Routing the Way to Seamless Mobility-as-a-Service: Providing Multimodal Mobility through SSI and Digital Wallets

Owing to the growing awareness for sustainability and convenience expectations, customers are increasingly demanding integrated and seamless mobility in the form of mobility-as-a-service (MaaS). However, there is an apparent lack of solutions that allow travelers to efficiently combine the various mobility services required for a seamless end-to-end trip coverage. So far, attempts to provide MaaS via centralized platforms have failed to integrate a critical share of mobility service providers (MSP), since large MSPs hesitate to devolve control over strategic resources such as customer interfaces or sensitive business data. On the other hand, decentralized approaches that aim to avoid organizational lock-in effects and threats of concentration of market power by using a blockchain-based, open platform face substantial problems related to sensitive customer information and the alignment of competing MSPs' business goals. This article explores the potential of an emerging paradigm for digital identity management based on digital wallets for seamless MaaS that could provide an alternative to both centralized and blockchain-based decentralized approaches. We use design science research to develop and instantiate a corresponding MaaS architecture. We also elevate this artifact for theoretical discussion by deriving nascent design principles for coopetitive service provisioning market scenarios. Our research suggests that when building decentralized solutions, one should also consider approaches beyond blockchain and smart contracts.

Keywords - *Blockchain, Coopetition, Digital identity, Digital infrastructure, Platform, Self-sovereign identity*

1 Introduction

The increasing societal awareness of climate change and the ongoing digital transformation pressure and incentivize mobility providers to offer more sustainable and seamless mobility solutions (Schulz et al., 2021; Willing et al., 2017). Information and communication technologies (ICTs) can facilitate such business models, levering an improved mobility service procurement that aims to provide environmentally friendly mobility services and the efficient coordination of using vehicles and transport infrastructure due to low transaction costs (Jittrapirom et al., 2017; Sochor et al., 2015). As a result, customer preferences and behavior are shifting towards shared mobility. For instance, up to one in ten cars sold in 2030 may be a shared vehicle (Gao et al., 2016). Against this backdrop, researchers and practitioners increasingly advocate a sharing mobility economy and a shift from personal car ownership towards service-based mobility integrating multiple transport modes such as railway services, flights, e-scooters, or car-sharing in the form of Mobility-as-a-Service (MaaS) (Willing et al., 2017). However, mobility systems currently lack adequate solutions for travelers to efficiently combine the various mobility services required for a seamless end-to-end trip coverage, especially for planned long-distance trips (Albrecht & Ehmke, 2016; Butler et al., 2021; Schulz et al., 2021). Such trips typically demand travelers to navigate through multiple booking processes of various Mobility Service Providers (MSPs) for one travel itinerary (I. Hoffmann et al., 2021). This circumstance involves not only managing several mobile applications and accounts but also time-consuming on-boarding processes. As a result, travelers often opt for personal car ownership to avoid such an inconvenient travel planning and booking process of mobility services (Cottrill, 2020; Georgakis et al., 2019). Approaches that aim at advancing climate protection and providing more seamless public transport instead of individual traffic hence require a reduction of booking complexity within shared mobility service solutions (Barr, 2018). These enhancements could have profound economic and social impacts. According to a McKinsey & Company analysis, integrated mobility systems in 50 major cities around the world, with a population of 500 million, could deliver benefits such as improved safety and reduced pollution worth up to $600 billion (Bouton et al., 2017).

While various proprietary and regional MaaS platform solutions exist, these solutions currently fail to align and integrate multiple transport types, such as flight, railway, or car-sharing services, specifically at the international level (Hoess et al., 2021; Schulz et al., 2018). In this context, the concept of coopetition – i.e., the concurrent co-operation and competition between stakeholders, is important to enable value

co-creation and ensure individual MSPs' value capture through competition (W. Hoffmann et al., 2018). However, coopetition is especially challenging when exchanging sensitive business and personal data is required for value co-creation, and at the same time, such data contains strategic value and serves as competitive advantage for MSPs (Ford & Håkansson, 2013; Ritala, 2001). In particular, MSPs refuse to devolve control over service offerings and strategic resources, for instance, by ceding the customer interface and strategic data to a MaaS platform provider, as they fear losing their strategic position in the mobility market and being subject to a dominant platform provider (Hoess et al., 2021).

Nonetheless, patterns such as increasing market sales, creating new market structures, efficiency in resource utilization, or improving the competitive position of companies within the MaaS market are generic drivers for cooperation-related business models (Ritala, 2001). Not only researchers but also companies have identified these potentials and are increasingly investing in the direction of promising decentralized solutions to provide an open platform without organizational lock-in effects or threats of concentration of market power. First decentralized approaches like the Open Mobility System (OMOS)[1], TravelSpirit[2], or BloxMove[3] aim to lever distributed ledger technology (DLT) and its ability to provide a neutral platform, transparency, and trust (Alt, 2020; Bons et al., 2020; Fridgen et al., 2018). Those abilities enable the realization of a chain of intermodal mobility service offerings without dedicated intermediary actors (Goulding & Kamargianni, 2018; Hecht, 2021; I. Hoffmann et al., 2021). DLT-based approaches arguably motivated stakeholders to rethink centralized ecosystem structures and foster collaboration among MSPs (Hoess et al., 2021). Nonetheless, we could not observe that these efforts led to a solution with considerable backing or market share. Some decentralized approaches did not even go beyond the concept stage, so far. Moreover, research in the field of DLT illustrates that solutions solely based on DLT may not provide sufficient means for a privacy-preserving exchange of sensitive and personal data and needs to be combined with additional components (Köhler & Pizzol, 2020; Schlatt et al., 2021; Zhang et al., 2019). In particular, the inherent transparent and replicated storage of information in a blockchain network (Butijn et al., 2020) leads to considerable challenges associated with the protection of end-users personal data (Schellinger et al., 2022) and conflicts with MSPs' desire to gain a competitive advantage from travelers' data. Consequently, the question arises whether smart contracts, which

[1] https://www.omos.io/wp-content/uploads/whitepaper/OMOS_concept_paper.pdf
[2] https://travelspirit.io/
[3] https://bloxmove.com/

are used to process business logic while storing all inputs and outputs in replicated form, are suitable for MaaS provisioning (Kannengiesser et al., 2021; Schlatt et al., 2021).

To mitigate the aforementioned issues, recent research and policy-making emphasizes the concept of end users' digital identity management based on portable mobile apps, so-called digital wallets. End users can manage machine-verifiable identity documents like the ID cards or driver's license and share attributes verifiably with relying parties (Schlatt et al., 2021; Weigl et al., 2022). In particular, digital wallets offer a promising alternative concept for an efficient and cross-domain interoperale exchange of verifiable identity information bilaterally with a high level of users' control over which data they share (Ehrlich et al., 2021; Sedlmeir, Smethurst, et al., 2021; Sporny et al., 2019). These opportunities are also reflected in current policy-making such as the EU's eIDAS revision[4], UK digital identity and attributes trust framework[5], or Canadas' Verifiable Organization Network [6] that seek to lever verifiable credentials and digital wallets for enabling secure, privacy-preserving digital identity management for private and public sectors. Thus, digital wallets could be an essential component for a privacy-preserving interaction between travelers and MSPs considering aspects of coopetition from a providers perspective.

Nevertheless, the use and design of self-sovereign identity (SSI)-based architectures and their differences from current blockchain-based decentralized approaches have, so far, only been scarcely explored in research. Accordingly, the question arises of how to design an MaaS solution based on the concept of SSI technically enabled through digital wallets. Thus, we ask: *How to design seamless MaaS provisioning by using SSI and digital wallets?*

We answer this research question through a design science research (DSR) approach following Peffers et al. (2007). We first identify design objectives for MaaS solutions by conducting a multivocal systematic literature review (SLR) and 17 ex-ante expert interviews. Further, incorporating the existing body of knowledge on SSI and MaaS solutions, we develop our initial conceptual architecture for digital wallet-based MaaS. We qualitatively evaluate our architecture on the basis of seven ex-post expert interviews (Sonnenberg & vom Brocke, 2012). Based on our artifact and its evaluation, we derive nascent design theory in the form of three common applicable design principles for seamless MaaS provisioning architectures (Gregor & Hevner, 2013). Furthermore, these design principles provide practical guidance

[4]https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

[5]https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2

[6]https://vonx.io

for implementing identity management layers in service-oriented infrastructures to facilitate the seamless provisioning for coopetitive service architectures.

2 Foundations

2.1 Mobility-as-a-Service

Travelers increasingly demand seamless and combined mobility service offerings. The so-called MaaS provisioning describes a mobility model that allows travelers to combine different mobility services and means of transportation in a journey through bundling services offered by various MSPs with minimal planning and booking effort (Heikkilä et al., 2014; Sochor et al., 2018). Today's travelers typically have to go through a complex booking process for each MSP involved to use their services. The booking process can hence consist of many individual booking steps including time-consuming on-boarding processes to complete the booking of a travel itinerary. As part of this, travelers must identify the subroutes and required services of their desired itinerary and make use of different booking portals to coordinate their itinerary with the respective MSPs. This individual booking of mobility-services naturally contradicts with the desire of seamless mobility provisioning intended by MaaS. Consequently, promoting the adoption of MaaS requires a solution that avoids the repeated, time-consuming submission of personal data for booking processes (Pangbourne et al., 2020). To this end, MSPs are currently exploring unified solutions for MaaS at both a regional and a global level. On a regional level, multiple municipal and national mobility providers, e.g., Transport for London (UK), TransLink Systems (Netherlands), or Pasmo (Japan) introduced RFID-cards that allow the payment of various mobility services. These providers typically employ check-in/check-out system when entering the mode of transportation, while booking of services in advance is typically not provided. Other initiatives, focus on integrating various mobility services within a single app, such as Ubigo, WienMobil, Leipzig mobil, kvv Mobil, VIA goMobile, and Whim (Arias-Molinares & Garcia-Palomares, 2020; G. Smith et al., 2018). For instance, Whim is a pilot project providing MaaS to public and private transport travelers (e.g., public transport, car rental, cabs) via various subscription packages and targets regional mobility service offerings in the Helsinki area. This approach enables a successful integration of a variety of mobility services within a region, for instance, regional train and rail transport or cab service providers. Practitioners are also working on larger-scale projects to provide MaaS on a national and international (e.g., EU-wide) level. For example, the moovit project presents such an approach alongside similar projects such as Reach Now (Germany) or

Shift (USA), providing multiple mobility services internationally (Arias-Molinares & Garcia-Palomares, 2020; Santos & Nikolaev, 2021). However, these projects struggle with establishing a cross-regional stakeholder collaboration between individual public and private MSPs, on a cross-regional and, more crucially, an international level. This is especially challenging as various mobility services are often simultaneously dependent on a central regional provider (Zhao et al., 2020). For example, monoproduct-portals such as momondo.com, pricelines.com, or thetrainline.com consolidate only one type of mobility service. These providers list and select mobility service offerings according to various customer preferences concerning price and convenience based on comparison websites and customer rating tools. However, mono-product portals' service portfolio is commonly limited to a single mode or mobility, and thus, provides an insufficient service offering for end-to-end trip coverage.

2.2 Challenges and Potential Solutions to MaaS

Seamless MaaS is based on the interaction between MSPs and travelers and, even more critical, the collaboration between MSPs. In particular, the contractual alignment between MSPs across regional and international borders constitutes a significant component to cooperation (Polydoropoulou, Pagoni, Tsirimpa, et al., 2020). To ensure seamless interaction between travelers and MSPs, existing research and practice, have initially explored centralized approaches to MaaS (Calderón & Miller, 2019; Jittrapirom et al., 2017). Centralized approaches comprise an intermediary platform provider, typically operated by a single MSP or a dedicated joint-ventured consortium of MSPs that aggregates mobility services and makes them available to travelers for booking. Centralized solutions commonly exhibit network effects and offer technical standardization with low implementation complexity to provide seamless MaaS offerings and increase organizational revenue in a regional area (Casady, 2020; Esztergár-Kiss et al., 2020). However, centralized approaches face problems of market power concentration on the part of intermediaries. Such market players may ultimately become dominant and, thus, impose unfair market conditions through their pricing of mobility services (I. Hoffmann et al., 2021). Consequently, centralized solutions fail to attract and align a critical mass of MSPs required for a holistic MaaS offering. More specifically, MSPs resent to offer their mobility services via a third-party's platform, due to the fear of being dependent on and potentially subject to price discrimination by a dominant market player (Hoess et al., 2021). Moreover, such platform-based solutions contribute to centralized data storage and create organizational lock-in effects by using proprietary protocols and interfaces that require substantial integration efforts.

Those lock-in effects lead to structural inertia by locking travelers into a single MSP platform while affecting or even denying the chance to make use of a seamless MaaS across different platforms (Bothos et al., 2019; Constantinides et al., 2018).

To avoid these problems, practitioners and researchers recently have emphasized the potential of decentralized approaches to establish interoperable MaaS solutions that offer participating MSPs opportunities for equal market access (Hoess et al., 2021; I. Hoffmann et al., 2021; Lamberti et al., 2019). These decentralized solutions intend to enable trust and transparency through collaboration and decentralized data storage (Bothos et al., 2019; Stockburger et al., 2021).

Technically, considerations to decentralized MaaS often propose blockchain as a joint inter-organizational information infrastructure (Lamberti et al., 2019; Nguyen et al., 2019). For instance, Lamberti et al. (2019) suggest a permissionless mobility platform as decentralized marketplace for MaaS offerings. The solution suggests to provide an accurate and fair payment and billing modalities for the use of different transportation services on a ne-granular basis using the IOTA distributed ledger. According to the permissionless design, the suggested approach constitutes a platform open to any MSPs. Nguyen et al. (2019) propose a blockchain-based approach in which the traveler sends itinerary-speci c offers to a smart contract. A smart contract can represent can represent scripts or business logic on blockchain, e.g. payment or the execution of a program whose code is speci ed through a previous transaction (Kannengiesser et al., 2021). Likewise, I. Hoffmann et al. (2021) propose blockchain-based smart contracts as decentralized payment infrastructure for mobility services.

While these approaches arguably address some of the above-mentioned challenges, they may also face signi cant obstacles regarding practical diffusion. For example, it could be dif cult for all parties involved in a smart contract to agree on a “fair” implementation that respects all differing business interests (Kannengiesser et al., 2021). The implementation of blockchain-based solutions also entails technical and organizational complexities that challenge the prevailing information systems of MSP (Sternberg et al., 2020; Toufaily et al., 2021). For example, blockchain-based systems, especially for the MaaS area, likely have extensive demands on throughput, latency and transaction costs (Schaffner, 2021; Sedlmeir, Ross, et al., 2021). Moreover, blockchain-based projects often face issues resulting from the transparent processing and tamper-resistant storage of sensitive business and personal data (Zhang et al., 2019). However, these projects often discuss privacy problems only super cially or restrict to the “right to be forgotten” (Schellinger et al., 2022). For example, Nguyen et al. (2019) and I. Hoffmann et al. (2021)

do not clearly de ne how they solve problems related to the transparent processing of data. This hurdle is particularly noticeable in the trade-off between the required data sharing of sensitive business and traveler data versus con dentiality of the data (Kannengießer et al., 2020). In the MaaS context, the exchange of data underlies on an extremely fragmented booking system with complex service levels regarding veri able identity management, ticketing procedures or trusted payment processes (Bons et al., 2020; Lamberti et al., 2019; Schlatt et al., 2021). Novel solutions therefore propose the use of certi cate-based identity management provided by digital wallet apps for end-users to avoid replicated and tamper-resistant storage of personal data on a distributed ledger, in favor of a user-centric storage of personal data and bilateral disclosure of information on a case-by-case basis (Bothos et al., 2019; I. Hoffmann et al., 2021; Stockburger et al., 2021). For instance, I. Hoffmann et al. (2021) develop a decentralized modular architecture for MaaS based on DLT using Decentralized Identi ers (DIDs) and veri able credentials (VCs). The authors advocate the use of digital identity claims issued by governmental institutions to lever the exchange of authentic personal data in bilateral interactions between travelers and MSPs. In doing so, a DLT is used to register a unique (DID) for each traveler and generate a binding between travelers and their identity claims on-chain. However, this approach may again result in privacy-related problems (Hoess et al., 2022; Rieger et al., 2021; Schlatt et al., 2021). Moreover, to regulate market access, the proposed architecture introduces dedicated authorities that act as discovery service providers, who provide routing services in the form of search tools to users. To this end, a discovery service runs a node on the DLT and acts as a gatekeeper for other third-party service providers. As a result, the proposed architecture may yield in a monopolistic or oligopolistic market structure consisting of multiple centralized platforms restricting service offerings and third-party providers' access to the mobility market.

2.3 The Building Blocks of Self-Sovereign Identities

SSI means a self-determined, digital identity. The central starting point of SSI is that the users manage their digital identities themselves, i.e., without being dependent on a central identity service provider. Personal identity features such as an address, ID number, access codes, or creditworthiness information are to be stored in a kind of digital wallet on a users' device (Cucko & Turkanovic, 2021; Ehrlich et al., 2021).

Digital wallets are open and portable systems to allow individuals to fully own and manage their own identities, leading to the idea of “self-sovereign” identity systems. These systems use digital signatures to create tamper-resistant identity records stored on the users device within the digital wallet. Any organization, including public and private institutions, can issue those identity records in the form of credentials containing attributes, which the user can manually accept and store in the digital wallet (Tobin & Reed, 2016; Weigl et al., 2022). Once stored in the wallet, these credentials serve as veri able proof of the same information that a physical credential contains. Through the use of technologies such as digital signatures, veri able credentials become more autonomous, veri able and trustworthy than their physical counterparts and can be presented to third parties veri ed and secure (Soltani et al., 2021; Sporny et al., 2019).

The system consists of mandatory building blocks: Stakeholders (Issuer, Holder, Veri er), VCs, DIDs, Digital Wallets and Digital Agents (Davie et al., 2019; Ferdous et al., 2019; Laatikainen et al., 2021). Each identity record is created by an Issuer, held by a Holder, and information contained therein is presented to the Veri er. Issuers are trusted parties whose identity is publicly visible. Those Issuers and so-called authorities attest, digitally sign, and transfer machine-veri able identity records or certi cates, so-called VCs to the Holder. VCs can either contain self-attested identity attributes (claims) or those attested by third parties. To increase integrity, VCs are cryptographically signed while containing speci c individual information. The Holders can then store these VCs in their digital wallet and use it to present speci c identity claims to the Veri er by means of a veri able presentation (VP), i.e., the presentation of selectively chosen claims (Sporny et al., 2019). VPs are often enhanced through zero-knowledge proofs (ZKPs) to allow the selective disclosure of identity claims to consent to present speci c parts of their data regarding data minimization aspects compliant with GDPR.

Typically, digital wallets or universal wallets provide features to store veri able identity information and to process mandatory interactions with other self-sovereign identities. These include message signing, authentication (DID-Auth), or the management of VCs (Strüker et al., 2021; Vescent et al., 2018). In this context, the DIDComm-messaging protocol use DIDs for transferring stored credentials bilaterally. In practice, a digital wallet is a software application (e.g., a mobile application) for managing VCs. The use of cryptographic keys provides a high level of security which is necessary to enable travelers to provide a secure and VP. In this context, however, the Veri er must trust the Issuer as a superior authority,

since the Veri er can already verify the cryptographic secured VC through bilateral interaction with the Holder (Reed et al., 2020).

The topic of digital wallets is also gaining momentum in practice. More and more organizations and consortia, such as the Veri able Organizations Network (VON)[7] or IDUnion[8] are joining forces intending to establish SSI with a practical environment. Also, from a political point of view, speci c SSI-based showcase projects, such as that of the European Self Sovereign Identity Framework (eSSIF)[9] or the showcase projects of the German Federal Chancellery (e.g., SSI-based Hotel Check-in)[10] already employ digital wallets to practically implement business-related case studies based on SSI. As a result, the potential of SSI-based solutions also appears to be growing rapidly in practice (S. S. Smith, 2020; Soltani et al., 2021; Weigl et al., 2022).

3 Design Science Research Approach

To conceptualize a seamless MaaS architecture, we follow a DSR approach. This approach involves the design and development of innovative and meaningful artifacts such as constructs, methods, models, or instantiations for a speci c problem in the eld of information systems research (Gregor & Hevner, 2013; Hevner et al., 2004). Within our study, we developed a model in form of a comprehensive architecture that provides a solution approach for delivering 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) through grounding our work on previous research and practical insights provided through expert interviews, and iterative build-and-evaluate working steps. For an IT artifact to strongly contribute to IS research, it must address a relevant business need, which can result from the persons, organizations, or technologies used in an environment (Hevner et al., 2004). As argued in Section 1, the provision of a seamless MaaS platform represents such a business need.

We follow the method of Peffers et al. (2007) to create a meaningful IT artifact. From a technical and governance perspective, we identify a lack of coordination among competing MSPs, risks of concentration of market power, and insuf cient solutions for data protection as core problems of current centralized and decentralized MaaS solutions.

[7] https://vonx.io/
[8] https://idunion.org/
[9] https://decentralized-id.com/government/europe/eSSIF/
[10] https://www.bundesregierung.de/breg-de/suche/start-pilot-hotel-check-in-1914392

Following the problem formulation, we de ne the objectives and associated requirements of a potential solution. To this end, we conducted a SLR (Webster & Watson, 2002) and complement it with 17 qualitative ex-ante expert interviews, which were conducted as part of a prior study related to decentralized MaaS (Section 4.1.1 and 4.1.2). We analyzed the publications and interviews through open and axial coding and derived four design objectives and 12 corresponding design requirements for seamless MaaS (Section 4.2) (Saldaña, 2013). We then performed iterative build-and-evaluate loops to develop a MaaS architecture that addresses the identi ed design objectives and requirements. In doing so, we iterate through the design and development of the IT artifact by demonstrating and evaluating the artifact's functionality at each stage of development. For exhibition, we instantiated a prototype of our architecture, to demonstrate the feasibility and illustrate its characteristics of our conceptual architecture. We present the nal stage of our architecture in Section 4.3.

A rigorous evaluation needs to consider both: the underlying fundamental problem and the artifact (Peffers et al., 2007; Venable et al., 2016). We opted for a qualitative evaluation based on additional seven ex-post expert interviews (Sonnenberg & vom Brocke, 2012; Venable et al., 2016). More speci cally, we conducted those expert interviews to evaluate our architecture and ultimately ensure the relevance of our research in Section 5. In these interviews, we demonstrated our prototype to provide our experts with a broad overview of the architecture's characteristics and functionalities. We analyzed codes from the interviews related to our architecture's technical building blocks (e.g., VCs, digital agents, digital wallets, standardized interfaces, APIs and data storage) to elevate the implicit knowledge contribution in our IT artifact to more abstract and generalizable knowledge that can be used for theoretical discussion (Gregor & Hevner, 2013). For this purpose, we formulated design principles for SSI-based MaaS architectures, as this technical approach is both novel and increasingly discussed but no general DPs currently exist in literature. More speci cally, we identi ed three generic principles which may also be applicable to similar services provisioning architectures. Finally, we share the ndings trough this article taking into account the experts' assessments (Gregor & Hevner, 2013; vom Brocke et al., 2020).

4 Proposed Architecture

4.1 Derivation of Design Objectives and Respective Requirements

4.1.1 Systematic Literature Review

To ground our work on prior knowledge, we conducted a SLR according to Webster and Watson (2002). We used the search string ("mobility as a service" OR MaaS) AND (intermodal OR multimodal) AND (transport OR mobility) to cover the eld of intermodal and multimodal transport as well as the eld of MaaS. We conducted our search using seven different databases, including Scopus, Science Direct, ACM Digital Library, EBSCOHost, IEEEXplore, Web of Science, and AIS eLibrary. We performed all search runs on "full text and metadata analysis". Our initial search returned a total of 2,165 hits, excluding 114 occurrences of duplicates. Next, we screened these results in four process steps 1) title screening, 2) abstract screening, 3) full text analysis and 4) a forward and backward search. Within each step, we focused on articles that outline holistic requirements for MaaS, consider the (technical) design of MaaS systems, and provide guidelines to implement MaaS. In doing so, we considered both centralized and decentralized solutions to MaaS to ground our design on knowledge generated by prior solution approaches (vom Brocke et al., 2015). Taking these criteria into account, we identi ed 147 articles after the initial title screening that we considered relevant for further analysis. Out of these, we identi ed 23 articles as relevant by screening the abstracts of all remaining articles. We selected these articles, as they directly relate to the conceptualization or implementation of centralized or decentralized MaaS-related solutions. The full-text analysis yielded a subset of 10 relevant articles, which we supplemented with four additional articles that we found through a forward and backward search and an additional grey literature analysis using Google Scholar or various search engines such as the Google Search Engine. Ultimately, our nal data set includes a foundation of 14 publication. Figure 1 summarizes the process of our SLR.

4.1.2 Ex-ante Interviews for Design Objectives and Prototype Development

Due to the relative scarcity of relevant literature, we considered the results of our SLR alone insuf - cient for deriving comprehensive design objectives that are relevant for the practical environment. In particular, the articles derived through our SLR all focused mainly on technical components and did not incorporate business perspectives. Therefore, we enriched our literature with 17 expert interviews that one of our authors conducted as part of a prior study related to decentralized MaaS. This interview set

Figure 1: Systematic Literature Review following Webster and Watson (2002).

includes experts from 14 organizations in the mobility services industry, including among other, established MSPs, Original Equipment Manufacturers (OEMs), MSP start-ups or IT consultancies, of different mobility providers, as illustrated in Table 1. The selected practitioners and researchers were knowledgeable about both the organizational and technical requirements of the public and private mobility sector in general, as well as the speci c business and technical needs for MaaS. The various backgrounds of these experts enabled us to deduce requirements for a seamless MaaS solution from a broad socio-technical perspective, as suggested by vom Brocke et al. (2020). In these interviews, the experst provided insights on the challenges of current MaaS solutions as well as the requirements and opportunities of an open and decentralized MaaS system. Furthermore, they discussed the role and current challenges of blockchain as a technical basis for decentralized MaaS. The interviews had a total duration of 869 minutes with an average duration of 50 minutes per interview and were fully audio-recorded and transcribed. We coded each interview following a two-staged process of open and axial coding (Saldaña, 2013). We conducted an open-coding to gather a broad overview about the needed requirements within the rst round of coding. Thereupon, we performed a second round of axial-coding to categorize and condense our ndings to generalizable design objectives (Saldaña, 2013).

#	Organizational Responsibility	Experience	Interview Duration
1	Project & Productmanager (private MSP)	1 years	62 Minutes
2	Business Developer & IT-Consultant (Consultancy)	2 years	62 Minutes
3	Business Developer (public MSP)	7 years	49 Minutes
4	Head of Strategic Future Projects (OEM)	2 years	52 Minutes
5	Head of Business Development (Transportation & Rail)	7 years	21 Minutes
6	CEO (IT Consultancy)	5 years	73 Minutes
7	CTO (private MSP)	3 years	42 Minutes
8	Product Owner (Tech Mobility)	1 years	49 Minutes
9	Business Developer (public MSP)	3 years	48 Minutes
10	CEO (Tech Mobility)	10 years	68 Minutes
11	Consortium Partner (Mobility Association)	10 years	60 Minutes
12	DLT Business Developer (OEM)	3 years	59 Minutes
13	Head of B2A and Partnering (OEM)	5 years	58 Minutes
14	CEO (Mobility Association)	3 years	36 Minutes
15	Blockchain Developer (Tech Company)	5 years	42 Minutes
16	Managing Consultant (Tech Company)	3 years	49 Minutes
17	Blockchain Project Manager (Tech Company)	4 years	39 Minutes

Table 1: Ex-ante Interviews.

4.2 Design Objectives

To de ne the general properties of our MaaS architecture, we derived four design objectives and twelve respective requirements from our SLR and ex-ante expert interviews. In the following we describe our identi ed design objectives and requirements. To provide further detail on the coherence of our ndings, we reference the corresponding literature and the amount of experts textually (in parenthesis). In addition, Table 3 summarizes the design objectives and requirements that we obtained and provides a detailed overview of the corresponding experts and literature we draw our statements from.

4.2.1 Neutrality

MaaS solutions need to incentivize various MSPs to work together. In this context, cooperation and collaboration of MSPs are of central importance for successful MaaS implementations and, at the same time, the biggest challenge (Calderón & Miller, 2019). This challenge is typically driven by the prevailing competition between providers, their aim for a dominant position in the mobility market, as well as their varying business goals. For example, the private sector strives for increasing revenues, while the public sector aims to reduce the use of personal vehicles and expanding the use of public transportation (Arias-Molinares & Garcia-Palomares, 2020). While MSPs typically compete for providing individual service offerings to travelers, the presence of complementary service offerings – even provided by another MSP – increases their own services' value and allows them to bene t from network effects (Jacobides et al., 2018; Katz & Shapiro, 1994)(7 Experts).

As a result, MSPs appreciate a certain degree of cooperation to foster value-creation by leveraging network effects on both sides (Smichowski, 2018; Tomaino et al., 2020). Therefore, our experts recommend considering the aspect of Coopetition (R1) between MSPs (W. Hoffmann et al., 2018) (17 Experts). In terms of developing and implementing a corresponding platform solution, this means that the established MSPs in particular are interested in creating and hosting such a platform themselves. The role as an intermediary allows MSPs to maintain their current market and product power. Simultaneously, acting as an intermediary reduces threats of cannibalizing their mobility service portfolio by controlling third-party services offered through a potential platform solution, as well as protecting sensitive business data and potentially create value from the business data of other parties involved (Bothos et al., 2019; Polydoropoulou, Pagoni, & Tsirimpa, 2020). Thus, they often resent integrating their services into another provider's platform because they fear of becoming merely a service provider, on a (centralized or decentralized) platform and thus losing the direct customer contact and interface (Jittrapirom et al., 2018; Sochor et al., 2016) (11 Experts). Aggregating all customer interactions at a single intermediary substantially increases the market power of this actor, due to their ability to control strategic data and third-party provider/services. Consequently, those platform operators may gain a monopolistic or at least dominant position in the MaaS market (G. Smith et al., 2020).

To avoid such dominance by a single or small set of MSPs, a potential large-scale solution for MaaS should grant all MSPs equal opportunities to place service offerings and compete within the mobility market (Calderón & Miller, 2019; Lamberti et al., 2019; Mattsson & Jenelius, 2015). Therefore, as part of a potential solution, practitioners recommend addressing this problem through Disintermediation (R2) (5 Experts). Furthermore, the possible solution needs to provide Openness (R3), independent of market power and governance hierarchies, to onboard all potential MSPs as participants of such a seamless mobility solution without having barriers-to-entry and business-related disadvantages. This includes the possibility to seamlessly integrate multiple services of different MSPs and to provide them with the opportunity to offer their entire service portfolio (Arias-Molinares & Garcia-Palomares, 2020; Kamargianni et al., 2016; Paiva et al., 2021) (7 Experts). In particular, to foster coopetition, our experts stress the need for standardized and public application programming interfaces (APIs), which each participant in the platform can integrate to position the brand and its conditions on the market (10 Experts). Such open APIs could also solve the complex challenge in terms of an accurate and fair distribution of costs and pro ts compensation among all involved parties (Lamberti et al., 2019). However, the basis for an

accurate and fair distribution of costs is trust or the will to cooperate among the MSPs (Polydoropoulou, Pagoni, Tsirimpa, et al., 2020).

4.2.2 Data Protection

Prior literature illustrates that the implementation of ef cient MaaS platforms requires real-time data sharing amongst 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 personal data. The need for data protection is two-fold. MSPs are interested in protecting their business data (R4) as well as customer information they obtain during booking processes and service usage. MSPs typically exploit data such as personal information of their customers, payment histories, transaction references, movement pro les or habits from other MSPs, to improve their service offerings and gain a competitive advantage (Experts 5-7). As such data may serve as a competitive advantage, they are hesitant to share it with competitors. Moreover, they are strictly bound to regulatory laws – such as antitrust law or GDPR – that they must ensure the protection of sensitive data, such as personal data of their customers, from other third parties (Paiva et al., 2021; Surakka et al., 2018) (12 Experts). Limiting the sharing of personal data is also in the sense of customers, who aim to preserve their privacy and prevent user tracking (R5). In this sense, appropriate data management is necessary to ensure confidentiality and reduce privacy concerns (Cottrill, 2020) (11 Experts). However, since MaaS solutions integrate multiple services at different hierarchical levels, sharing required data while safeguarding data protection becomes even more challenging (Expert 16). For instance, the solution has to assign well-de ned responsibilities and provide clear terms and conditions on how to process sensitive data. This is especially important for ticket issuing and veri cation as well as clearing and payment processes within a traveling route with multiple sub-routes (Polydoropoulou, Pagoni, Tsirimpa, et al., 2020; Stockburger et al., 2021). Privacy concerns and security techniques are very dissimilar. For instance, according to the General Data Protection Regulation (GDPR), organizations should reduce the processing of personal data and related privacy risks through data minimization, purpose limitation, and privacy by design and default.

4.2.3 Manageability

From a management perspective, the interviewed experts believe that a seamless MaaS solution is also characterized by its Modularity (R6)(12 Experts). In this context, a modular solution requires open and

decentralized design concepts enabling each MSP to offer its mobility services through proprietary but standardized, interoperable, and accessible interfaces. This approach of modularity and decentralization can facilitate a shared market structure without intermediaries (R2) and creates resilience of the entire market compared to centralized solutions (Bothos et al., 2019; Lamberti et al., 2019; Nguyen et al., 2019). Ultimately, standardized customer interfaces, e.g. MSPs' booking applications, are required in this context to prevent the unnecessary development of isolated stand-alone solutions of individual MSPs and to create an interoperable solution (12 Experts 12).

Nonetheless, these modular stand-alone solutions must be able to support a high number of customer transactions, which are characteristic for the mobility market. Consequently, a MaaS solution must provide a high level of Process Ef ciency (R7) to be able to seamlessly provide this frequency of supply and demand and also take the aspect of scalability into account (4 Experts). This development of the MaaS sector is especially critical for a trusted and secure environment that enables business processes and the handling of personal as well as business-sensitive data (Sümmermann et al., 2017).

4.2.4 User Experience

To improve the user experience for travelers, MaaS solutions should especially ensure a seamless data sharing (R8) for customers' identity data (Paiva et al., 2021). This portability of identity data is intended to enable customers to interoperate across all mobility services, so they do not have to re-register with each service. As customer preferences can be shared among the different applications, seamless data sharing thus helps to avoid vendor lock-in effects from a customer perspective (8 Experts). The various types of implementations of transportation services lead to many challenges concerning cross-system data handling, like fare management (Lamberti et al., 2019). These challenges require a suitable solution to increase the overall accessibility and transparency within the MaaS solution for the customer (Stockburger et al., 2021) (7 Experts). In this context, interoperability and a solution that takes various customer preferences into account can help address the challenge of application fatigue – the observation customers are negatively affected by an oversupply of applications (Harper, 2020). Moreover, the overall solution needs to be usable as fast as possible (R7), open to rebuild by every MSP, re ect various customer preferences of different customer segments and should be easy to use for customers (Paiva et al., 2021). Ultimately, however, a decentralized and interoperable solution, taking into account a broad-variety of customer preferences and a large set of MSP, faces the problem that in the event of an issue with a

speci c mobility service, the customer must also know exactly whom to contact (Giesecke et al., 2016). Since a total trip may consist of multiple services, which may have been offered by different MSPs, this may lead to inconsistencies of responsibility and also liability in case of service issues. Therefore, it is important that the MaaS solution de nes the responsibilities of MSPs concerning customer support (R9).

4.3 Seamless MaaS Architecture Based on SSI and Digital Wallets

Considering the derived design objectives and corresponding requirements, we developed a conceptual architecture for seamless MaaS, which we illustrate in Figure 3 (see Appendix). Fundamentally, the architecture is based on SSI and digital wallets for decentralized identity management using secure communication protocols. Similar to typical SSI-based solutions, our architecture consists of three central entities: the travelers as the travel ticket holder, the MSP as travel ticket issuer, and the travel ticket inspector as ticket veri er. The seamless MaaS architecture requires an additional fourth entity as a decentralized coordinate instance: the routing service. The routing service serves as a coordinator of the traveler's itinerary information to the respective MSPs without getting, nor exposing sensitive personal data.

For communication among those entities, we employ REST-APIs secured via Hyper Transfer Protocol Secure (HTTPS) for business-to-business (B2B) interactions – in our case in particular between the MSPs and the routing service. The DIDComm messaging speci cation (DIDComm) provides the technical basis for transferring VCs within business-to-customer (B2C) communication – in our case between the traveller and MSPs – as used in many present digital wallet applications. In contrast to conventional X.509 certi cates, the use of VCs and DIDComm provides additional features such as zero-knowledge proofs (ZKPs) that enable selective disclosure of speci c attributes stored in a credential document (Hoess et al., 2022; Sporny et al., 2019).

Each entity requires several components to enable communication and/or execute business logic, which we will describe in the following. In addition, DIDComm communication requires an arbitrary database for server-side data storage, an existing legacy system provided by a trusted authority, or a public blockchain solution, e.g., Hyperledger Indy. This database (not necessarily an DLT based database) solely provides DIDs and the corresponding DID documents, VCs schemata, and de nitions, as well as the privacy-preserving revocation registries to ensure the veri ability of travel tickets and of travelers'

personal data required for the individual booking processes. This data can be leveraged on the client-side through common, reusable, and interoperable toolkits, such as Hyperledger Aries, using APIs for the exchange of data.

Travelers are at the center of the architecture, because travelers are those who make use of the mobility services, actively decide on the services to be supplied by each MSP and initiate the corresponding by booking processes. In our architecture, travelers are therefore dependent on a digital wallet to interact with the respective MSPs. Digital wallets are an indispensable component in this context as they enable bilateral interaction with MSPs based on public key infrastructure (PKI). They store information as VCs and user keys encrypted while providing the opportunity to present selectively disclosed information, such as required identity attributes, to the issuer by using ZKP (Veseli et al., 2019).

The MSPs issue the tickets for a trip. For this purpose, the MSP consists of two components. One is the MSP controller, which executes the business logic. Business logic means that the MSP controller receives and coordinates solely trip information such as departure location, destination, departure time, and the traveler's customer number. Moreover, it instructs the MSP cloud agent, the second component of the MSP, to initiate the booking process between the traveler's digital wallet and itself. The MSP cloud agent can connect to the corresponding legacy system to publish the issuer's information such as DIDs and DID documents. Besides, it operationally issues the travel tickets to the travelers. Moreover, the MSP can establish a revocation registry on the public legacy system to be able to revoke issued travel tickets, for instance, in case of invalidity after completion of the itinerary.

The travel inspector veri es the validity of the issued travel tickets. For this purpose, the travel inspector also requires two components: the travel inspector controller and the travel inspector cloud agent. Verifying the validity of the issued travel tickets requires a travel inspector controller that can, for example, scan a QR code of the travel ticket to check it against the booking information stored on the respective legacy system. To verify the validity of tickets, the travel inspector also needs a cloud agent that can connect to the corresponding legacy system to retrieve the information. In case of services, such as car sharing, where no travel inspector is present, a static QR code can be attached to the vehicle that initiates the veri cation process.

The routing service serves as a coordination instance and requires four components to enable seamless MaaS. For this purpose, the service constitutes an extension to existing booking applications of each MSPs. The Routing Service controller is the major component coordinating three sub-components.

First, the existing booking applications of the individual MSPs. Second, a Routing Service Agent can also connect to the existing legacy system to process the publicly available custom and issuer-related attachment points. Third, the routing search algorithm which is responsible for determining the optimal transport route for the customer according to the customer preference and the current offers of the MSPs. Finally, the routing service controller packages the required coordinating information and forwards it to the appropriate MSPs.

The MaaS booking process starts with the traveler's search request to the MSP booking application of their choice. In this context, we build a modular architectures design offering the opportunity to empower MSPs to establish its proprietary and individual routing service while they are able to consider their differing business needs. The planning application forwards the travel information provided within the request to the routing service controller via HTTPS, which uses the routing search algorithm to identify the optimal MSPs mobility service offerings. The information provided by the traveller does not contain any sensitive personal data. It only includes information related to the travel itinerary, such as departure time, departure location, destination or price- or comfort preferences that the routing service coordinates. Based on the obtained preferences of the traveler, the routing service controller identi es an approximate optimal MSPs for speci c sub-route of the itinerary. Thereby, an itinerary can consist of many different sub-routes that require different types of MSPs, such as train or air mobility services, or different qualities from inferior to premium mobility service offerings. Afterward, the routing service controller instructs the routing service cloud agent to retrieve the issuer-speci c contact points (e.g., the public DIDs) of the MSPs and forwards the corresponding travel information of the booked subroute to the respective MSPs via HTTPS. For example, if an itinerary consists of two subroutes – as MSP 1 for subroute 1 and MSP 2 for subroute 2 – only MSP 1 receives the required information for subroute 1 and MSP2 receives only the required information for subroute 2. Consequently, the routing service instructs the MSPs to introduce themselves to the respective traveler.

The MSP controller receives the provided information and instructs the MSP cloud agent to send a connection invitation to the traveler's digital wallet via DIDComm. The travelers can then manually accept this connection invitation on their digital wallet establishing an end-to-end encrypted bilateral connection to MSP 1. In the next step, the MSP cloud agent sends a proof request to the traveler's digital wallet. The proof request requests speci c information, which are potentially necessary to book the ticket. In the next step, the traveler must present those to the MSP cloud agent through a veri able

presentation. For example, MSP 1 could be a car-sharing service provider that also requires a driver's license in addition to the customer's full name. Additionally, depending on the payment method, MSPs may also request relevant payment information, such as credit card number. Once the traveler has presented all the required information, the corresponding travel ticket is issued, which can be stored within his digital wallet. After completing the booking process for subroute 1, the traveler carries out the settlement process for subroute 2 analogously and bilaterally with MSP 2. Now the traveler can start the itinerary according to his seamless and individually booked travel tickets.

Ultimately, the traveler begins their journey. In the course of this, service providers' inspectors typically check the validity of issued travel tickets. In our architecture, the issued travel tickets contain a QR code, which is also stored within the digital wallet. The inspectors can scan these QR codes using the travel inspector controller forwarding the travel ticket information to the travel inspector agent. The travel inspector agents then veri es the existing validity status of the respective ticket by accessing the validity state of the travelers ticket using the public revocation registry. In case of validity of the ticket, the travelers are allowed to continue their itinerary. Alternatively, if services do not employ a travel inspector, a static QR code can be attached to the vehicle that initiates the veri cation process. Travelers can scan the QR code and thereby requests a proof request from the MSP's controller which triggers the cloud agent to request and verify a corresponding proof.

5 Evaluation

We perform an iterative evaluation along our design and development process to evaluate our artifact. Accordingly, we conduct seven additional qualitative ex-post expert interviews, as listed in Table 2. This process step is intended to support our research in evaluating our elicited requirements gathered out of SLR and ex-ante interviews. Therefore, we interviewed the experts about the structure of the framework and its feasibility to assess the applicability of our requirements. Correspondingly, we evaluate how our decentralized identity management MaaS provisioning solution is speci cally designed with SSI and universal wallets based on our derived design objectives.

In detail, we discussed how to provide a seamless MaaS architecture considering aspects concerning the design of travel planning applications, the interaction among travelers and MSPs, the corresponding processing of sensitive business and personal data, and the role of the digital wallet for decentralized MaaS provisioning. The interviews provide us an exploratory insight into how MSPs and travelers per-

Figure 2: Overview of the demonstrator

ceive their requirements for the structure of digital wallets and how those might address general architectural and constructional requirements. Furthermore, we demonstrated a prototypical implementation of our MaaS architecture to present our artifact in-use and to discuss the SSI-based MaaS work ows and user experience of our solution. Figure 2 presents our demonstrator.

With the help of this feedback, we continuously rede ned our conceptual architecture in iterative build-and-evaluate loops as suggested by Hevner et al. (2004). We audio-recorded and transcribed each interview and analyzed the conducted transcripts using a two-staged approach of open and axial coding, similar as we described in Section 4.2 (Saldaña, 2013). We also consulted with experts from different backgrounds during the ex-post evaluation to assess the implementation of our SSI-based MaaS architecture as holistically as possible. Therefore, we selected our experts from a wide range of organizations, such as established MSPs, OEMs, MSP start-ups or IT consultancies, of different mobility providers as within our ex-ante interview sessions. We conducted 407 minutes of total duration within seven interview sessions while the average duration of an interview was about 60 minutes.

#	Organizational Responsibility	Experience	Interview Duration
18	CEO (MaaS-Provider)	20 years	58 Minutes
19	CEO (IT Consultancy)	10 years	62 Minutes
20	Project Manager and Researcher (OEM)	10 years	56 Minutes
21	Product Owner for Data Exchange (OEM)	6 years	56 Minutes
22	Product Owner for Emerging Technologies (OEM)	4 years	64 Minutes
23	Head of Blockchain (IT Service Provider)	20 years	57 Minutes
24	Chief Blockchain Architect (Transport IT & Services)	9 years	54 Minutes

Table 2: Ex-post Interviews