the platform and its services.	User needs an account and ID to access the services of the platform.
U2	*Technical*	The system shall allow the user to plan a trip according to his preferences.	Personalization is a core characteristic of MaaS.
U3	*Technical*	The system shall users to book their trips.	User needs to book their trips and it is a core characteristic.
U4	*Technical*	The system shall provide access to real-time information for its users.	Services are needed in real-time.
U5	*Technical*	The system shall provide payment options and means for its users.	Payment options and means are needed for providers to make a business and user to pay for the services offered by those businesses.
U6	*Technical*	The system shall provide a ticketing system for its users.	When a user book a trip, the assigned AV must be reserved to him and not used for other users.
U7	*Institutional*	The system shall comply with GDPR regulations.	Data protection regulations.
U8	*Stakeholder*	The transport provider shall provide users access to AVs, additional services, and access to real-time information.	The transport provider must provide transport means and information to users.
U9	*Stakeholder*	The MaaS provider shall provide a platform that enables its users to plan their journeys and payment options.	MaaS systems use a digital platform, it is a core characteristic.
U10	*Stakeholder*	The data provider shall provide the system with secure data and analytics.	The data provider acts as a data intermediary in the ecosystem.
U11	*Stakeholder*	The insurance provider shall provide insurance to AVs, users, and a third party.	Laws and regulations specify the need for insurance.
U12	*Stakeholder*	The system shall be trusted for the users.	Increase adaptation rate and usability.

Table 3: System requirements.

ID	Source	Type	Requirement	Justification
S1.1	Technical	F	The system shall enable user registration.	Registration is required to have an ID and user preferences.
S1.2	Technical	F	The system shall enable the user to personalize his account according to his preferences.	It is a core characteristic of MaaS.
S1.3	Technical	F	The system shall provide the user with a unique ID.	A unique identifier is needed to relate the user in different transactions.
S1.4	Technical	F	The system shall enable the user to access the services provided.	User needs access to services to use them.
S2.1	Technical	F	The system shall enable the user to plan a trip by filtering: type of road, fastest route, avoid tolls,	Provide options to the user to plan their trips.

			cheapest, time.	
S2.2	Technical	F	The system shall enable the user to select the number of passengers.	The number of passengers is relevant for capacity and insurance purposes.
S2.3	Technical	F	The system shall enable the user to select the type of AVs.	If different sizes of AVs are offered user must be able to select according to his preferences.
S2.4	Technical	F	The system shall enable the user to select a starting point.	Needed starting location to route planning.
S2.5	Technical	F	The system shall enable the user to select an ending point.	Needed ending location to route planning.
S3.1	Technical	F	The system shall enable the user to reserve a trip.	Needed to lock an AVs to a specific user.
S3.2	Technical	F	The system shall enable the user to cancel the trip.	If the user must cancel the trip for any reason.
S3.3	Technical	F	The system shall enable the user to choose a route.	The user might want to use a particular route.
S4.1	Technical	F	The system shall provide the user with real-time information.	A core characteristic of MaaS.
S4.2	Technical	F	The system shall provide the user with high-speed connectivity.	High speed is needed for AVs and real-time information.
S4.3	Technical	F	The system shall provide extensive geographical availability in the city of Amsterdam.	To get coverage in the whole city of Amsterdam.
S5.1	Technical	F	The system shall provide online payment solutions.	All systems transactions are online.
S5.2	Technical	F	The system shall provide cashless payment solutions.	All systems transactions are online.
S5.3	Technical	NF	The system shall be easy to use.	Easy access to lower entry barriers.
S5.4	Technical	F	The system shall provide the ability to track payments.	The user might want to check his payments or report them.
S6.1	Technical	F	The system shall provide an identification of the AV for the user.	The user needs to recognize which is his vehicle.
S6.2	Technical	F	The system must allow the AV to recognize clients via smartphone, smartwatch, or wearable device.	Means for the AV to find the user.
S6.3	Technical	F	The system must allow the user to AV via smartphone, smartwatch, or wearable device.	Means for the user to find the AV.
S6.4	Technical	F	The system must allow the user to gain access to the AVs.	The user would need to unlock the car to enter.
S6.5	Technical	F	The system must enable the AV to let the user in.	AV will need to be unlocked by the user to board it.
S7.1	Institutional	NF	The system must consider privacy by design.	User data could be sensitive and should comply with GDPR.
S7.2	Institutional	NF	The system must consider data minimization and purpose limitation regarding user data.	GDPR principles for processing personal data.
S7.3	Institutional	F	The system must notify the user if personal data is a breach.	GDPR breach notification compliance.
S7.4	Institutional	F	The system must allow the user to access his personal data.	GDPR right of access compliance.
S7.5	Institutional	F	The system must allow the user to delete his data.	GDPR right to erasure compliance.
S7.6	Institutional	F	The system must ask for consent for data gathering and processing.	GDPR affirmative consent compliance.
S7.7	Institutional	F	The system must process data lawfully, fairly and in a transparent manner.	GDPR data processing compliance.
S7.8	Institutional	F	The system must maintain user data accurate and up to date.	GDPR data accuracy compliance.
S7.9	Institutional	F	The system must keep user data no longer than it is necessary.	GDPR storage limitation compliance.
S7.10	Institutional	F	The system must process data in a secure way and protect it against unauthorized processing, accidental loss, destruction, or damage.	GDPR integrity and confidentiality compliance.

S8.1	Stakeholder	F	The system must offer transport operator capacity to the users.	To offer AVs to the users.
S8.2	Stakeholder	F	The system must allow the transport provider to offer additional services.	To offer additional services to users, like Wi-Fi, music, video, games, etc.
S8.3	Stakeholder	F	The system must enable transport payments for additional services.	Payments for additional services are needed.
S8.4	Stakeholder	F	The system must be able to receive and process transport provider data.	A core characteristic of MaaS.
S9.1	Stakeholder	F	The system must provide a unique central platform.	A core characteristic of MaaS.
S9.2	Stakeholder	F	The system must be able to receive and process data from the MaaS provider.	A core characteristic of MaaS.
S10.1	Stakeholder	F	The system must be able to receive and process data from the data provider.	A core characteristic of MaaS.
S10.2	Stakeholder	F	The system must be able to receive data securely and reliably.	To ensure data granularity.
S10.3	Stakeholder	F	The system must be able to capture data from users.	To offer personalized services.
S10.4	Stakeholder	F	The system must be able to capture data from the infrastructure.	Data from infrastructure is needed to provide key services.
S11	Stakeholder	F	The system must be able to receive and process data from the insurance provider.	Data such as payments, AV telemetry, and infrastructure could be useful for liabilities purposes.
S12	Technical	NF	The system must support a diversity of actors.	Able to support a multi-actor system.
S13	Technical	NF	The system must be scalable.	Possibilities of further expansion of the system.
S14	Technical	F	The system must be able to take transactions automatically.	Transactions are needed between all the stakeholders.

Figure 2: BC Architecture, adapted from Tasca et al., (2017)