Bus Inf Syst Eng
https://doi.org/10.1007/s12599-024-00856-9

RESEARCH PAPER

Toward Seamless Mobility-as-a-Service

Providing Multimodal Mobility Through Digital Wallets

Alexandra Hoess · Jonathan Lautenschlager · Johannes Sedlmeir · Gilbert Fridgen · Vincent Schlatt · Nils Urbach

Received: 10 February 2022 / Accepted: 14 November 2023

Abstract With growing awareness of sustainability and convenience expectations, customers are increasingly demanding integrated and seamless mobility in the form of mobility-as-a-service (MaaS). However, as centralized MaaS platforms have thus far failed to integrate a critical share of mobility service providers (MSPs), travelers lack opportunities to efficiently combine the various mobility services required for seamless end-to-end itinerary coverage. Particularly, MSPs often refuse to collaborate by devolving control over customer interfaces or sensitive data owing to threats of market power concentration. While alternative blockchain-based approaches aim to provide equal market access, they cannot sufficiently align competing business goals and face substantial problems resulting from the replicated processing of sensitive data. Both researchers and practitioners have recently suggested decentralized digital identity management enabled by digital wallets as a promising mechanism to exchange verifiable identity attributes while mitigating problems related to data aggregation. Following a design science research approach, the article accordingly explores how digital wallets can address the shortcomings of existing approaches to MaaS. It contributes a novel IS architecture and principles for a design at the nexus of centralized and decentralized solutions to mitigate tensions between cooperation and competition. Further, the findings indicate that when building decentralized solutions, one should also consider components beyond blockchain and smart contracts.

Keywords Coopetition · Digital identity · Digital wallet · MaaS · Self-sovereign identity

Accepted after 3 revisions by Óscar Pastor

A. Hoess · J. Sedlmeir · G. Fridgen
Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, Luxembourg
e-mail: alexandra.hoess@uni.lu

J. Sedlmeir
e-mail: johannes.sedlmeir@uni.lu

G. Fridgen
e-mail: gilbert.fridgen@uni.lu

J. Lautenschlager · N. Urbach
Frankfurt University of Applied Sciences, Frankfurt am Main, Germany
e-mail: nils.urbach@fb3.fra-uas.de

J. Lautenschlager (✉) · J. Sedlmeir · V. Schlatt · N. Urbach
Branch Business and Information Systems Engineering of the Fraunhofer FIT, Bayreuth, Germany
e-mail: jonathan.lautenschlager@fit.fraunhofer.de

V. Schlatt
e-mail: vincent.schlatt@uni-bayreuth.de

J. Sedlmeir · V. Schlatt
FIM Research Center, University of Bayreuth, Bayreuth, Germany

1 Introduction

The increasing societal awareness of climate change and the ongoing digital transformation are pressuring and incentivizing mobility providers to offer more sustainable and seamless mobility (Schulz et al. 2021; Willing et al. 2017). Researchers and practitioners are increasingly advocating mobilityas-a-service (MaaS) as a means to meet these customer preferences. MaaS involves the integration and seamless combination of various mobility services (Willing et al. 2017). Information and communication technologies (ICTs) can promote corresponding

Published online: 19 February 2024

business models by facilitating the procurement and coordination of environmentally friendly mobility services and transport infrastructures (Ketter et al. 2022; Sochor et al. 2015). Yet, we still lack corresponding IT solutions that enable MaaS. Particularly, travelers seek solutions to efficiently combine and book the various mobility services required for seamless end-to-end trip coverage (Butler et al. 2021; Schulz et al. 2021). For a single itinerary, travelers often need to navigate multiple travel planning applications, web interfaces, and booking processes of various public and private (MSPs) (Hoffmann et al. 2021). However, related booking processes involve inconvenient onboarding and log-in processes, as they force travelers to create and manage several accounts. Consequently, many travelers opt for personal car ownership instead (Cottrill 2020; Georgakis et al. 2019). It is evident that climate protection through seamless and shared mobility services requires less complex booking processes (Barr 2018). Such improvements could have a profound environmental and economic impact. For instance, integrated mobility systems in 50 major cities worldwide with a total population of 50 million could improve safety and reduce pollution-related damages by up to $600 billion per year (Bouton et al. 2017).

Although some MaaS solutions already exist, these struggle to align and integrate multiple modes of public and private mobility services (e.g., flights, railway, and car-sharing services); specifically on an international level (-Hoess et al. 2021; Schulz et al. 2020). In particular, they seem to fail to sufficiently balance coopetition – i.e., the concurrent co-operation and competition (Hoffmann et al. 2018) – between MSPs, which is important to enable value co-creation and ensure individual MSPs' value capture (Hoess et al. 2021). Coopetition within the MaaS ecosystem is especially challenging owing to the ambivalent role of data. On the one hand, the exchange of MSPs' sensitive business data and travelers' identity data are required for value co-creation. However, at the same time, such data need to be protected by MSPs not only to comply with customers' privacy expectations and data protection regulations but also because it gives them a competitive advantage (Ford and Håkansson 2013; Ritala 2022; Hermes et al. 2020). Accordingly, centralized MaaS platforms, operated by individual MSPs, struggle with attracting other MSPs to join the platform to cooperate. In particular, MSPs often refuse to integrate their services into a competitor's platform, as they fear losing their strategic position in the mobility market by ceding the customer interface and strategic data (Hoess et al. 2021; Schulz et al. 2020).

To break this impasse, researchers and MSPs are exploring the potentials of decentralized, mostly blockchain-based, infrastructures. These allow for the combination of mobility services on a neutral platform that is independent of a distinguished service aggregator (Hoffmann et al. 2021; Goulding and Kamargianni 2018). While blockchain-based approaches have demonstrated some potential to create more balanced competition (Hoess et al. 2021; Jensen et al. 2019), they are not without limitations. In particular, blockchain technology provides only limited capabilities to protect strategic business data owing to its characteristic of replicated transaction processing (Sedlmeir et al. 2022b; Zhang et al. 2019; Köhler and Pizzol 2020). This degree of transparency naturally conflicts with MSPs' needs to protect strategic data for gaining a competitive advantage in the market. Further, the processing of travelers' personal data on blockchains would raise substantial regulatory concerns (Rieger et al. 2019; Sedlmeir et al. 2022b).

To mitigate these challenges, recent research has suggested to base MaaS systems on a bilateral exchange of verifiable identity attributes between MSPs and travelers (Hoffmann et al. 2021). Here, the use of self-sovereign identity (SSI) and digital wallets may play a pivotal role. Digital wallets empower users to manage selected machine-verifiable identity documents, such as ID cards, driver's licenses, or credit cards, and share attributes bilaterally with any verifier, for instance, an MSP (Sedlmeir et al. 2022a; Weigl et al. 2022). In doing so, digital wallets offer a promising solution for the seamless and interoperable exchange of verifiable identity information (Feulner et al. 2022). These opportunities are also reflected in current policy making, such as the European Union (EU)'s revision of the electronic Identification, Authentication and Trust Services (eIDAS) regulation and the decision to provide its citizens with European Digital Identity Wallets (Anke and Richter 2023; Hoess et al. 2023). Thus, digital wallets could be used for designing a decentralized system that facilitates interaction between travelers and coopeting MSPs. However, so far, little is known about the general requirements of an IT architecture to enable seamless MaaS provision. Further, in this context, the potential role and design of digital wallet-based architectures and their differences compared to alternative, blockchain-based decentralized approaches have not been explored in previous research. In this paper, we systematically identify these requirements and design and evaluate an IT architecture that aims to address them to provide seamless MaaS. Thus, we ask the following research questions (RQs):

RQ1: *What are the requirements for an IT architecture to support seamless MaaS provisioning?*
RQ2: *How can these requirements be addressed through an IT architecture based on digital wallets?*

We approach these RQs with design science research (DSR) (Peffers et al. 2007) and structure this paper

accordingly. We first outline the theoretical background of our work in Sect. 2 to introduce the knowledge base on which we ground our design and introduce our applied DSR approach in Sect. 3. We then turn to our solution space and comprehensively describe the requirements and design objectives for MaaS solutions (Sect. 4) as well as the proposed design – an IT architecture for MaaS based on digital wallets (Sect. 5). Sect. 6 reports on our expository instantiation and qualitative criteria-based evaluation of the artifact through expert interviews (Sonnenberg and vom Brocke 2012). Building on these results, we derive a nascent design theory in the form of three design principles (DPs) for seamless MaaS provisioning architectures based on our artifact and its qualitative evaluation (Gregor and Hevner 2013) in Sect. 7. This design theory contributes to research on MaaS and coopetitive service markets by highlighting the importance of a hybrid design comprising both centralized and decentralized components to balance coopetitive needs. These DPs also provide practical guidance for implementing identity management layers in coopetitive markets to facilitate service provisioning.

2 Theoretical Background

We now outline the theoretical background that underlies our work. We first introduce the concept of MaaS and illustrate existing solution approaches and related challenges. After describing the problem space we aim to contribute to, we introduce the key concepts that underlie SSI and digital wallets, which form the basis of our artifact.

2.1 Mobility-as-a-Service

Travelers increasingly demand more sustainable and efficient mobility offers in the sense of a common sharing mobility economy (Ketter et al. 2022; Willing et al. 2017). To date, traveling along itineraries with multiple mobility services is often cumbersome. This process involves many individual steps for each of potentially multiple MSPs; including the selection of suitable services for the different subroutes, time-consuming onboarding or authentication processes to log into booking portals, and payment (Sochor et al. 2018). To mitigate these problems, travelers and MSPs turn to the concept of MaaS, which aims to enable travelers to seamlessly combine different publicly or privately offered mobility services (e.g., car and bike sharing, taxis, buses, subways, rail services, or air travel) with low planning and booking effort (Sochor et al. 2018). In doing so, MaaS intends to provide more sustainable mobility solutions by inducing a shift from personal vehicle ownership to a comprehensive portfolio of public and private mobility services (Willing et al. 2017). MaaS not only means a paradigm shift for travelers but also for competing MaaS who need to collaboratively coordinate their services to enable the seamless planning, ticketing, and payment of services from different MSPs and make use of corresponding network effects (Hoffmann et al. 2021; Smichowski 2018).

Various MSPs have explored how to enable MSPs at both regional and global levels (Willing et al. 2017). These approaches mainly build on centralized systems (Calderón and Miller 2019; Jittrapirom et al. 2017), which typically comprise a proprietary two-sided platform that is operated by a single MSP or a dedicated joint venture between MSPs (Hoess et al. 2021; Schulz et al. 2020). This entity aggregates mobility services and makes them available to travelers for booking. Centralized solutions seem promising because they exhibit strong network effects and offer technical standardization with low implementation complexity (Casady 2020; Esztergár-Kiss et al. 2020). However, existing centralized solutions are limited in their regional scope or in the diversity of integrated mobility services. For instance, some regional and national solutions allow travelers to pay for mobility services via an RFID card or with a mobile app when entering a vehicle (Shaheen and Cohen 2012). While these RFID card-based or app-based systems cover a large set of public mobility services that are not subject to capacity-bound ticketing, they do not allow for booking mobility services in advance and are often restricted only to public services. Other approaches, such as Whim or Moovel, contain a broader portfolio including public and private mobility service offerings (Arias-Molinares and Garcia-Palomares 2020; Santos and Nikolaev 2021). These solutions are, in turn, restricted to specific municipal regions and do not support long-distance travel. Other popular aggregators, such as skyscanner.net or thetrainline.com, have managed to consolidate a global service portfolio but are limited to a single mode of mobility (i.e., flights and rail services, respectively) and thus cannot meet the expectations of travelers who seek seamless multimodal mobility.

Accordingly, centralized platforms have struggled to establish cross-regional stakeholder cooperation between various public and private MSPs despite the apparent presence of positive network effects. They particularly fail to attract a critical mass of MSPs required for a holistic MSPs offering (Schulz et al. 2020). Previous research has hinted at centralized data storage and proprietary protocols and interfaces as key barriers to the adoption of comprehensive MaaS solutions (Bothos et al. 2019; Schulz et al. 2020). These designs lock MSPs into one MSP's platform and limit opportunities to offer services across different platforms (Constantinides et al. 2018). As a result, centralized approaches entail problems relating to intermediaries' market power (Nguyen et al. 2019). A potential

reason is that such market players may become dominant and may impose unfair market conditions through their pricing of mobility services (Hoffmann et al. 2021). Fearing such behaviors, MSPs resent offering their mobility services via a third-party's platform when they expect to become dependent on this platform and potentially be subject to price discrimination by a dominant market player in the future (Hoess et al. 2021; Schulz et al. 2020).

To avoid these problems, practitioners and researchers have pointed to decentralized alternatives that establish non-proprietary, interoperable MSPs solutions and offer the participating MSPs opportunities for equal market access while avoiding lock-in effects (Hoffmann et al. 2021; Hoess et al. 2021; Lamberti et al. 2019). In particular, these solutions aim to foster cooperation through the decentralized and transparent exchange of mobility service offerings (Bothos et al. 2019; Stockburger et al. 2021). Technical considerations to decentralized MaaS often include blockchain as a neutral, inter-organizational system for mobility services (Hoffmann et al. 2021; Lamberti et al. 2019; Nguyen et al. 2019). These approaches use smart contracts to represent business logic, streamline processes, increase transparency, as well as automate payments. While such designs arguably address some of the above-mentioned challenges, they face significant obstacles regarding practical diffusion. For instance, in inter-organizational settings, organizations may find it hard to agree on a smart contract implementation that everyone considers fair and reflects all affected businesses' interests (Kannengießer et al. 2022). The implementation of blockchain-based solutions also entails several operational complexities for MSPs (Sternberg et al. 2020; Toufaily et al. 2021). For instance, blockchain-based MaaS solutions have to meet high demands on throughput and latency while keeping transaction costs low, which may be challenging to meet even with dedicated enterprise blockchains (Guggenberger et al. 2021). Owing to the replicated processing and tamper-resistant storage of information, blockchain-based solutions also face significant issues regarding the handling of sensitive business and personal data (Zhang et al. 2019; Platt et al. 2021; Sedlmeir et al. 2022b). This hurdle stems from the well-known and fundamental trade-off between data confidentiality and the need for availability and related processing of business and traveler data in smart contracts on-chain (Kannengießer et al. 2020).

An alternative to smart contract-based solutions could be provided by SSI and digital wallets for travelers. This approach avoids the replicated and immutable storage of travelers' personal and ticket data on a blockchain and the complexity of smart contract governance. Instead, sensitive information is exchanged bilaterally between MSPs and travelers. More specifically, travelers store personal data and tickets locally in their wallet in the form of machine-verifiable attestations and selectively disclose relevant identity data to MSPs (Bothos et al. 2019; Hoffmann et al. 2021; Stockburger et al. 2021). Hoffmann et al. (2021) developed a decentralized modular architecture for MaaS based on such digitally signed attestations and blockchain technology. To support traveler authentication, a blockchain provides a decentralized public key infrastructures (PKIs) that equips travelers with globally unique identifiers. However, this approach results in privacy-related problems (Hoess et al. 2023; Schlatt et al. 2022). Hoffmann et al. (2021) also introduce dedicated discovery service providers that use the blockchain to maintain a registry of MSPs and their public keys. As such, they govern market access and support travelers in selecting compatible mobility services. However, it remains unclear which kind of data is stored in these registries. Moreover, while the authors describe that travelers negotiate transport conditions and settle corresponding transactions in bilateral interactions with the respective MSP, they do not specify how travelers identify relevant mobility services and whether smart contracts play a role in the coordination of mobility services.

2.2 Self-Sovereign Identity and Digital Wallets

SSI aims to empower end users to control their digital identities by managing machine-verifiable attestations in their digital wallet, without being dependent on a distinguished identity provider (Weigl et al. 2022; Sedlmeir et al. 2022a). As such, the general concept of SSI is inspired by today's identity management in the physical realm. An emerging standard for corresponding attestations is verifiable credentials (VCs). A VC is a digital certificate (i.e., it is cryptographically signed) and confirms one or multiple attributes of a subject (Schlatt et al. 2022; Lacity et al. 2023). Digital signatures make VCs less susceptible to tampering than their physical counterparts and allow them to be machine-verifiably presented to third parties (Soltani et al. 2021; Feulner et al. 2022; Lacity et al. 2023). The exchange of these certificates appears in bilateral interactions between issuers and holders, and holders and verifiers, respectively (Sedlmeir et al. 2022a; Mühle et al. 2018). Issuers attest, digitally sign, and transfer these VCs to the holder. Holders then store VCs on their device and, when needed, present them to a verifier (Fig. 1). In doing so, holders generate a verifiable presentation (VP) that can combine and disclose selected identity attributes from multiple VCs in a data-minimizing way instead of transferring the VC directly (Feulner et al. 2022; Babel and Sedlmeir 2023). To digitally verify VPs, verifiers typically rely on public registries that provide additional information about the issuer – for instance, the corresponding public

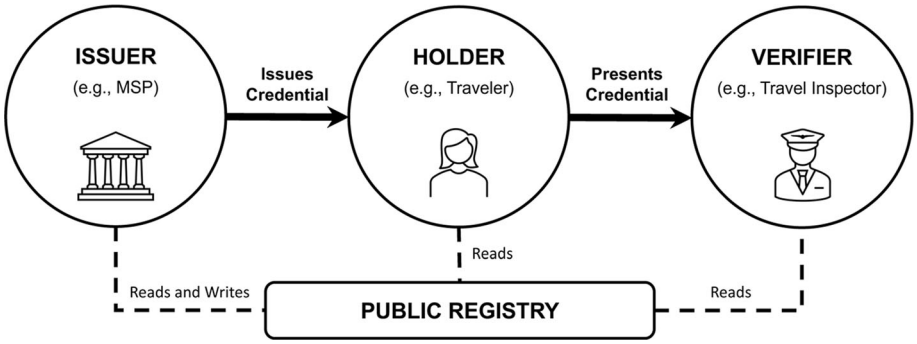

Fig. 1 SSI-based exchange of verifiable credentials

key that allows for the verification of a signature – or on the VC's state of revocation (Davie et al. 2019; Schlatt et al. 2022). A prerequisite is that a verifier trusts the issuer to truthfully issue VCs (Davie et al. 2019).

To manage their VCs and interact with issuers and verifiers, holders require dedicated software applications (e.g. a mobile app) – referred to as digital wallets (Lacity et al. 2023). Digital wallets are portable applications that allow their users to securely store and manage their digital identifiers and attestations, such as digital representations of ID cards or passports (Jørgensen and Beck 2022; Sartor et al. 2022). Digital wallets give users direct control over their identity information and deploy features to selectively disclose identity attributes (Lacity et al. 2023). They implement message signing protocols, the identification of other entities (e.g., via their decentralized identifiers (DIDs) and the related DID-Auth protocol), support establishing and maintaining secure connections with other entities, and facilitate the storage of VCs (Sartor et al. 2022). Furthermore, digital wallets can implement zero-knowledge proofs (ZKPs) (Sedlmeir et al. 2022a; Babel and Sedlmeir 2023) which allow a subject to prove an identity claim to another entity without disclosing any information beyond what is required. For instance, using zero-knowledge proofs (ZKPs) the holder can derive a proof of being older than 18 at the time of the VP from their VC without sharing the date of birth included in a VC (Lacity et al. 2023). More intricate examples are proofs of non-inclusion of VCs (corresponding to disclosed identity attributes) in a public revocation registry and proofs of hardware binding without revealing the corresponding unique, persistent cryptographic identifiers included in a VC (Babel and Sedlmeir 2023; Feulner et al. 2022).

Issuers and verifiers use cloud agents integrated into their back-ends – as a pendant to travelers' digital wallets – to sign or revoke VCs, verify VPs, and manage the communication with users' digital wallets. An advantage of cloud agents running on a server is that they are permanently online and have a persistent IP address. In contrast, messages that are sent to mobile wallet apps need to be relayed by a service that is authorized to send notifications to a wallet app (Hardman 2021). This "mediation agent" is typically operated by the wallet app provider and pushes notifications to the wallet.

3 Research Method

To conceptualize a seamless MaaS architecture that builds on digital wallets, we followed a DSR approach. DSR involves the design and development of innovative and meaningful artifacts such as constructs, methods, models, or instantiations for a specific practical problem (Hevner et al. 2004; Gregor and Hevner 2013). We developed a model in the form of a comprehensive architecture and corresponding required processes that facilitates seamless MaaS based on the use of digital wallets (Hevner et al. 2004). We addressed the need for rigor and relevance (Peffers et al. 2007) by grounding our work on previous research as well as practical insights provided through our expert interviews. For an IT artifact to strongly contribute to IS research, it must address a relevant business need, which can result from the individuals, organizations, or technologies present in an environment (Hevner et al. 2004). As discussed in Sect. 1, the development of a seamless MaaS architecture that can manage to unite a broad spectrum of MSPs represents such a business need.

We adopted the approach of Peffers et al. (2007) to create such a meaningful IT artifact. From a technical and organizational perspective, we identified a lack of coordination among competing MSPs, risks of concentration of market power, and insufficient access control and data protection as core problems of current (de)centralized MaaS solutions. Following the problem formulation, we answer RQ1 by identifying design objectives and associated requirements of a potential solution. To this end, we complemented our DSR approach with a systematic literature review (SLR) (Brereton et al. 2007; Webster and Watson 2002) and 17 ex-ante expert interviews, which we conducted as part of a previous study relating to decentralized MaaS, as outlined in Sect. 3.1. We then performed

iterative build-and-evaluate loops to develop a MaaS architecture that addresses the identified design objectives and requirements. We iterated through the design and development of the IT artifact by demonstrating and evaluating its functionality and usefulness at each stage of development. To this end, we opted for a criteria-based qualitative evaluation. As we will outline in Sect. 3.2, we instantiated a prototype that allows for booking and verifying travel tickets using a digital wallet app to demonstrate our conceptual architecture in use (Sonnenberg and vom Brocke 2012) and conducted a criteria-based evaluation by means of seven ex-post expert interviews (Sonnenberg and vom Brocke 2012; Venable et al. 2016). We present the final stage of our architecture in Sect. 5.

To also contribute more abstract and generalizable knowledge that can be used for theoretical discussion (Gregor and Hevner 2013), we elevated the implicit knowledge contribution in our IT artifact in the form of DPs for SSI-based MaaS architectures. This is helpful, since the potential of SSI-based solutions for MaaS is increasingly discussed in research and practice, yet there are no general DPs in the existing literature. Specifically, we identified three generic principles that may also be applicable to other coopetitive service markets. We discuss these design principles in Sect. 7. The communication of our research findings and the sharing of the code for our prototype conclude our DSR.

3.1 Derivation of Design Objectives

To answer RQ1, which concerns the identification of design requirements, and to ground our work on prior knowledge, we conducted an SLR following the best practices outlined by Brereton et al. (2007) and Webster and Watson (2002). We used the search string *("mobility as a service" OR "mobility-as-a-service" OR MaaS) AND (intermodal OR multimodal) AND (transport OR mobility)* to cover related work on intermodal and multimodal transport as well as MaaS. We conducted our search using seven databases (*Scopus*, *Science Direct*, *ACM Digital Library*, *EBSCOHost*, *IEEEXplore*, *Web of Science*, and *AIS eLibrary*). We performed all search runs on full text and metadata. Our initial search returned 2,165 hits, in which we identified and removed 114 duplicates. Next, we screened these results (2,051 hits) in four process steps: (1) title screening, (2) abstract screening, (3) full-text analysis, and (4) forward and backward search (Brereton et al. 2007; Moher et al. 2009). In each step, we focused on articles that match the following inclusion criteria: the article identifies requirements for MaaS architectures or presents a design or implementation of MaaS systems. We included both centralized and decentralized MaaS solutions to avoid bias and to ground our design on a rich knowledge base (vom Brocke et al. 2015). We excluded articles that are not related to the MaaS domain, or that do not provide any architectural requirements, challenges, or solution approaches. We also excluded articles not written in English. Considering these criteria, we identified 147 articles after the initial title screening that we considered relevant for further analysis. Of these, we classified 21 as relevant after screening all remaining articles' abstracts. The full-text analysis yielded a subset of 10 relevant articles, which we supplemented with four additional articles we found through a forward and backward search and an additional gray literature analysis using *Google Scholar* and other search engines (e.g., Google Search). Our final selection thus comprises a foundation of 14 publications.

Owing to the small number of results, we considered the SLR insufficient for deriving comprehensive design objectives that are relevant to the practical environment. In particular, the articles we identified all focus on technical components and do not incorporate business perspectives. Therefore, we decided to enrich our literature study with 17 expert interviews that one of the authors conducted as part of a prior study on decentralized MaaS. This interview set includes experts from 14 different organizations in the mobility services industry, including established MSPs, original equipment manufacturers (OEMs), MSP start-ups, and IT consultancies. Table 1a features the selected practitioners' and researchers' backgrounds. All experts were knowledgeable about both the organizational and technical requirements of public and private stakeholders in the mobility sector, as well as the specific business and technical needs for MaaS. The diverse backgrounds of these experts enabled us to complement the requirements for a seamless MaaS solution from the SLR from a broad socio-technical perspective, as suggested by vom Brocke et al. (2020). In these interviews, the experts provided insights on the challenges of current MaaS solutions as well as the requirements and opportunities of an open, decentralized MaaS system. They also discussed the role and current challenges of blockchain as a technical basis for decentralized MaaS. The interviews lasted on average around 51 minutes. We audio-recorded and fully transcribed the interviews and subsequently coded each interview following a two-stage process of open and axial coding (Saldaña 2013). We conducted open coding to gain a first broad overview of the needed requirements and performed the second round (axial coding) to further categorize and condense our findings into generalizable design objectives (Strauss and Corbin 1998).

3.2 Evaluation and Demonstration

We carried out expert interviews and a qualitative, criteria-based evaluation to assess the feasibility and usefulness of

Table 1 Experts' professional background and experience

#	Organizational responsibility	Experience
(a) Ex-ante interviews		
1	Project and product manager (private MSP)	$\geq$ 1 years
2	Business developer and IT consultant (consultancy)	$\geq$ 2 years
3	Business developer (public MSP)	$\geq$ 7 years
4	Head of strategic future projects (OEM)	$\geq$ 2 years
5	Head of business development (transportation & rail)	$\geq$ 7 years
6	CEO (IT consultancy)	$\geq$ 5 years
7	CTO (private MSP)	$\geq$ 3 years
8	Product owner (tech mobility)	$\geq$ 1 years
9	Business developer (public MSP)	$\geq$ 3 years
10	CEO (tech mobility)	$\geq$ 10 years
11	Consortium partner (mobility association)	$\geq$ 10 years
12	Blockchain business developer (OEM)	$\geq$ 3 years
13	Partner Management (OEM)	$\geq$ 5 years
14	CEO (mobility association)	$\geq$ 3 years
15	Blockchain developer (tech company)	$\geq$ 5 years
16	Managing consultant (tech company)	$\geq$ 3 years
17	Blockchain project manager (tech company)	$\geq$ 4 years
(b) Ex-post interviews		
18	CEO (MaaS provider)	$\geq$ 20 years
19	CEO (IT consultancy)	$\geq$ 10 years
20	Project manager and researcher (OEM)	$\geq$ 10 years
21	Product owner for data exchange (OEM)	$\geq$ 6 years
22	Product owner for emerging technologies (OEM)	$\geq$ 4 years
23	Head of blockchain (IT service provider)	$\geq$ 20 years
24	Chief blockchain architect (transport IT and services)	$\geq$ 9 years

our MaaS architecture (Venable et al. 2016). With the help of the experts' feedback, we continually redefined the components and processes in iterative build-and-evaluate loops as suggested by Hevner et al. (2004). We conducted seven ex-post expert interviews. As for the ex-ante interviews, we approached experts from different backgrounds to assess the implementation of our MaaS architecture from multiple angles (see Table 1b).

We conducted semi-structured interviews to generate rich data (Myers and Newman 2007) and applied the following logical sequence (Schultze and Avital 2011). First, we presented our research by suggesting SSI enabled by digital wallets as promising approach to facilitate seamless MaaS. We then presented our prototype in a live demonstration to illustrate our artifact in use and to inform the subsequent discussions. Specifically, our prototype allowed us to demonstrate the processes of requesting and storing travel tickets as well as the subsequent ticket verification from the traveler's perspective using a digital wallet. In addition to our prototype, we presented our key artifact – the underlying architecture, including components and processes. Following our demonstration, we discussed our design's feasibility and usefulness, considering the requirements that we had identified for seamless MaaS architectures. To this end, we first asked for open feedback on the architecture and our demonstration. We then discussed the feasibility of our solution and both its fitness and remaining needs for improvement in relation to our design objectives. We focused on the data management implied by our solution, its effects on the cooperation and competition between MSPs, manageability aspects, and opportunities to connect our solution to existing MaaS platforms. Finally, we discussed user experience-related aspects.

Each interview lasted around 58 minutes on average. As for the ex-ante interviews, we audio-recorded and transcribed each ex-post interview and analyzed the transcripts through two cycles of coding. We then applied provisional coding, i.e., we coded the statements based on the identified design objectives and requirements, which served as the initial list of coding categories (Saldaña 2013). This helped us to assess our artifact's fit. In the second coding cycle, we revised our codes to identify more overarching mechanisms of our solutions and linked our codes through axial coding (Saldaña 2013; Strauss and Corbin 1998).

From this axial coding, we derived three DPs for IT architectures for MaaS (Gregor and Hevner 2013).

4 Design Objectives and Requirements for MaaS Architectures

We derived four design objectives and 12 associated requirements for MaaS architectures from our SLR and the ex-ante expert interviews. We now describe these design objectives and requirements in detail. To justify their relevance, we refer to previous studies and highlight the number of experts that confirmed each statement leading to our objective (in parentheses). Table 2 summarizes the design objectives and requirements and provides a detailed overview of the corresponding experts and the studies that we drew our statements from.

4.1 Design Objective 1 – Neutrality

Successful MaaS implementations need to incentivize various MSPs to cooperate, but this remains a major challenge (Calderón and Miller 2019). This challenge is driven by the prevailing competition between MSPs, their individual goals of dominance in the mobility market, as well as their heterogeneous business interests (Schulz et al. 2020). For instance, the private sector typically seeks to increase revenues or market share while the public sector often considers other gloals, such as reducing the use of privately owned vehicles and expanding the demand for public mobility services (Arias-Molinares and Garcia-Palomares 2020). While MSPs typically compete for providing individual service offerings and selling them to travelers, the presence of complementary service offerings – even provided by another MSP – increases their own services' value and allows them to benefit from network effects (Jacobides et al. 2018; Katz and Shapiro 1994) (7 experts). Thus, MSPs appreciate some degree of

Table 2 Design objectives and requirements for a seamless MaaS solution

Design objective	Requirements		Description	References	Experts
Neutrality	R1	Coopetition	MSPs must be able to compete and cooperate at the same time	Arias-Molinares and Garcia-Palomares (2020), Calderón and Miller (2019), Polydoropoulou et al. (2020b)	1–17
	R2	Disintermediation	Avoidance of intermediaries that aggregate market power	Jittrapirom et al. (2017), Sochor et al. (2016)	2, 6, 8, 15–17
	R3	Openness	Openness allows MSPs to integrate other MSPs' service offerings and vice versa	Arias-Molinares and Garcia-Palomares (2020), Kamargianni et al. (2016), Paiva et al. (2021)	2, 4, 7–10, 15–17
Data protection	R4	Processing of business data	The MaaS solution must protect sensitive business data	Cottrill (2020), Paiva et al. (2021)	1, 5–7, 9–10, 12–17
	R5	User privacy protection	The MaaS solution must protect sensitive user data	Hoffmann et al. (2021), Lamberti et al. (2019), Stockburger et al. (2021), Zhao et al. (2020)	5–7, 9, 12
Manageability	R6	Modularity	Modularity and the inherent decentralization enable the diversification of services offerings	Bothos et al. (2019), Hoffmann et al. (2021), Lamberti et al. (2019), Nguyen et al. (2019)	1–4, 6, 8, 10, 12–13, 15–17
	R7	Process efficiency	The MaaS solution needs to process interactions between mobility users and MSPs efficiently to handle the high frequency and demand of mobility service usage	Calderón and Miller (2019), Lamberti et al. (2019), Nguyen et al. (2019)	2, 12–15
End-user experience	R8	Seamless data sharing	The MaaS solution should enable seamless and verifiable personal data sharing to ensure fast on-boarding and booking processes	Hoffmann et al. (2021), Paiva et al. (2021), Stockburger et al. (2021)	1–2, 5–6, 8, 13–14
	R9	Customer support	Travelers need to know who to contact in case of issues with the requested mobility service	Polydoropoulou et al. (2020a)	1–2, 4, 6–10, 13–14, 16

cooperation to foster value creation by levering network effects on both sides (Smichowski 2018; Tomaino et al. 2020). Our experts, therefore, recommend considering the aspect of *coopetition (R1)* between MSPs (Hoffmann et al. 2018) (17 experts). Regarding the design of a corresponding platform solution, an intermediary role allows MSP to establish strong ties with the customer and maintain or extend their current market share and profits (de Reuver et al. 2009; Schulz et al. 2020). Acting as an intermediary allows an MSP to reduce threats of cannibalizing its own mobility service portfolio, as it grants them control of third-party service offerings. An intermediary role also allows an MSP to protect its own business data and even create value from other parties' business data (Bothos et al. 2019; Polydoropoulou et al. 2020a). Thus, these intermediaries may gain a monopolistic or at least dominant position in the MaaS domain (Smith et al. 2020). This means that established MSPs are particularly interested in creating and hosting such a platform themselves and managing all customer interactions (Schulz et al. 2020; Smith et al. 2020). On the other hand, MSPs fear becoming merely a service provider when integrating their services and devolving customer interfaces to another MSPs's platform (Jittrapirom et al. 2018; Sochor et al. 2016) (11 experts). Expert 2, describes this dilemma as follows: *"everyone would like to be the central spider on the web. Everybody would like to be the central player who integrates all mobility providers, and everybody is afraid that someone else will become this player, and therefore it hinders these integration efforts, as one would imagine it now."*

To avoid a deadlock that inhibits the establishment of an integrated solution that can unlock value co-creation and network effects, MaaS systems should grant all MSPs the opportunity to maintain their customer interfaces and compete in the mobility market (Calderón and Miller 2019; Lamberti et al. 2019; Mattsson and Jenelius 2015). Therefore, as part of a potential solution, practitioners recommend addressing this problem through *disintermediation* (R2) (5 experts). Further, a solution needs to provide *openness* (R3), independent of market power and governance hierarchies, to onboard all potential MSPs as participants of the seamless mobility platform without facing substantial barriers to entry and business-related disadvantages. This includes the opportunity to seamlessly integrate services by different MSPs and to offer their entire service portfolio (Arias-Molinares and Garcia-Palomares 2020; Kamargianni et al. 2016; Paiva et al. 2021) (7 experts). The foundations of such an open system, which also involves a mechanism for the fair distribution of revenues from an aggregate service offer, are trust and the commitment to cooperate among MSPs (Polydoropoulou et al. 2020b).

4.2 Design Objective 2 – Data Protection

Previous studies have illustrated that the implementation of efficient MaaS platforms requires real-time data sharing among various MSPs to ensure seamless mobility services for travelers (Surakka et al. 2018). This implies preventing the unintended disclosure and misuse of sensitive business data as well as travelers' and service providers' personal data (R4): MSPs typically use data, such as their customers' identity information, payment histories, transaction references, movement profiles, or habits, to improve their service offerings and gain a competitive advantage (3 experts). Thus, MSPs naturally hesitate to share these data with competitors. Further, they are strictly bound to regulations, such as antitrust laws or the GDPR. These regulations restrict the extent to which MSPs can share business-related and customer-related information with third parties in the absence of explicit need and consent, respectively (Surakka et al. 2018; Paiva et al. 2021) (12 experts). Customers also expect that their personal data will not be shared, particularly to *prevent user tracking* (R5). In this sense, appropriate data management is necessary to ensure confidentiality and reduce privacy concerns (Cottrill 2020) (11 experts). Since MaaS solutions aim to compose multiple services provided by different MSPs while offering a consistent user experience, sharing required data while safeguarding data protection becomes even more challenging (Expert 16). A solution must also assign well-defined responsibilities and provide clear terms and conditions on how to process sensitive data. This is especially important for ticket issuance and verification as well as clearing and payment processes within a traveling route with multiple sub-routes (Polydoropoulou et al. 2020b; Stockburger et al. 2021).

4.3 Design Objective 3 – Manageability

From a management perspective, the experts stated that a seamless MaaS solution should incorporate *modularity (R6)* (12 experts). A modular solution involves open and decentralized design concepts, enabling each MSP to offer its mobility services through potentially proprietary yet standardized, interoperable, and accessible interfaces. Modularity and decentralization can facilitate a shared market structure without intermediaries (R2), creating more robust markets than centralized solutions (Bothos et al. 2019; Lamberti et al. 2019; Nguyen et al. 2019). In this context, Expert 4 emphasizes that *"the challenge of offering a multimodal and cluster-overlapping mobility platform often fails due to the centrally organized service providers' different interests."* Ultimately, standardized customer interfaces, for instance, MSPs' booking applications, are required to prevent the unnecessary development

of isolated stand-alone solutions by individual MSPs and to create an interoperable solution (12 experts). These stand-alone modular solutions must support a high number of customer transactions, a characteristic of the mobility market. Thus, a MaaS solution must provide high *process efficiency (R7)* and consider the aspect of scalability (4 experts) (Sümmermann et al. 2017).

4.4 Design Objective 4 – End-User Experience

To improve travelers' user experience, MaaS solutions should enable *seamless data sharing (R8)* for customers' identity attributes (Paiva et al. 2021). According to eight experts, one way to achieve seamless data sharing is data portability which enables a "single sign-on" user experience by avoiding tedious registrations with each service. Travelers' preferences could also be shared bilaterally with different applications, further avoiding vendor lock-in effects from a customer perspective. The current various implementations of mobility services also lead to many challenges concerning cross-system data handling, such as fare management (Lamberti et al. 2019). These challenges require a suitable solution to increase the overall accessibility and transparency for customers (Stockburger et al. 2021) (7 experts). In this context, interoperability and a solution that considers various customer preferences can help address the challenge of application fatigue – the observation that customers are negatively affected by an oversupply of applications (Harper 2020), such as individual MSPs' mobile apps or web interfaces. An overall solution must also be *efficient* and quick to use (R7), be open to being rebuilt by each MSP, and reflect the various preferences of different customer segments (Paiva et al. 2021). Ultimately, an interoperable solution that considers a wide variety of customer preferences and a large set of MSPs faces the problem that in the event of an issue with a specific mobility service, travelers must also know exactly whom to contact (Giesecke et al. 2016). When an itinerary involves multiple MSPs' services, this may lead to inconsistencies of responsibility and liability. Thus, it is important that the MaaS solution clearly defines MSPs' responsibilities concerning *customer support (R9)* and makes them transparent to users.

5 Seamless MaaS Architecture Based on Digital Wallets

Informed by the identified design objectives and corresponding requirements, we developed a conceptual IT architecture for seamless MaaS. In doing so, we incorporated a physical view as well as a process view of our IT architecture (Kruchten 1995).

5.1 Components and Roles

Fundamentally, our architecture employs digital wallets to allow for data portability and in particular the convenient and secure exchange of information between travelers and MSPs (R5). As Fig. 2 illustrates, our architecture covers the three central entities of any SSI solution: MSPs that provide mobility services and act as issuers of travel tickets, travelers who use mobility services (and accordingly receive and present corresponding travel tickets), and travel inspectors acting as ticket verifiers. To facilitate the seamless planning and booking of mobility services for travelers, our architecture comprises an additional entity – the routing service. This service serves as a coordination instance that retrieves mobility service offerings from different MSPs and presents them to travelers. Specifically, the routing service constitutes a complementary modular extension of MSP's booking interfaces that provides travelers with information on external service offerings (retrieved via open APIs) (R3) without exposing sensitive personal or business data (R4, R5). However, it can also be run as a standalone component for providers that do not offer mobility services themselves. Any MSP can integrate this modular extension (e.g., a municipal authority for transportation, or an international airline) (R2). Thus, our architecture seeks to facilitate coopetition by allowing for the coexistence of proprietary routing services that can be adapted to specific business needs (R1, R6). We built a modular architecture design that empowers MSPs to create proprietary and individual routing services while respecting potentially heterogeneous business needs (R2, R6). Our architecture also incorporates a public data registry that facilitates the efficient verifiability of issued travel tickets (R4, R5). This registry only handles non-sensitive information and, therefore, can be hosted either in a centralized way by a trusted third party or in a decentralized way by multiple MSPs, for instance, on a public blockchain. For communication between these entities, we suggest REST-APIs secured via Hyper Transfer Protocol Secure (HTTPS) for business-to-business (B2B) interactions – in our case, between the MSPs and the routing service. On the other hand, the DIDComm Messaging (DIDComm) specification provides the technical basis for the exchange of personal information between travelers and MSPs. DIDComm has evolved into a common communication standard in many existing digital wallet applications (Sartor et al. 2022). For exchanging travel tickets and other personal information, the architecture relies on the VC and VP specifications.

5.1.1 Travelers

Travelers are at the center of our proposed MaaS architecture. They make use of mobility services, actively

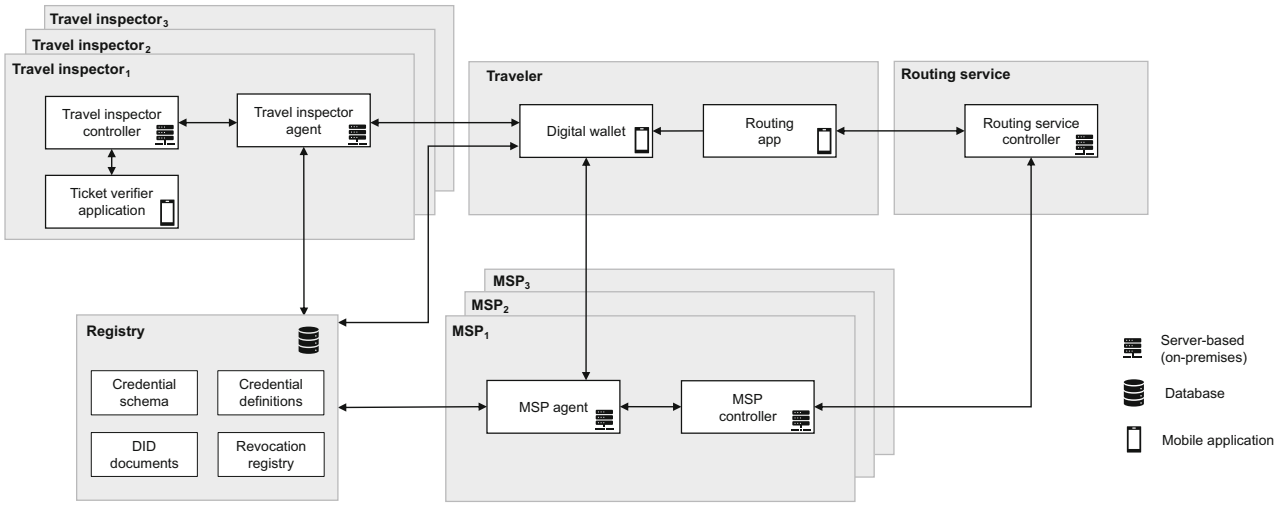

Fig. 2 Architecture and components for MaaS based on digital wallets

deciding which MSPs they want to engage with. In our design, travelers first access a routing app to select the parts of the itinerary that are required to initiate the corresponding booking processes. Second, we assume that travelers have access to a digital wallet that allows them to seamlessly and selectively share machine-verifiable identity information with each MSP (R8) and also to prove their ownership of valid tickets to travel inspectors.

5.1.2 Routing Service

The routing service component serves as a coordination instance. The corresponding routing service controller collects and stores specific information about each available service offering, such as departure time, location, and destination. Based on the traveler's indicated itinerary plan and preferred selection criteria, the routing service suggests suitable combinations of mobility services for the requested itinerary. Once a traveler has selected their preferred route, the routing service controller dismembers the entire itinerary into individual sub-queries and forwards it to the corresponding MSPs to trigger the individual ticket purchase processes.

5.1.3 Mobility Service Providers

MSPs provide mobility services and issue tickets for the corresponding mobility service. To do so, MSPs require two core technical components. The MSP controller acts as the core component for executing MSPs' business logic. That is, the MSP controller receives all service-related information required for a booking – such as departure time, location, and destination – stores selected personal information of travelers, and coordinates the data flow and storage during the ticket purchase and issuance process. Travelers provide their personal data according to their preferences when they initiate the booking process. To this end, the MSP controller instructs the MSP cloud agent to handle the communication between the traveler's digital wallet and the MSP, i.e., to receive and verify travelers' identity information and to issue travel tickets to travelers' digital wallets during the booking process. In doing so, the MSP cloud agent also connects to the corresponding public registry to write or read selected issuer- and revocation-related information. The MSP cloud agent hence serves as an ancillary microservice accessible to the MSP controller for handling the communication with travelers' digital wallets and corresponding cryptographic operations.

5.1.4 Travel Inspector

The travel inspector component verifies the issued travel tickets' validity and consists of three sub-components: the ticket verifier application (front-end), the travel inspector controller, and the travel inspector agent. The ticket verifier application runs on a travel inspector's portable device and displays a QR code that represents a dynamic link. Travelers need to scan this link with their mobile phone to initiate the ticket verification process. As for the MSP, the travel inspector controller represents the core component that executes and orchestrates the ticket verification process. The travel inspector agent microservice interacts with the traveler's digital wallet and retrieves some information stored on the public registry to check whether a ticket is authentic and whether it has been invalidated (revoked), for instance, in the case of a cancellation. For some services where no travel inspector is present, such as car sharing, a static QR code representing the URL of the corresponding MSPs's controller can be attached to the vehicle to initiate the verification process.

5.1.5 Registry

Trust registries – be it in the form of a centralized database or based on a blockchain – are a pivotal component of our architecture to validate VPs. In more detail, to assess the authenticity of VCs, verifiers need to maintain or require access to a list of trusted issuers. These lists include relevant issuer metadata, such as DIDs and their respective public keys, that enable verifiers to associate a digital signature with the corresponding issuing organization. The information provided by trusted registries is not only beneficial for verifiers but also prevents holders from machine-in-the-middle-attacks and sharing their personal information with malicious actors (Babel and Sedlmeir 2023). To this end, digital wallets can connect to the registry to identify the verifier based on its public key before a secure connection is established and any personal data is shared. Furthermore, issuers may also rely on trust registries to publish cryptographic accumulators that allow to verify a VC's revocation state in a privacy-preserving way (Feulner et al. 2022). As developing a proprietary list of potentially hundreds or thousands of trusted organizations can be a complex task for credential verifiers and holders, such trust registries are particularly useful when they are provided by an established private or public entity (e.g., a certificate authority or regulator). A shared trusted registry may also help to facilitate the semantic interpretation and standardization of credentials by providing a public list of industry standards for VC schemata.

5.2 Travel Ticket Booking and Verification Process

The MaaS booking process (Fig. 3) starts with the traveler requesting a mobility service by accessing the routing app. The routing app forwards the travel information provided within the request to the routing service controller, which uses the routing search algorithm to identify the optimal composition of individual MSPs' mobility service offerings. At this stage, the information provided by the traveler comprises only less sensitive information related to the travel itinerary – such as the desired departure time, departure location, destination, price- and comfort preferences, or potentially self-attested (not yet verifiable) discount eligibilities. This practice helps to protect travelers' privacy and to avoid comprehensive tracking (R5) through the routing service provider. Based on the obtained preferences, the routing service controller utilizes the routing algorithm to identify a selection of suitable MSPs and the corresponding specific subroutes of the itinerary. Thus, an itinerary can consist of many different subroutes offered by different public or private MSPs (e.g. train or air mobility services), or different qualities (from standard to premium mobility service offerings). When travelers confirm their intention to book a specific composed itinerary, the routing service controller dismembers the requested itinerary into the separate subroutes. For each subroute, it creates and forwards to the routing app a specific link, for instance, a public DID that resolves to more detailed contact information for an MSP on the public registry, or the URL of that MSP's service endpoint directly. Each link also includes the corresponding travel information (e.g., as URL parameters) of the requested itinerary. For instance, if an itinerary consists of two subroutes – MSP_1 for subroute 1 and MSP_2 for subroute 2 – only MSP_1 receives the required information associated with subroute 1, and only MSP_2 receives the required information for subroute 2. Thus, the routing service follows the principle of disintermediation by instructing the traveler's routing app to connect and introduce themselves to MSPs (R2). By following the link, the routing app requests the corresponding mobility service. The MSP controller receives the request containing the provided information and instantiates a new booking process by persisting the parameters of the subroute as indicated by the routing service's request and mapping it to a unique booking ID. The MSP controller instructs the MSP cloud agent to generate a new connection invitation and synchronously returns a deeplink to the routing application. Subsequently, the connection invitation is directly accessed within the traveler's digital wallet, enabling the wallet to authenticate the MSP's identity and ascertain its trustworthiness via the trust registry, which is then presented to the traveler for perusal. Travelers possess the discretion to accept this connection invitation within their digital wallet, facilitating the establishment of a secure, encrypted bilateral linkage with an MSP. In the future, these connections might also serve as a direct portal for customer assistance (R9).

The process continues with the verification of the traveler's personal information to transition to the ticket issuance process. Once the traveler and the corresponding MSP are successfully connected, the MSP cloud agent sends a corresponding notification to the MSP controller via a webhook that references the booking ID. Based on the booking information that the MSP controller has stored under this booking ID, the MSP controller creates a proof request that corresponds to the requested mobility service and triggers the MSP cloud agent to send it to the traveler's digital wallet. The proof request is a standardized, partially cryptographic, representation of the verifiable personal information required that the MSP needs from the user for the booking process. The agent knows how to communicate with the digital wallet based on the contact information associated with the booking ID that was used to establish the initial connection. Technically, this exchange of DIDComm messages between the cloud agent and the wallet involves a mediation agent (as presented in Sect. 2).

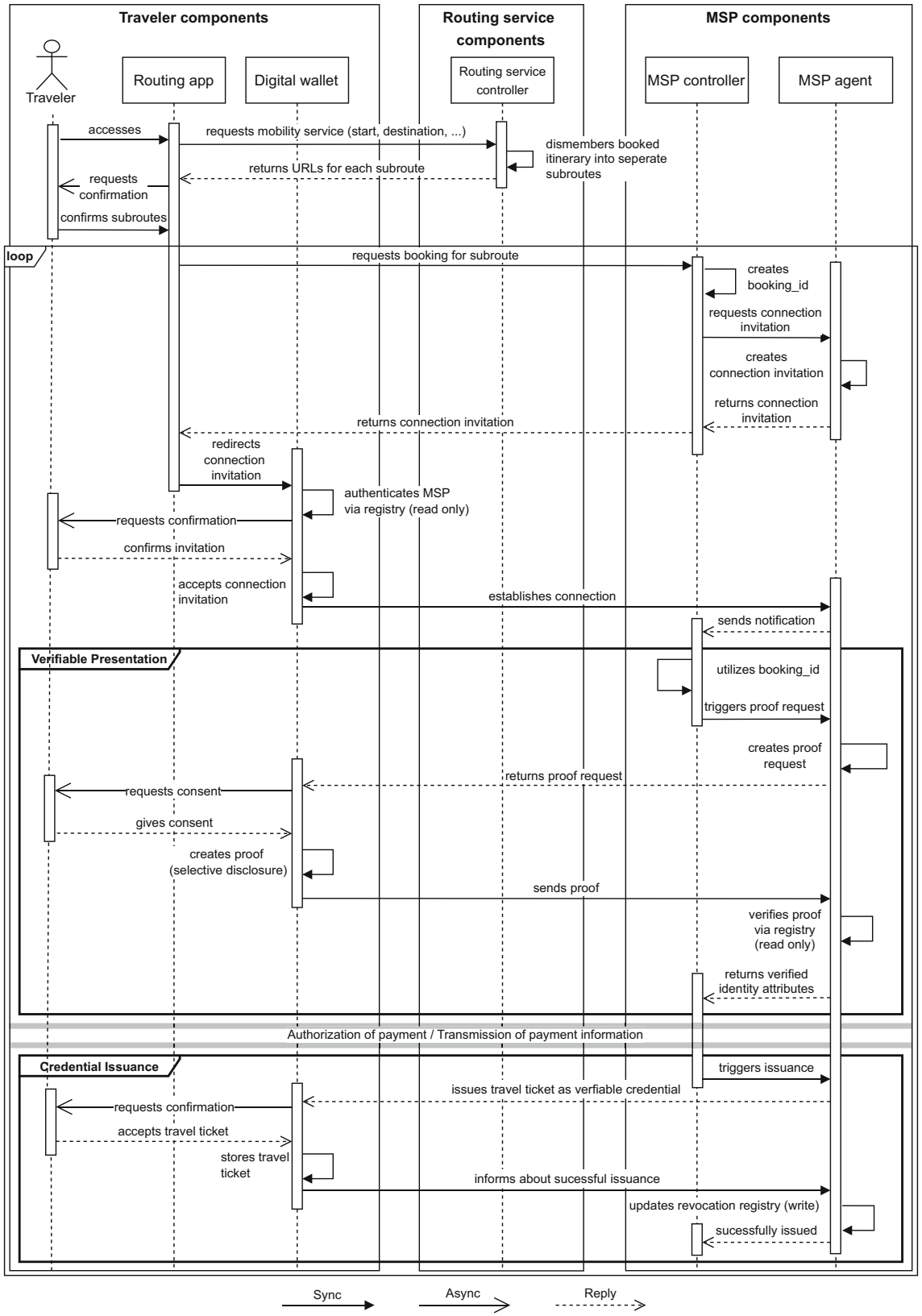

Fig. 3 Seamless MaaS travel ticket issuance based on digital wallets

By giving consent to the disclosure of the requested identity attributes and creating a VP based on the VCs available in their digital wallet, travelers provide this information to the MSP cloud agent. The digital wallet gives travelers a high degree of control over the presented information (selective disclosure) (R5). For instance, MSP_1 could be a car-sharing service provider that requires a valid driver's license and the traveler's full name. The traveler can then selectively disclose the attributes that state the full name and the vehicle class for which they have the authorization to drive from their digital driving license. Also, VCs that make a traveler eligible for a discount (they may have been indicated through the booking request already, but not necessarily) can be requested. In doing so, ZKPs (e.g., a proof of possession of a non-expired and non-revoked driver's license) avoid the disclosure of any information beyond what is requested, for instance, the driver's license's serial number or other unique cryptographic identifiers (Babel and Sedlmeir 2023) (R4, R5). By default, the traveler's digital wallet can even use a new cryptographic key pair in each interaction and nonetheless prove control over the key pairs to which its VCs are bound (Schlatt et al. 2022). Further, depending on the payment method, MSPs may also request relevant payment information, such as a credit card number and its security code. Once the traveler has presented all the required information, the MSP issues the corresponding travel ticket and sends it to the traveler's digital wallet, which stores the VC for future use. After completing the booking process for subroute 1, the traveler carries out the same process for subroute 2 analogously and bilaterally with MSP_2. After that, the traveler is prepared to start their itinerary.

A key feature of the SSI-based booking process is the machine-verifiability of travel tickets. Once a traveler starts their itinerary, the service providers' or third parties' travel inspectors may check the issued travel tickets' validity, in a process similar to the VP illustrated in Fig. 3. To initiate the procedure, the traveler utilizes a QR code furnished by the travel inspector and proceeds to access the corresponding HTTPS link. The travel inspector controller then transmits the request to the travel inspector agent, which expeditiously creates a proof request accompanied by a deep link. As in the case of the MSP's connection invitation above, this deep link is recognized by the traveler's edge device, which opens the traveler's digital wallet to process it. After verifying the identity of the verifying organization (e.g., the travel inspector's employer that runs the corresponding cloud agent and controller) the traveler sends a cryptographic proof of ticket ownership to the travel inspector agent. The travel inspector agent verifies the ticket's cryptographic validity, i.e., whether it was digitally signed by the corresponding MSP, and that it has not been revoked, using additional information stored in the public revocation registry. The travel inspector agent verifies the proof and reports the result of the verification and the disclosed personal and ticket information to the travel inspector's controller. The controller compares the presented content of the ticket to the inspector's location (start and destination), time (validity date), as well as potentially other properties of the trip, and reports the result to the inspector's front-end via a webhook. If the ticket is valid, the traveler can continue their itinerary; otherwise, common measures for unauthorized travel will be applied. For services that do not rely on travel inspectors, a static QR code can be attached at the gate of the mobility service or at the vehicle itself.

6 Evaluation of the Artifact

Throughout our design and development process, we iteratively evaluated our artifact's fitness to meet the identified design objectives and requirements. In doing so, we applied a qualitative evaluation based on expert interviews (Sonnenberg and vom Brocke 2012; Venable et al. 2016). In these interviews, we demonstrated our architecture by presenting an expository instantiation (Sonnenberg and vom Brocke 2012) for mobility service ticket booking and verification (Fig. 4). We discussed our architecture and the prototype (*"Routenplaner+"*) with the experts to identify its strengths and weaknesses. Our prototypical routing application was instantiated as a web-based application. Consequently, in contrast to the process flow outlined in the previous section, an automated redirection of the deep link could not be implemented for establishing a connection between the MSP agent and the digital wallet. The prototype required user intervention by scanning a QR code with the digital wallet (when accessing the routing web-app and digital wallet through different devices) or clicking the URL in a browser for an HTTPS redirect (when accessing the routing web-app and digital wallet through a mobile phone). Based on the experts' feedback, we redefined our IT architecture in iterative build-and-evaluate loops (Hevner et al. 2004) and performed a qualitative criteria-based evaluation of our MaaS architecture.

6.1 Evaluation – Neutrality

The experts appreciated the architecture's design as they considered it a more neutral solution than prevailing centralized MaaS systems. According to Expert 20, the architecture considers the coopetition required for a successful MaaS ecosystem (R1). This can be achieved mainly through the opportunity for MSPs to implement a

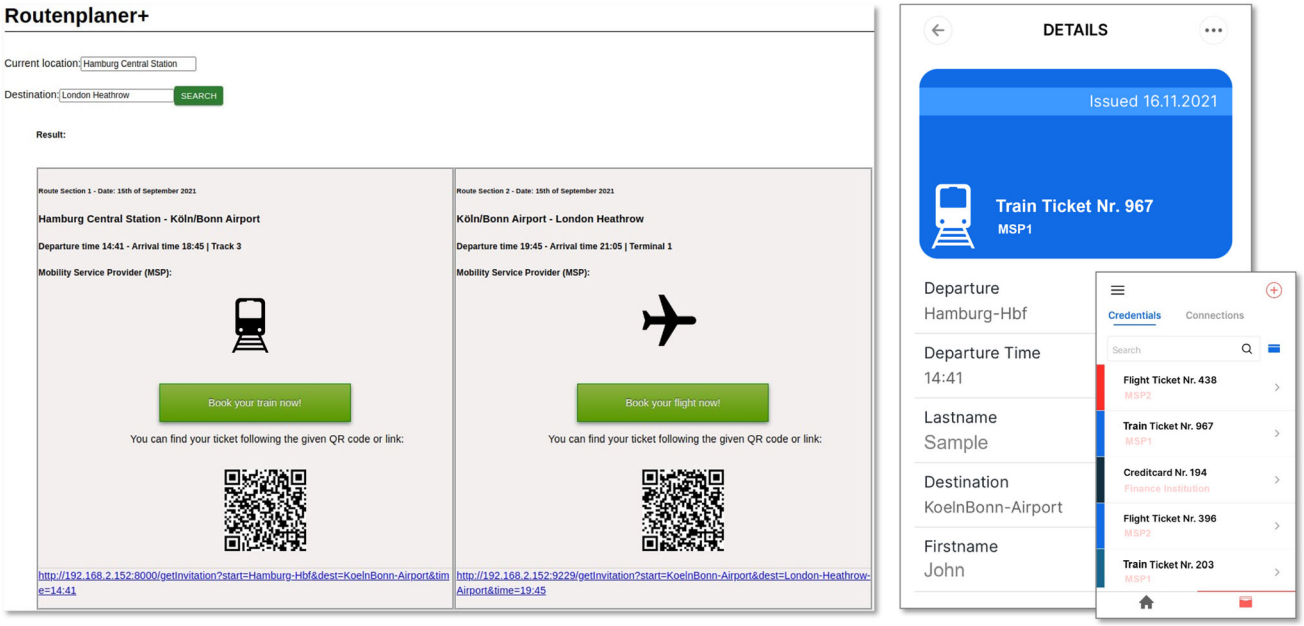

Fig. 4 Travel planning interface (left) and digital wallet (right) in our prototype *"Routenplaner+"*

proprietary routing service by themselves. In particular, our architecture supports the implementation of many coexisting routing services. In this context, Expert 24 raised concerns that the routing service still functions as some kind of service aggregator, resulting in a certain degree of centralization that ultimately may evoke a "*monopolist*". However, according to Experts 20, 21, and 23, this is a viable approach to enable fair competition, as each MSP can be a *"routing service and then just the best one prevails on the market"* (Expert 21). Further, Expert 22 believes that it *"is the only sensible solution and also the fastest solution that the market then simply decides which one, which routing service is considered the best, because the user journey is good."* To participate in fair competition and stand out from their competitors, MSPs can modify their routing service according to various customer preferences; for instance, by providing special service offerings or establishing customer loyalty programs. Simultaneously, the co-existence of routing services overcomes the MSPs' fear of losing a dominant position to a competitor. Expert 19 appreciated our architecture's decentralized design, as MaaS systems do not need a single intermediary operating a central *"routing service, but many different ones"* to avoid concentration of market power (R2).

The SSI-based MaaS solution must enable the functionality that all MSPs can seamlessly interact with one another. In this sense, open and standardized interfaces (APIs) (R3) are pivotal to allow MSPs to cooperate in the form of integrating other MSPs' services within their routing services and to provide an easily accessible onboarding process for MSPs (Experts 22, 23). Expert 23 also perceived the use of open APIs as an enabler for new players to enter the MaaS market *"that could not carry the effort to implement a routing services by themselves, so far. [...] And this will foster competition."* Although there is currently no universally adopted standard for developing open APIs, substantial efforts have been made in recent years to facilitate the sharing of mobility service offerings. For instance, the EU's delegated regulation 2017/1926 related to the provisioning of EU-wide multi-modal travel information services recommends the integration of an "open API for distributed journey planning" which may support a routing service to retrieve mobility service information from various MSPs (European Commission 2017). The European Committee for Standardization has defined a corresponding standard under the reference CEN/TS 17118:2017. In the aviation industry, many airlines have already deployed open APIs to increase their revenue. To make use of the benefits of these open APIs across the aviation industry and promote standardization, the International Air Transport Association (IATA) recently established an open API hub (IATA 2023). These efforts may serve as a promising foundation to implement a routing service as proposed in this work.

6.2 Evaluation – Data Protection

To augment coopetition, our architectural framework follows and extends the proposal by Hoffmann et al. (2021) to provide seamless and verifiable interactions between mobility users and MSPs without shifting market power

and access to mobility users to intermediaries. According to Expert 19, in the MaaS area there is a particularly strong need for information exchange *"which ensures that transactions are executed correctly and also takes privacy into account, so that no more information is transported for a particular transaction than necessary."* In other words, the confidentiality of sensitive business and personal data must be ensured by avoiding their disclosure to third parties and in particular to competitors (Expert 22). Our routing service operates according to this "need-to-know" principle: It does not require the disclosure of any personally identifiable information, such as a traveler's name or date of birth, to the routing service. The routing service also does not learn whether the traveler has in fact booked a suggested itinerary completely or in parts. Instead, only the MSPs in question receives the information needed to issue tickets associated with the subroutes assigned to them. This approach facilitates cooperation while protecting each stakeholder's sensitive data from disclosure to third parties. Expert 23 appreciated this approach, as it allows customers to *"identify their most suitable mobility offerings and then they have to authenticate in a privacy-preserving way."* Our architecture implements this need-to-know principle by design through bilateral and selective information exchange between travelers and MSPs. Furthermore, we consider secure communication protocols and bilateral data-sharing using interoperable formats for the exchange of verifiable information between MSPs' digital agents and travelers' digital wallets (R4) in the ticketing process (Feulner et al. 2022). According to Expert 23, such decentralized digital identity management enables *"different opportunities to dissolve data silos than a centralized platform could ever offer so far."* Regarding the exchange of personal data, Expert 22 sees the need *"on the one hand, to make the user journey as simple as possible and, at the same time, to ensure personal data protection."* Our architecture facilitates this by building on an open, decentralized identity management solution using digital wallets and a routing service to coordinate these processes. This solution also has the capacity to further minimize the disclosure of personal data (R5) with advanced cryptographic solutions, namely ZKPs.

6.3 Evaluation – Manageability

From a business perspective, our architecture based on digital wallets levers its openness and clear separation of responsibilities and data access to address corresponding issues of centralized alternatives. Expert 21 sees an essential aspect in the support for multiple routing services, as they enable a diverse portfolio of mobility service offerings. Besides, diverse routing services not only enable an open market (R3) but also ensure distributed and decentralized market structures without dependencies on a single intermediary (R2). The coexistence of multiple routing services may also increase the resilience of the entire MaaS market (Expert 21). In this context, Expert 22 highlighted that *"MSPs should host proprietary routing algorithms that favor their own service offerings and complement them with third-party services if necessary."* Modular and dedicated applications for travel planning are used solely to determine the best offer for the traveler (without the need to share sensitive data), while the ticketing process utilizes bilateral MSPs-traveler communication to ensure the separate handling of the exchange of sensitive business and personal data. These bilateral interactions avoid a single point of failure, avoid performance bottlenecks (in contrast to blockchain technology), and provide process efficiency through end-to-end machine-verifiability.

Consequently, our proposed architecture also does not require any complex B2B contracts that regulate the processing of sensitive and personal data between MSPs. Instead, it only requires coordination at the (B2C) level. This setup enables the more efficient and automated processing of travel bookings (R6). According to Expert 22, the seamless exchange of information without inconsistencies in processing personal data through a single digital wallet enables MSPs to substantially simplify the user journey and to operate much more efficiently (R7). Expert 22 also sees an independent high potential of introducing digital wallets and SSI without the need to change existing processes. In this regard, Expert 22 believes "*that there is much value already easily possible through SSI.*" Likewise, Expert 23 emphasized that *"the question is no longer whether, but only when"* digital wallets will be widely adopted for onboarding processes.

6.4 Evaluation – End-User Experience

Our architecture sought to facilitate booking processes that are as seamless as possible for travelers while avoiding the centralized coordination of MSPs' services that involve the aggregation of personal information. Our solution achieves this through leveraging digital wallets for a seamless booking process, particularly, efficient and targeted data-sharing through VCs (R8). In this context, travelers have the opportunity to use their identity-related VCs (such as a government-issued ID card, a driver's license, or a credit card for payment) and present their required identity attributes to MSPs within the ticketing process. Expert 19, therefore, sees considerable potential to improve MaaS-related processes by integrating digital identities: *"If we would have an identity and could then simply link them, this would already be a major intermediate step. So even in the current status quo, where we have many different*

mobility service providers [...] there, for example, barriers to access could be significantly reduced." This portability of identities not only lowers barriers for travelers who want to use MSPs' offerings, it also *"prevents the risk of vendor lock-in"* (Expert 23) of customers. In our architecture, Expert 20 appreciates the usage of digital wallets as an *"interoperability layer"* that allows travelers to use a booking process that interacts with various MSPs within a single, non-proprietary application. However, in the context of seamless data exchange, MSPs must ensure that travelers at all times know which MSP they can contact in the case of problems with the booking process or the mobility service itself. According to Expert 19, our solution addresses this requirement by providing the technical basis for bilateral communication channels between travelers and MSPs that could also be used for customer support. The connection between the travelers' digital wallets and MSPs' cloud agents ensures that travelers at all times know which MSP is responsible for what section of the route (R9). However, while bilateral communication channels can be advantageous for addressing issues with individual services, they may not always be the most convenient option for travelers, especially in cases where problems affect multiple subroutes. For instance, if there are significant delays or disruptions that impact several subroutes of a traveler's itinerary, travelers will also have to consult with multiple different customer support services. In such cases, our solution may not be able to deliver the same user experience as approaches that provide centralized customer support.

7 Discussion and Design Principles

Our research's core contribution is an IT architecture for seamless MaaS. In contrast to related work that emphasizes either centralized (Arias-Molinares and Garcia-Palomares 2020; Smith et al. 2018) or decentralized, mostly blockchain-based (Hoffmann et al. 2021; Lamberti et al. 2019; Nguyen et al. 2019) designs for MaaS, our findings suggest that centralization and decentralization are equally important to reflect coopetitive needs in the design of MaaS solutions. Specifically, in line with Arias-Molinares and Garcia-Palomares (2020), Smith et al. (2018), we find that travel planning processes may benefit from centralized designs, as they facilitate the combination of service offerings among MSPs and itinerary planning for travelers. Simultaneously, our findings indicate that the decentralization of ticket booking, and verification processes is essential to ensure more user control of the disclosure of sensitive identity information and to avoid the aggregation of such data by an intermediary, preventing a loss of competitive advantage for individual MSPs. In line with the proposed design by Hoffmann et al. (2021), our architecture establishes such decentralization through digital wallets and implements the exchange of sensitive information in bilateral traveler to MSP interactions. However, in contrast, our solution abstains from the publication of travelers' DIDs on a blockchain to guarantee a higher degree of privacy. Furthermore, our solution considers more traditional centralized approaches in combination with open APIs for the implementation of routing applications. This way, our solution reduces entry barriers by avoiding the need for registration authorities that maintain registries for MSPs. What is more, it thereby also eliminates issues related to governance and scalability of implementing routing algorithms through smart contracts.

We now translate the design knowledge generated through our research into three DPs (Gregor and Hevner 2013; vom Brocke et al. 2020). From a theoretical perspective, these DPs aim to provide a nuanced understanding of the roles and implications of centralized and decentralized IS designs in coopetitive service markets. These DPs can also guide practical implementations of seamless MaaS and help balance coopetition between MSPs. We hypothesize that practitioners can also apply these generalizable DPs to similar B2C market scenarios that need to process end users' personal data and at the same time require coopetition between businesses.

7.1 DP1 – Separate Coordination and the Exchange of General Service Information from the Exchange of Personal or Sensitive Business Data

Our research has illustrated that prevailing seamless MaaS approaches do not adequately solve the challenges of the ticketing process owing to the ambivalent role of data and the resulting complex requirements for data processing. While centralized solutions tend to overemphasize competitive needs and demand MSPs to devolve control over strategic data, decentralized, blockchain-based solutions often put too much focus on cooperation and symmetric data access and thereby eliminate opportunities for competition and data protection. In other words, neither fully centralized nor fully decentralized solutions provide sufficient means for fostering coopetition among MSPs. Thus, in line with prior research on coopetition, our design proposes an alternative approach, i.e., the bilateral sharing of sensitive data. In more detail, our design suggests separating the processing of non-sensitive data required for general service offerings from the processing of highly sensitive business and personal data that may constitute a competitive advantage (Gast et al. 2019). In particular, we suggest separating identity management and booking from processes that coordinate entities' service offers.

7.2 DP2 – Coordinate General Service Information Through Multiple Competing Service Aggregator Applications

A sensible degree of (de)centralization is essential for a routing application that aggregates mobility services offerings. In particular, MSPs aim to retain competitive advantages from processing the users' preferences indicated in the routing planner as well as advertising and bundling mobility services within proprietary routing applications (Experts 20, 21, 22). As a result, seamless MaaS solutions need to enable every MSP to provide a routing service as an extension on top of its existing customer interfaces to offer customized services that also foster innovation on the side of the routing service (Willing et al. 2017). This approach has the potential to mitigate interdependencies within the MaaS market while still providing the opportunity to gain a competitive edge over other MSPs (Experts 19, 23).

Further, seamless MaaS solutions should employ open standards for APIs to integrate service offerings within routing applications. MSPs also need incentives for providing this data and enforcing non-discrimination. The open availability of service offerings in a cooperative environment provides MSPs incentives in the form of simplified multi-homing in routing planning applications and the resulting enlarged customer base. Such open-standard APIs also reduce the risks of centralization by lowering entry barriers and reducing lock-in effects (Bakos and Halaburda 2020). Nonetheless, these standardized APIs must consider all offerings of the various MSPs, which may lead to increased complexity in governing the entire MaaS ecosystem. Thus, in practice, one needs to limit complexity so that the overall system can be implemented by all MSPs (Expert 24).

7.3 DP3 – Use Digital Wallets for the Secure and Efficient Exchange of Verifiable Personal Data

Our architecture was built on the assumption that competitors should not be dependent on one another within the scope of their service distribution. Current studies advocate the use of blockchain as a means for fair competition and interoperable cooperation (Hoffmann et al. 2021; Lamberti et al. 2019; Nguyen et al. 2019; Stockburger et al. 2021). Our results suggest that this is not necessarily practical when taking coordination and in particular the protection of sensitive data into account. The replicated processing of booking-related data on a blockchain leads to excessive transparency. On the other hand, when personal data is obfuscated on-chain, some additional data must be passed to MSPs during travel booking via another communication channel in blockchain-based approaches, and smart contracts also cannot process data that is not available on-chain (Sedlmeir et al. 2022b). We suggest addressing these problems by making sensitive personal data portable while maintaining verifiability and ease of data sharing and by giving control over its disclosure to the user. Sensitive data should be only shared in bilateral interactions between the traveler and related MSPs. Bilateral connections between MSPs and travelers enhance users' control over data disclosure since only the corresponding MSP receives and processes the sensitive user data required for the respective ticketing process. To implement such data-sharing capabilities without compromising user experience, one should rely on a single app. This single app is represented by the digital wallet, which enables self-determined administration of identity documents and eliminates the need for a separate account for every service provider (Expert 23). Further, digital wallets provide high levels of assurance about users' identity through hardware-binding or credential-linking while at the same time reducing the amount of sensitive information disclosed (Schlatt et al. 2022; Feulner et al. 2022). Such a decentralized approach based on digital wallets serves as a cross-organizational interoperability layer. For instance, credentials such as a personal ID card or driver's license can also be used and stored within the digital wallet for the verification of required booking-specific data, such as selectively choosing claims such as first name, last name, or the driver's license when booking car-sharing services.

Fundamental to any new solution, such as our derived architecture, is the organizations' willingness to adopt such a system and the related business models that may enable them to do so. Thus, we conclude our discussion by elaborating on prospective business models that may underlie and drive the adoption of our solution, in particular, the routing service. One key stakeholder group for the funding and operation of routing services is the public sector. National or local governments or municipalities could financially support routing services or operate their own routing service as part of their national or local transportation infrastructures and citizen services (Hoffmann et al. 2021). They may be particularly motivated to do so to facilitate the use of public transportation and thereby encourage more sustainable mobility behavior. However, our approach based on routing services does not aim to close the doors to the private sector. Different business models may promote privately operated routing services. For instance, dedicated routing service providers may offer additional services, such as travel insurance or advanced customer support. Moreover, routing service providers could generate revenues through the integration of sponsored advertising of certain mobility services. Operating their own routing service might also help to increase MSPs' own revenues, as offering a larger service portfolio

– albeit including services from competing providers – would allow them to increase the attractiveness of their own services (Ritala 2022). Yet, further research is required to investigate the viability of these or other business models and to assess whether they will be able to resolve prevailing issues of MaaS.

8 Conclusion

Using a DSR approach, this research developed a novel IT architecture for MaaS based on digital wallets. Our research also contributes design principles located at the nexus of centralized and decentralized designs. Thus, our research opens the discussion on the role of hybrid architectures, including both centralized and decentralized components, for coopetitive service markets. We hypothesize that practitioners and researchers could apply these generalizable DPs to similar B2C market scenarios that feature coopetition between service providers and require the processing of sensitive data.

Our research is not without limitations. First, our research applied a qualitative criteria-based evaluation with expert interviews and does not yet comprise a holistic, real-world deployment of our proposed architecture. Future work could focus on a more elaborated real-world instantiation so as to identify additional requirements for the practical diffusion of our architecture within the MaaS sector. For instance, our proposed architecture advocates using open and standardized customer interfaces (APIs). However, the architecture does not yet specify data models to exchange ticketing information that often includes complex pricing schemes.

Second, our research is focused on the design of an IT architecture for MaaS. Our research does not cover the design of routing algorithms that are essential to identify suitable itineraries. Further research may address this gap by investigating requirements and the design of complex routing algorithms that optimize the combination of mobility services based on different objectives, such as user preferences (e.g., cost and time) or environmental impact.

Third, our proposed architecture assumes bilateral relationships between travelers and MSPs. Such bilateral interactions may not always be sufficient to ensure a seamless user experience. In particular, when travel plans change or massive delays occur that affect multiple subroutes, travelers would have to bilaterally approach each MSP's customer support. However, what may be a limitation of our technical design could also be a business opportunity. In this sense, future research may investigate potential business models and complementary services, such as extended customer support coordinated by the routing service, to ensure a seamless user experience.

Finally, our research suggests a solution at the nexus between centralized and decentralized designs. It is unclear whether such a market design will evolve toward a more centralized or a more decentralized direction in the long run. Thus, further quantitative research may assess such MaaS market structure's evolution to also identify additional features that must be met to ensure long-term balanced coopetition. Our DPs could point the way towards a broadly applicable design theory for coopetitive service systems and shed light on the capabilities of digital wallets in these settings.

Acknowledgements This research was funded in part by the Bavarian Ministry of Economic Affairs, Regional Development and Energy through the project "Fraunhofer Blockchain Center (20-3066-2-6-14)"; Luxembourg's Ministry for Digitalisation; the Luxembourg National Research Fund (FNR) through the PABLO (grant reference 16326754) and FiReSpARX (grant reference 14783405) projects; and FNR and PayPal, PEARL grant reference 13342933/Gilbert Fridgen.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Anke J, Richter D (2023) Digitale Identitäten. HMD Prax Wirtschaftsinform 60:261–282

Arias-Molinares D, Garcia-Palomares JC (2020) The Ws of MaaS: understanding mobility as a service from a literature review. IATSS Res 44(3):253–263

Babel M, Sedlmeir J (2023) Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs. arXiv:org/abs/2301.00823. Accessed 19 Nov 2023

Bakos Y, Halaburda H (2020) Platform competition with multihoming on both sides: subsidize or not? Manag Sci 66(12):5599–5607

Barr S (2018) Personal mobility and climate change. WIREs Clim Change. https://doi.org/10.1002/wcc.542

Bothos E, Magoutas B, Arnaoutaki K, Mentzas G (2019) Leveraging blockchain for open mobility-as-a-service ecosystems. In: IEEE/WIC/ACM international conference on web intelligence—companion volume. ACM. https://doi.org/10.1145/3358695.3361844

Bouton S, Hannon E, Knupfer S, Ramkumar S (2017) The future(s) of mobility: how cities can benefit. McKinsey & Company. https://www.mckinsey.com/capabilities/sustainability/our-insights/the-futures-of-mobility-how-cities-can-benefit. Accessed 19 Nov 2023

Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M (2007) Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw 80(4):571–583

Butler L, Yigitcanlar T, Paz A (2021) Barriers and risks of mobility-as-a-service (MaaS) adoption in cities: a systematic review of the literature. Cities. https://doi.org/10.1016/j.cities.2020.103036

Calderón F, Miller EJ (2019) A literature review of mobility services: definitions, modelling state-of-the-art, and key considerations for a conceptual modelling framework. Transp Rev 40(3):312–332. https://doi.org/10.1080/01441647.2019.1704916

Casady CB (2020) Customer-led mobility: a research agenda for mobility-as-a-service (MaaS) enablement. Case Stud Transp Policy 8(4):1451–1457. https://doi.org/10.1016/j.cstp.2020.10.009

Constantinides P, Henfridsson O, Parker GG (2018) Introduction - platforms and infrastructures in the digital age. Inf Syst Res 29(2):381–400. https://doi.org/10.1287/isre.2018.0794

Cottrill CD (2020) MaaS surveillance: privacy considerations in mobility as a service. Transp Res Part A Policy Pract 131:50–57. https://doi.org/10.1016/j.tra.2019.09.026

Davie M, Gisolfi D, Hardman D, Jordan J, O'Donnell D, Reed D (2019) The trust over IP stack. IEEE Commun Stand Mag 3(4):46–51. https://doi.org/10.1109/mcomstd.001.1900029

de Reuver M, Bouwman H, Haaker T (2009) Mobile business models: organizational and financial design issues that matter. Electron Mark 19:3–13

Esztergár-Kiss D, Kerényi T, Mátrai T, Aba A (2020) Exploring the MaaS market with systematic analysis. Europ Transp Res Rev. https://doi.org/10.1186/s12544-020-00465-z

European Commission (2017) Commission delegated regulation (EU) 2017/1926. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1926 &rid=6. Accessed 19 Nov 2023

Feulner S, Sedlmeir J, Schlatt V, Urbach N (2022) Exploring the use of self-sovereign identity for event ticketing systems. Electron Mark 32:1759–1777. https://doi.org/10.1007/s12525-022-00573-9

Ford D, Håkansson H (2013) Competition in business networks. Ind Mark Manag 42(7):1017–1024. https://doi.org/10.1016/j.indmarman.2013.07.015

Gast J, Gundolf K, Harms R, Collado EM (2019) Knowledge management and coopetition: how do cooperating competitors balance the needs to share and protect their knowledge? Ind Mark Manag 77:65–74. https://doi.org/10.1016/j.indmarman.2018.12.007

Georgakis P, Almohammad A, Bothos E, Magoutas B, Arnaoutaki K, Mentzas G (2019) MultiModal route planning in mobility as a service. In: IEEE/WIC/ACM international conference on web intelligence – companion volume. ACM. https://doi.org/10.1145/3358695.3361843

Giesecke R, Surakka T, Hakonen M (2016) Conceptualising mobility as a service. In: 11th international conference on ecological vehicles and renewable energies. IEEE https://doi.org/10.1109/ever.2016.7476443

Goulding R, Kamargianni M (2018) The mobility as a service maturity index: preparing the cities for the mobility as a service era. In: Proceedings of 7th transport research arena, Zenodo. https://doi.org/10.5281/ZENODO.1485002

Gregor S, Hevner AR (2013) Positioning and presenting design science research for maximum impact. MIS Q 37(2):337–355. https://doi.org/10.25300/misq/2013/37.2.01

Guggenberger T, Sedlmeir J, Fridgen G, Luckow A (2021) An in-depth investigation of the performance characteristics of Hyperledger Fabric. Comput Ind Eng. https://doi.org/10.1016/j.cie.2022.108716

Hardman D (2021) Aries RFC 0004: agents. https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0004-agents/README.md. Accessed 19 Nov 2023

Harper S (2020) Why your brand probably doesn't need an app. https://www.forbes.com/sites/theyec/2020/03/02/why-your-brand-probably-doesnt-need-an-app/?sh=7163972c12c5. Accessed 19 Nov 2023

Hermes S, Kaufmann-Ludwig J, Schreieck M, Weking J, Böhm M (2020) A taxonomy of platform envelopment: revealing patterns and particularities. In: Proceedings of the 26th Americas conference on information systems

Hevner M, March S, Park R, Ram S (2004) Design science in information systems research. MIS Q 28(1):75–105. https://doi.org/10.2307/25148625

Hoess A, Rieger A, Roth T, Fridgen G, Young AG (2023) Managing fashionable organizing visions: evidence from the European blockchain services infrastructure. In: Proceedings of the 31st European conference on information systems

Hoess A, Schlatt V, Rieger A, Fridgen G (2021) The blockchain effect: from inter-ecosystem to intra-ecosystem competition. In: Proceedings of the 29th European conference on information systems

Hoffmann W, Lavie D, Reuer JJ, Shipilov A (2018) The interplay of competition and cooperation. Strateg Manag J 39(12):3033–3052. https://doi.org/10.1002/smj.2965

Hoffmann I, Jensen N, Cristescu A (2021) Decentralized governance for digital platforms – architecture proposal for the mobility market to enhance data privacy and market diversity. In: 18th annual consumer communications & networking conference. IEEE

IATA (2023) Building open API connections for the digital transformation. https://airlines.iata.org/analysis/building-open-api-connections-for-the-digital-transformation. Accessed 19 Nov 2023

Jacobides MG, Cennamo C, Gawer A (2018) Towards a theory of ecosystems. Strat Manag J 39(8):2255–2276. https://doi.org/10.1002/smj.2904

Jensen T, Hedman J, Henningsson S (2019) How TradeLens delivers business value with blockchain technology. MIS Q Exec 18(4):221–243. https://doi.org/10.17705/2msqe.00018

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

Jittrapirom P, Marchau V, van der Heijden R, Meurs H (2018) Dynamic adaptive policymaking for implementing mobility-as-a service (MaaS). Res Transp Bus Manag 27:46–55. https://doi.org/10.1016/j.rtbm.2018.07.001

Jørgensen KP, Beck R (2022) Universal wallets. Bus Inf Syst Eng 64(1):115–125. https://doi.org/10.1007/s12599-021-00736-6

Kamargianni M, Li W, Matyas M, Schäfer A (2016) A critical review of new mobility services for urban transport. Transp Res Procedia 14:3294–3303. https://doi.org/10.1016/j.trpro.2016.05.277

Kannengießer N, Lins S, Dehling T, Sunyaev A (2020) Trade-offs between distributed ledger technology characteristics. ACM Comput Surv. https://doi.org/10.1145/3379463

Kannengießer N, Lins S, Sander C, Winter K, Frey H, Sunyaev A (2022) Challenges and common solutions in smart contract development. IEEE Transact Softw Eng 48:4291–4318. https://doi.org/10.1109/tse.2021.3116808

Katz ML, Shapiro C (1994) Systems competition and network effects. J Econ Perspect 8(2):93–115. https://doi.org/10.1257/jep.8.2.93

Ketter W, Schroer K, Valogianni K (2022) Information systems research for smart sustainable mobility: a framework and call for action. Inf Syst Res 34(3):1045–1065. https://doi.org/10.1287/isre.2022.1167

Köhler S, Pizzol M (2020) Technology assessment of blockchain-based technologies in the food supply chain. J Clean Prod. https://doi.org/10.1016/j.jclepro.2020.122193

Kruchten P (1995) The 4+1 view model of architecture. IEEE Softw 12(6):42–50. https://doi.org/10.1109/52.469759

Lacity M, Carmel E, Young AG, Roth T (2023) The quiet corner of Web3 that means business. MIT Sloan Manag Rev 64(3):20–26

Lamberti R, Fries C, Lücking M, Manke R, Kannengießer N, Sturm B, Komarov MM, Stork W, Sunyaev A (2019) An open multimodal mobility platform based on distributed ledger technology. In: Internet of things, smart spaces, and next generation networks and systems. Springer, Heidelberg, pp 41–52, https://doi.org/10.1007/978-3-030-30859-9_4

Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems – a discussion of recent research. Transp Res Part A Policy Pract 81:16–34. https://doi.org/10.1016/j.tra.2015.06.002

Moher D, Liberati A, Tetzlaff J, Altman DG, PRISMA Group (2009) Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Ann Intern Med 151(4):264–269

Mühle A, Grüner A, Gayvoronskaya T, Meinel C (2018) A survey on essential components of a self-sovereign identity. Comput Sci Rev 30:80–86

Myers MD, Newman M (2007) The qualitative interview in IS research: examining the craft. Inf Organ 17(1):2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Nguyen TH, Partala J, Pirttikangas S (2019) Blockchain-based mobility-as-a-service. In: 28th international conference on computer communication and networks. IEEE. https://doi.org/10.1109/icccn.2019.8847027

Paiva S, Ahad M, Tripathi G, Feroz N, Casalino G (2021) Enabling technologies for urban smart mobility: recent trends, opportunities and challenges. Sens. https://doi.org/10.3390/s21062143

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–77. https://doi.org/10.2753/mis0742-1222240302

Platt M, Bandara RJ, Drăgnoiu AE, Krishnamoorthy S (2021) Information privacy in decentralized applications. In: ur Rehman MH, Svetinovic D, Salah K, Damiani E (eds) Trust models for next-generation blockchain ecosystems. Springer, Heidelberg, pp 85–104. https://doi.org/10.1007/978-3-030-75107-4_4

Polydoropoulou A, Pagoni I, Tsirimpa A (2020) Ready for mobility as a service? Insights from stakeholders and end-users. Travel Behav Soc 21:295–306. https://doi.org/10.1016/j.tbs.2018.11.003

Polydoropoulou A, Pagoni I, Tsirimpa A, Roumboutsos A, Kamargianni M, Tsouros I (2020) Prototype business models for mobility-as-a-service. Transp Res Part A Policy Pract 131:149–162. https://doi.org/10.1016/j.tra.2019.09.035

Rieger A, Guggenmos F, Lockl J, Fridgen G, Urbach N (2019) Building a blockchain application that complies with the EU general data protection regulation. MIS Q Exec 18:263–279

Ritala P (2022) Coopetition strategy - when is it successful? Empirical evidence on innovation and market performance. Br J Manag 23:307–324. https://doi.org/10.1111/j.1467-8551.2011.00741.x

Saldaña J (2013) The coding manual for qualitative researchers, 2nd edn. SAGE, Thousand Oaks

Santos G, Nikolaev N (2021) Mobility as a service and public transport: a rapid literature review and the case of Moovit. Sustain. https://doi.org/10.3390/su13073666

Sartor S, Sedlmeir J, Rieger A, Roth T (2022) Love at first sight? A user experience study of self-sovereign identity wallets. In: Proceedings of the 30th European conference on information systems. AIS

Schlatt V, Sedlmeir J, Feulner S, Urbach N (2022) Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Inf Manag 59(7):103553. https://doi.org/10.1016/j.im.2021.103553

Schultze U, Avital M (2011) Designing interviews to generate rich data for information systems research. Inf Organ 21(1):1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Schulz T, Gewald H, Böhm M, Krcmar H (2020) Smart mobility: contradictions in value co-creation. Inf Syst Front 25:1125–1145. https://doi.org/10.1007/s10796-020-10055-y

Schulz T, Zimmermann S, Böhm M, Gewald H, Krcmar H (2021) Value co-creation and co-destruction in service ecosystems: the case of the Reach Now app. Technol Forecast Soc Change. https://doi.org/10.1016/j.techfore.2021.120926

Sedlmeir J, Lautenschlager J, Fridgen G, Urbach N (2022) The transparency challenge of blockchain in organizations. Electron Mark 32:1779–1794. https://doi.org/10.1007/s12525-022-00536-0

Sedlmeir J, Barbereau T, Huber J, Weigl L, Roth T (2022a) Transition pathways towards design principles of self-sovereign identity. In: 43rd international conference on information systems. AIS. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4. Accessed 19 Nov 2023

Shaheen SA, Cohen AP (2012) Carsharing and personal vehicle services: worldwide market developments and emerging trends. In J Sustain Transp 7(1):5–34. https://doi.org/10.1080/15568318.2012.660103

Smichowski BC (2018) Determinants of coopetition through data sharing in MaaS. Manag Data Sci 2(3):1–9

Smith G, Sochor J, Karlsson IM (2018) Mobility as a service: development scenarios and implications for public transport. Res Transp Econ 69:592–599. https://doi.org/10.1016/j.retrec.2018.04.001

Smith G, Sochor J, Karlsson IM (2020) Intermediary MaaS integrators: a case study on hopes and fears. Transp Res Part A Policy Pract 131:163–177. https://doi.org/10.1016/j.tra.2019.09.024

Sochor J, Strömberg H, Karlsson ICM (2015) Implementing mobility as a service. Transp Res Rec J Transp Res Board 2536(1):1–9. https://doi.org/10.3141/2536-01

Sochor J, Karlsson ICM, Strömberg H (2016) Trying out mobility as a service: experiences from a field trial and implications for understanding demand. Transp Res Rec J Transp Res Board 2542(1):57–64. https://doi.org/10.3141/2542-07

Sochor J, Arby H, Karlsson IM, Sarasini S (2018) A topological approach to mobility as a service: a proposed tool for understanding requirements and effects, and for aiding the integration of societal goals. Res Transp Bus Manag 27:3–14. https://doi.org/10.1016/j.rtbm.2018.12.003

Soltani R, Nguyen UT, An A (2021) A survey of self-sovereign identity ecosystem. Secur Commun Netw 2021:1–26. https://doi.org/10.1155/2021/8873429

Sonnenberg C, vom Brocke J (2012) Evaluation patterns for design science research artefacts. In: Communications in computer and information science. Springer, Heidelberg, pp 71–83

Sternberg HS, Hofmann E, Roeck D (2020) The struggle is real: insights from a supply chain blockchain case. J Bus Logist 42(1):71–87

Stockburger L, Kokosioulis G, Mukkamala A, Mukkamala RR, Avital M (2021) Blockchain-enabled decentralized identity

management: the case of self-sovereign identity in public transportation. Blockchain: Res Appl 2(2):100014. https://doi.org/10.1016/j.bcra.2021.100014

Strauss A, Corbin J (1998) Basics of qualitative research: Techniques and procedures for developing grounded theory, 2nd edn. Sage

Sümmermann D, Öge CD, Smolenski M, Fridgen G, Rieger A (2017) Open mobility system OMOS: the joint journey towards seamless mobility. https://eref.uni-bayreuth.de/39645/

Surakka T, Härri F, Haahtela T, Horila A, Michl T (2018) Regulation and governance supporting systemic MaaS innovations. Res Transp Bus Manag 27:56–66. https://doi.org/10.1016/j.rtbm.2018.12.001

Tomaino G, Teow J, Carmon Z, Lee L, Ben-Akiva M, Chen C, Leong WY, Li S, Yang N, Zhao J (2020) Mobility as a service (MaaS): the importance of transportation psychology. Mark Lett 31(4):419–428. https://doi.org/10.1007/s11002-022-09617-8

Toufaily E, Zalan T, Dhaou SB (2021) A framework of blockchain technology adoption: an investigation of challenges and expected value. Inf Manag 58(3):103,444. https://doi.org/10.1016/j.im.2021.103444

Venable J, Pries-Heje J, Baskerville R (2016) FEDS: a framework for evaluation in design science research. Europ J Inf Syst 25(1):77–89. https://doi.org/10.1057/ejis.2014.36

vom Brocke J, Simons A, Riemer K, Niehaves B, Plattfaut R, Cleven A (2015) Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. Commun AIS 37(1):205–224. https://doi.org/10.17705/1CAIS.03709

vom Brocke J, Winter R, Hevner A, Maedche A (2020) Special issue editorial - accumulation and evolution of design knowledge in design science research: a journey through time and space. J Assoc Inf Syst 21(3):520–544. https://doi.org/10.17705/1jais.00611

Webster J, Watson RT (2002) Analyzing the past to prepare for the future: writing a literature review. MIS Q 26(2):8–23

Weigl L, Barbereau TJ, Rieger A, Fridgen G (2022) The social construction of self-sovereign identity: An extended model of interpretive flexibility. In: Proceedings of the 55th Hawaii international conference on system sciences, pp 2543–2552

Willing C, Brandt T, Neumann D (2017) Intermodal mobility. Bus Inf Syst Eng 59(3):173–179. https://doi.org/10.1007/s12599-017-0471-7

Zhang R, Xue R, Liu L (2019) Security and privacy on blockchain. ACM Comput Surv. https://doi.org/10.1145/3316481

Zhao X, Vaddadi B, Sjöman M, Hesselgren M, Pernestål A (2020) Key barriers in MaaS development and implementation: lessons learned from testing corporate MaaS (CMaaS). Transp Res Interdiscip Perspect. https://doi.org/10.1016/j.trip.2020.100227