Blockchain: Research and Applications 2 (2021) 100014

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation

Lukas Stockburger [a], Georgios Kokosioulis [a], Alivelu Mukkamala [a], Raghava Rao Mukkamala [a,b], Michel Avital [a,*]

[a] *Department of Digitalization, Copenhagen Business School, Howitzvej 60, Frederiksberg, DK-2000, Denmark*
[b] *Department of Technology, Kristiania University College, Kirkegata 24-26, 0153 Oslo, Norway*

ARTICLE INFO

Keywords:
Identity management
Self-sovereign identity
Blockchain
Distributed ledger
Intelligent transport systems
Payment systems infrastructure

ABSTRACT

Identity management has been ripe for disruption over the past few years due to recurring incidents of data breaches that have led to personal information leaks and identity theft. The rise of blockchain technology has paved the way for the development of self-sovereign identity (SSI)—a new class of user-controlled resilient identity management systems that are enabled by distributed ledger technology. This paper examines how SSI management can be used in a public transportation sector that spans different operators in multiple countries. Specifically, the paper explores how a blockchain-based decentralized identity management system can draw on the SSI framework to provide high-level security and transparency for all involved parties in public transportation ecosystems. Accordingly, building on analyses of the existing public transportation ticketing solutions, we elicited requirements of a comparable system based on the SSI principles. Next, we developed a low-fidelity prototype to showcase how passengers can utilize standardized travel credentials that are valid across different transportation networks in Europe. The proposed system eliminates the need for multiple travel cards (i.e., one for each transportation provider) and empowers individuals to have better control over the use of their identities while they utilize interoperable ticketing systems across Europe. Overall, building on the public transportation case, we offer a proof-of-concept that shows how individuals can better manage their identity credentials via the SSI framework.

1. Introduction

Over the years, the internet has become a driver of change that has brought about a fundamental shift in everyday life throughout society. The internet, which started as an open and decentralized communication network, has evolved into a backbone of countless applications that propel and bolster globalization and interconnectivity. The ripple effect of internet-driven disruption is evident in virtually any industry sector, including the transportation and mobility industry. We have witnessed the rise of Intelligent Transport Systems (ITS) that allow for improved transportation and traffic management systems in and around cities while lowering traffic congestion and CO_2 emissions.

The importance of transportation and traffic management systems to society is underscored by Goal 11 of the United Nations′ Sustainable Development Goals[1], which recognizes the need for more sustainable cities, including the need for improved public transportation options. Subsequently, the increased attention to transportation and mobility has stimulated the emergence of new sustainable transportation concepts such as Mobility as a Service [1], where different types of mobility modes are integrated into a single service. This concept includes, for example, ride-sharing, public transportation, and ride-hailing services such as Uber. However, these offerings seem to function as isolated services that do not offer platform interoperability. For example, public transportation systems in cities are notoriously highly isolated. In particular, the ticketing systems are dependent on a single transportation operator that is linked to the city or country. This fragmentation prompted the European Union to envision a smart ticketing solution that offers interoperability between public transportation authorities across Europe by 2050 [2].

* Corresponding author.
E-mail address: michel@avital.net (M. Avital).

[1] https://sdgs.un.org/goals.

https://doi.org/10.1016/j.bcra.2021.100014
Received 15 August 2020; Received in revised form 1 April 2021; Accepted 7 May 2021

This smart ticketing solution should allow users to have a single entry point into any public transportation system within Europe.

The current public transportation landscape is highly fragmented due to the prevailing variety of different solutions, pricing models, languages, and data formats. Some systems offer integrated solutions for different transportation modes within a country, whereas other systems only work within a specific network of a city or region. The ticketing solutions range from paper tickets and smart cards to account-based billing. One of the main challenges of this fragmentation is the management of user accounts across independent public transportation systems. Issues like data integrity, data privacy, and data ownership are important considerations if we aspire to a pan-European or even global transportation system.

Moreover, the internet is a double-edged sword that offers easy data exchange and connectivity at the increased risk of compromising confidential data. However, in combination with technologies like blockchain, the internet allows for maintaining data integrity and data ownership across a network of stakeholders. Blockchain systems are known for high transparency, which is important when dealing with multiple stakeholders such as the different transportation authorities. However, the use of any service requires an account management system that allows users to access and manage their data. In public transportation, for example, accounts can be used to manage account balances, ride histories, or user settings. Thus, public transportation providers can allow users to manage their accounts while also creating the best possible user experience.

Usually, identity management systems are hosted in centralized databases that are controlled and managed by the service-providing authority. However, organizations such as the World Wide Web Consortium (W3C) have been working on new concepts and standards for decentralized identity solutions. The decentralized identifiers allow for linking users with their associated data without relying on third parties. Thus, users not only gain more control over their data but also gain overall sovereignty from the existing centralized systems, which inherently expose them to risks of data breaches and misuse. The ability to own and control one's private data is one of the core principles of self-sovereign identity, and these fundamentals are also rooted in the concept of blockchain technology. A unified identity management system for public transportation in Europe must involve many stakeholders from different countries. Such a system will generate sensitive user data through ride histories, GPS locations, account balances, and other account-related personal information, thus exposing users to many new data risks potentially handled by a variety of publicly and privately held transportation companies. This raises the overall question of what such an identity management system for the public transport sector could look or be like.

The ITS Directive 2010/40/EU[2] of the European Commission outlines the goal of establishing a Europe-wide public transportation system that allows for seamless door-to-door mobility within and across member states. It provides a foundation for deploying an interoperable public transportation system by 2050 [2]. The envisioned ecosystem, which comprises a variety of independently-controlled public transportation systems, poses many technical challenges. Thus, promoting the development of a Single European Transport Area requires a thorough examination of the possible technical solutions. Moreover, the various types of implementations of public transportation networks in Europe lead to many challenges concerning cross-system data handling, like fare management. These challenges require a suitable solution that allows for cross-platform identity management.

A cross-platform solution requires establishing a trustworthy and transparent identity management system that can serve the many different stakeholders in the network. Naturally, this requirement opens the sector to a blockchain-based solution that enables trust between each stakeholder and aims at creating an interoperable system with a transparent accounting mechanism for each entity. Thus, the resulting solution needs to provide data privacy and trust for all the different entities in the blockchain network. Moreover, the need for high data privacy and trust between those systems needs to be considered to minimize fraud. As sensitive user data, such as ride history and personal information, will be aggregated, users should be in full control of how their data is being used. This relates to the idea of Self-sovereign Identity (SSI), which is gaining popularity within the identity space. When we examine current system implementations and the goal of a Single European Transport Area, we can observe that there is a research gap with regard to designing a feasible identity solution aligned with emerging SSI standards in identity management and blockchain technology. In this vein, we explore the following research question in this paper.

> *How can self-sovereign identity management be designed for a public transportation sector that spans different countries?*

To answer the above research question, we will first explore how users can be given full control over the management of their own identities and then explore how blockchain provides support for a decentralized identity management system via the use-case of self-sovereign identity management in the context of the public transportation sector. Finally, we will also explore the key requirements (both functional and non-functional) for such a system and test them by building a prototype. The rest of the paper is organized as follows. Section 2 presents the theoretical background of the underlying concepts. Section 3 reviews the prevailing blockchain-based SSI management systems. Next, section 4 briefly explains the research method. Section 5 then describes the use-case of self-sovereign identity in the context of public transportation. This section considers how blockchain-based decentralized identity management conforming to self-sovereign identity principles could help to achieve interoperability across different public transportation authorities. Finally, section 6 discusses the implications of the proposed system, and section 7 concludes the paper.

2. Theoretical background

In this section, we first review the fundamentals of identity types and management and then describe how blockchain technology can support identity management.

A plethora of research has focused on the notion of identity in different research areas of the social sciences, such as psychology, social psychology, and information systems (IS). The concept of identity in information systems has been studied at both the individual and the collective level [3,4], which is different from electronic identity [5] or digital identity [6]. At the collective level, Tajfel and Turner [7] proposed social identity theory, which is mainly focused on studying how identity arises from interactions and memberships among social groups. At the individual level, identity, role-identity, and identity control are prominent theories that explain how the roles and relationships of individuals within the networks influence their relational and personal identities [4].

In parallel to the notion of identity in psychology, researchers in IS have studied the management of digital identities for the purpose of embracing transactions in the digital space among citizens, businesses, and governments. Governments at both the local and the national level have invested heavily in implementing electronic identities (e-ID) and identity management technologies to ensure trust between service providers and clients or service consumers [5]. However, an editorial on identity and identification in the *European Journal of Information Systems* [6] pointed out that the research on identity in the IS field is sporadic and limited to organizational identity, practices, and organizational learning and knowledge work. In this paper, we focus on digital identity at the individual level and digital identity management that is used by multiple stakeholders in a decentralized and distributed manner.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040&amp;from=EN.

2.1. Identity types

According to Windley [8], digital identity management is the concept of managing records of different identities. Such management can include, for example, creating, managing, using and destroying records linked to a specific identity (e.g., the real name of the represented agent). The external agents represented by digital identities include not only individual persons but also devices, organizations, and applications. Thus, digital identity management is the overall layer that handles permissions and authorizations to execute certain tasks within a system. Whoever controls a digital identity has access to certain actions within a closed system that are defined by rules and permissions encoded into the digital identity. Thus, security and access management are crucial tasks of any identity management system [8]. These identity holders usually get access to their identities through credentials which they can use to authorize various tasks. Moreover, digital identity systems are becoming more complex since they need to provide access to an increasingly heterogeneous technology environment. Thus, digital identity systems are moving from centralized systems to more federated or even decentralized solutions. According to Christopher Allen [9], decentralized identity systems offer the benefit of increased portability and user control across different applications. Digital identities can be sorted into four classes: centralized, federated, user-centric and self-sovereign [9,10], which can be categorized along the dimensions of user control (how much control users have over their own identities) and portability (how easily an identity can be reused across systems or applications).

Centralized identities are issued by a centralized authority where the access to a user identity is issued and controlled by an underlying authority or third-party company (e.g., an online service provider like Amazon), generally for a specific purpose [11]. In general, centralized identities give more power to the issuing authority than the users associated with the identities. Centralized identity systems also lead to balkanization of identities, as many websites and online services force users to create separate identities, resulting in data silos that give less control to users and more control to the website or service. Such third-party services are not in the best interest of users because they have no binding commitment for service continuity and they can easily block users from using their own data without due process [12].

Federated identities can be used across multiple IT services or even across multiple organizations, allowing users to log in using the same credentials to different services that form a federation. For example, users can use their Google account credentials to log in to YouTube and other applications, as they share a federated identity across multiple services (popularly known as single-sign-on, or SSO). However, federated identity management is usually referred to as a circle of trust, where identity providers never share user credentials with external service providers [12]. Although federated identity may be offer users with convenience, the control is still with the identity provider.

User-centric identities are designed to delegate to the users more control their digital identity. In this approach, users are able to maintain and manage their digital identities independently using digital identity services such as OpenID [13] or OAuth [14]. User-centric identities require users to grant permission to a designated service provider that can verify their identity to third parties without disclosing any confidential information. For example, the "Login with Facebook" feature allows people with a Facebook account to verify their identity to any third-party that integrates this feature without exposing their identity credentials. However, while user-centric identities improve the portability of an identity, they do not give users full control over it. Thus, if users are, for example, banned by a designated identity provider, such as Facebook, they also lose access to any related third-party application that they have been using. Although user-centric identity is intended to provide more control to users, the ownership and control over the user identities remain with the designated identity providers [9].

Self-sovereign identity (SSI) is designed to provide users with full control of their respective identities. In contrast to other systems that require users to rely on a designated identity provider, SSI is autonomous and decoupled from any centralized services that can block, alter, or delete the identity credentials [15]. The ten common guiding principles for an SSI are listed in Table 1 along the dimensions of security, controllability, and portability [9,10]. However, these are only guiding principles and not hard requirements. While there is no clear consensus yet regarding the definition of an SSI, it is widely acceptable that identity becomes self-sovereign if a user has full control over it and if establishing the identity does not rely on a centralized system. Thus, moving towards a decentralized identity management solution where no central institution holds control over it would pave the way to an SSI system. Subsequently, in addition to Allen's ten principles for self-sovereign identity, Toth and Anderson-Priddy [16] proposed the following complementary considerations for designing systems: 1) Usability, 2) Counterfeit prevention, 3) Identity verification, 4) Identity assurance and 5) Secure transactions. Overall, these principles are helpful in evaluating systems that implement SSI including scenarios in which users lose their digital identities.

2.2. Identity management ecosystem

Identity management is a central concept in the context of managing access rights and authentication of services. The prevailing online identity management systems comprise three principal roles: identity owner, identity provider and service provider. Identity owners are those who receive credentials from different services. The wallet software that stores the credentials of the owner's identity may also contain further personal information about the identity owner. The identity owner could present the full credentials set, parts thereof, or even combinations of multiple credentials as proofs to service providers. The credentials can be entirely or selectively disclosed, and therefore the identity owners have full control over how their data are used and what is shared. An identity provider is a trusted system that manages identities on behalf of an entity and provides authentication and authorization for external service

Table 1
Guiding principles for a self-sovereign identity.

Principle	Description
Security Dimension	
Protection	The freedom and rights of individual users are the top priority.
Persistence	User identities must persist as long as the user wishes. Even if the underlying data (such as public and private keys) change, the user identity must remain the same.
Minimization	Disclosure of the user data should be minimal, and only the necessary data to verify a claim should be exposed.
Controllability Dimension	
Existence	An identity must be linked to a real person outside the digital world. Thus, users must have an independent existence outside the digital world.
Control	The users should have full control and ultimate authority over their identities and the privacy settings of their identities.
Consent	The sharing of data can only happen when a user provides consent.
Portability Dimension	
Interoperability	Identities should be able to work with any type of system and be available globally without losing user control.
Transparency	The system that operates and manages identities needs to be fully transparent.
Access	A user needs to be able to access all claims and data related to his or her identity.
Portability	Identities cannot be held by a single entity and must be transportable to any other type of system.

providers when requested. Thus, identity providers act as third parties that are responsible for a seamless exchange of credentials in order to authenticate users with services that are integrated within the ecosystem. Service providers are those who verify identities in order to provide a specific service. Many service providers are at the same time also issuers, as many services use their proprietary identity management system and databases to authenticate and onboard new users [8]. Finally, Know Your Customer (KYC) processes describe due diligence processes, often used in the banking sector, that facilitate the onboarding of new customers. This process is initiated when a customer intends to work with a financial institution. It includes the exchange of documents between parties and the collection of bare bones identity information of the beneficiary. Due to the growth of technology and regulations, the domain of KYC is undergoing fundamental changes that rely on distributed ledger technology (DLT). This provides more cost-efficient and faster identity verification processes when onboarding new customers [17].

2.3. Blockchain technology in identity management

Even though awareness of blockchain technology is widespread due to the rising popularity of the cryptocurrency Bitcoin, for the last few years, it has been the testing ground for countless new applications. Thus, many applications that use blockchain technology are built around trust-related issues, as blockchain technology can enable trustless networks. Through its inherent technology, blockchain can ensure that assets cannot be duplicated or double-spent even if the parties do not trust each other [18]. In general, identity management networks utilize blockchain technology to eliminate the need for any intermediary as an identity provider. For example, Sovrin facilitates a decentralized network to provide authentication services to identity holders [13]. Compared to a centralized federated identity system, a decentralized identity network cannot be shut down, use data without consent, or block users from using their identities. Therefore, controlling one's own data through cryptographic keys enforces the notion of controlling one's own identity. Thus, with regard to SSI, blockchain can be considered an important technology to give users control over their identities. Identities are linked to so-called decentralized identifiers (sometimes abbreviated as DIDs), which are created and stored on blockchains. These identifiers can be linked to certain documents and credentials, which users are able to control without the need for a third-party provider [19]. Moreover, interoperability between systems can be ensured, since users are not locked into one specific identity provider that is unwilling to integrate into services outside its own defined scope. This leads to an independent system that can be integrated by any service without any restrictions on content type, location or government [20].

Fig. 1 shows the main components of a DLT-based SSI system. Compared to a centralized identity management system, a distributed system relies on a shared ledger, which is validated and stored by several network nodes. The stored information belongs to different users, which in a decentralized identity system can be split into identity owners, service providers, and identity providers. However, user-sensitive information is stored off-chain and is not accessible to anyone other than the controlling entity. Therefore, storage can be off-chain or on-chain depending on the use case. On-chain storage is responsible for verification and revocation of claims and identities, whereas off-chain storage is used for static data like private data [21].

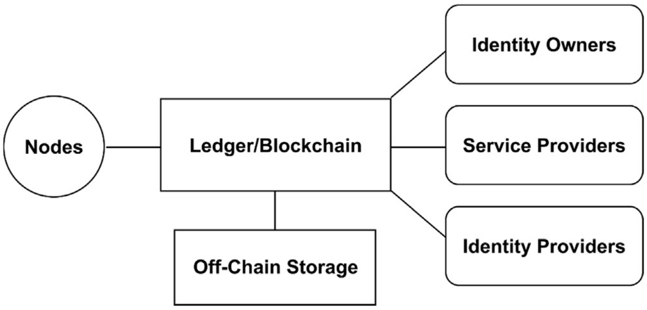


Fig. 1. Components of a blockchain-based self-sovereign identity system.

3. Blockchain-based SSI management system conceptualizations

In this section, we will first review blockchain-based SSI management systems and then review related research in blockchain-based public transportation.

3.1. Blockchain-based digital identity conceptualization

The research on blockchain-based identity has evolved during the last few years, but it is still nascent. Liu et al. [22] provided an extensive survey of blockchain-based identity management covering some of the current applications, such as Sovrin, uPort, ShoCard, and a comparison thereof using Cameron's law of identity [23]. Similarly, Bernabe et al. [24] provided a taxonomy of privacy-preserving techniques with a good overview of the various mechanisms, such as Secure Multiparty Computation and Zero-Knowledge Proofs. Their research also elaborated on how these privacy-preserving techniques could be used as part of SSI models for blockchain-based applications. Furthermore, Kuperberg [25] reviewed blockchain-based identity management systems from an enterprise and ecosystem perspective and evaluated various identity management systems from three perspectives: a) compliance and liability b) end-user experience and c) technological, implementation, integration, and operations criteria. Their evaluation found that none of the current blockchain-based identity management systems satisfy the requirements of their evaluation criteria. Most of the systems lack standard compliant interfaces, such as OAuth and SAML tokens.

Another stream of research focused on using blockchain-based digital identities in various application domains. The healthcare sector is one of the domains that seek to use blockchain and DLT technology for addressing the challenges of healthcare sectors, especially for secure data sharing of medical data and using self-sovereign patient identities. Zheng et al. [26] explored how DLT technologies like IOTA can be combined with Internet of Things (IoT) and wearable devices for secure sharing of healthcare data by building and validating a prototype. Another study by Alsayed Kassem et al. [27] on personal data sharing explored using blockchain technology along with self-sovereign identities. The authors proposed a blockchain-based decentralized identity management system using Ethereum blockchain with smart contracts to manage access to the self-sovereign identities. The security analysis of their proposed decentralized identity management system revealed that it is possible to build a secure and robust identity management system that can overcome the shortcomings of centralized identity management systems. Moreover, Houtan et al. [28] explored the usage of blockchain technology for offering decentralized electronic and patient health records, especially by focusing on self-sovereign-based identities to give patients more control over their healthcare data. Similarly, Faber et al. [29] proposed a blockchain-based personal management system combined with identity management. Their proposed conceptual design pertains to personal data sharing rather than a decentralized identity management system based on SSI principles. A systematic literature review was conducted by Soltanisehat et al. [30] to identify the challenges of using blockchain technology in the healthcare domain by looking into the technical, temporal, and spatial aspects of blockchain-based applications in the healthcare domain.

Concerning the transportation and mobility sector, a new concept called Mobility-as-a-service was proposed to achieve unified access to transport services by bridging the gap between public and private transport operators using a single digital platform [31]. Blockchain and DLT technologies have also been explored to offer open platforms focusing on mobility as a service. Bothos et al. [32] examined how blockchain technology can be used for seamless integration of different transport providers and other stakeholders to enable unified mobility for travelers. Under the smart cities and smart communities initiative, Bhushan et al. [33] surveyed the usefulness of blockchain technology in transport, smart grid and other sectors, then outlined some of the research challenges for enabling and developing decentralized applications for the advancement of various application domains. Furthermore, authentication and identity management using blockchain-based technologies have also been explored in wireless mobile networks as an alternative approach to the centralized management of identity information with the network operator. Xu et al. [34] proposed a self-sovereign based identity and authentication scheme for managing user identities in wireless mobile networks using a particular type of blockchain—redactable blockchain. Redactable blockchain [35,36] allows the blockchain to be redactable by allowing the following actions: 1) rewriting of blocks (e.g., to remove inappropriate content from blocks in a controlled and GDPR-compliant manner); 2) compressing blocks into a smaller number of blocks for efficiency purposes; and 3) inserting one or more blocks by using a new type of hash function (chameleon hash function). The performance evaluation presented in Xu et al. [34] shows that their proposed self-sovereign-based identity scheme can reduce network access delays in addition to reducing storage overhead.

In addition to the above-mentioned research on identity and identity management systems, there are explicit calls that suggest blockchain technology to enhance the security of public digital identity systems [37,38], especially to gain anonymity and pseudo-anonymity [39]. The research so far has focused on improving the Public Digital Identity System by preventing information leakage through the employment of various anonymity schemes, including the native pseudo-anonymity of blockchain, to support applications that need to be identity-aware. Moreover, Buccafurri et al. [38] used identity-based encryption to link the notion of identity with a role by allowing a direct link between asymmetric cryptographic keys (private and public keys) to the identity of the user who signs the transactions. As part of the Identity-based encryption, they used the private keys generator technique to allow a third party to generate a public key based on an identity value. A trusted third party can then generate a private key corresponding to the public key. For this to be feasible, a setup is needed in which public master key is published by the trusted third party while the corresponding master private key is kept securely with the trusted third party.

3.1.1. *Comparing the proposed system with current research*

The proposed system in this paper focuses on using self-sovereign identities and decentralized technologies such as blockchain in the context of transportation management. Specifically, the proposed system is designed to offer a unified and interoperable identity management solution that can be adopted by different public transportation providers that are spread across multiple jurisdictions. Therefore, the proposed system comes under Mobility-as-a-service to a certain extent and thus relates to Bothos et al.'s [32] discussion of the role of blockchain technology for enabling Mobility-as-a-service. However, we used an engineering approach to derive the requirements of a self-sovereign-based identity management system for the transportation sector and validated them by building a simple prototype application modeling the bare bones use cases. Similarly, the proposed system is also related to the research on using blockchain for digital identities and self-sovereign-based identities [24,27,28]. In the above-cited studies, the focus was on data sharing in healthcare and other related sectors; however, this paper focuses on the transportation sector. Specifically, we aim to draft the specifications for a unified and interoperable public transportation system that spans multiple countries in Europe.

3.2. *Blockchain-based SSI management systems*

Next, we present four solutions—those of Sovrin, uPort, Civic, and Namecoin—which have used blockchain technology to develop SSI systems (or, more specifically, a blockchain-based system that resides at the application layer).

3.2.1. *Sovrin*

Sovrin[3] Foundation is a private non-profit entity that aims to standardize and create an infrastructure for SSI by utilizing its proprietary blockchain, called Sovrin public ledger, based on Hyperledger's Indy. Sovrin uses a consensus algorithm called Plenum, that is responsible for validating new transactions [10]. The SSI model of Sovrin is independent of any available distributed ledger, but it has the flexibility to work with any blockchain that satisfies the fundamental principles. Sovrin utilizes a public permissioned blockchain using nodes also known as Stewards to achieve a global consensus. It also provides functionality for issuing and managing credentials in a privacy-preserving way by generating Zero-Knowledge Proofs. Sovrin's public-permissioned ledger requires a governing body to approve the participating nodes in a trusted way depending on the reputation of the Stewards (Protection). Although the Sovrin foundation has power over the ledger, user attributes are not shared with Stewards and administrators without the consent of the identity owners (Consent). All the private information is encrypted by the identity owners' keys, thereby giving the users full control over their identity. It can also be deployed on any distributed ledger that meets the requirements, making it interoperable with other ledgers (Interoperability). Selective disclosure of verifiable claims based on Zero-Knowledge Proofs is provided by Sovrin decentralized identifiers and public keys (Minimization). Users' private data are stored on their device or a selected Agent and do not reside in any of the system's databases (Access). Also, a Sovrin agent can enable secure messaging between the clients and maintain an encrypted backup of private storage by utilizing local containers (Persistence). The only way to unlock the users' identity is by using their key pair, which enables everything else in the system (Control). Portability of data can be ensured to some extent by utilizing system-independent data formats like JSON-LD.

3.2.2. *uPort*

uPort[4] is a decentralized identity system that supports the SSI model and is built on top of the Ethereum platform [40]. It comprises a mobile app and several Ethereum contracts, including a public registry of uPort identity. The uPort mobile app generates a key pair that allows a user to create, update and share identity information with other users. On the backend, three smart contracts are utilized to control the users' data. The bulk of identity data is stored on a distributed file system (IPFS), while the corresponding private key of a uPort identity is stored on the mobile app. The public registry is used to create a correlation between IPFS data and a uPort identifier. uPort allows users to create, update and control their identity (Control) and also share personal information with third parties at their discretion (Consent). The core identity is stored on the Ethereum Blockchain and therefore replicated and stored on several computers worldwide (Persistence). The private information is stored on the users' devices as well as off-chain with IPFS, which makes it always accessible by the users (Access). However, uPort is only partly decentralized due to having few centralized elements in their architecture. The application manager allows developers to create and manage identities for their applications (Portability).

3.2.3. *Civic*

Civic[5] is a blockchain-based ecosystem that is designed to facilitate low-cost access to identity verification and KYC processes. Civic utilizes the Ethereum blockchain and has created an ERC20 token called CVC that is stored in an Ethereum wallet. The token is used to reward and pay for services in the ecosystem, and it has a fixed supply. Identity

[3] https://sovrin.org/.

[4] https://www.uport.me/.

[5] https://www.civic.com/.

information is stored on the user's device, and Civic receives only hashes of the data, which are stored on the blockchain [41]. Since the identity information is stored on the user's device (Control), it is always accessible to the user (Access). Although the network is likely to be available in the foreseeable future, the actual data storage lifespan depends entirely on the user (Persistence). Applications connected to the Civic ecosystem can use the identity information (Protection), although the information cannot be ported to any other devices. Civic, among others, can provide claimed and verified identity attributes for all types of services and password-less login (Interoperability). Since all the information is stored on the user's device, the Identity Owner selects what information to share and with whom (Consent). The user decides what information to reveal, and this information is stored with hashes in a Merkle tree (Minimization).

3.2.4. Namecoin

Along similar lines, Namecoin[6] is an open-source decentralized framework for the management of decentralized identities and decentralized domain-specific names. It is built on the Bitcoin network as an altcoin and primarily focused on supporting free speech and the fight against censorship. If someone wants to use their identity or a domain-specific name on Namecoin, then he or she needs to acquire Namecoins to register and update names or identities. These Namecoins can be purchased in decentralized exchanges like Bitcoins. However, Namecoin also offers wallet services, which can be used to store Namecoins and perform operations on the names and identities.

3.2.5. Existing standards SAML and XACML

In the context of industrial applications on authentication and authorization, there are two primary standards: SAML[7] and XACML[8] for the specification of authentication, authorization and policy-based access control mechanisms. The current SAML standard refers to version 2.0 of Security Assertion Markup Language, which is mainly meant for exchanging of security information between different online service providers. The SAML standard primarily operates using security tokens, which contain assertions about the user profiles and their authorization to access various web resources. Along similar lines, XACML refers to version 3 of eXtensible Access Control Markup Language, which is a standard introduced in 2017 for defining fine-grained access controls using attributes for defining the security policies. However, both these standards are mainly XML-based languages, are consistent with each other, and are used as part of cross-domain single-sign-on authentication applications. These standards can only be used to define fine-grained access controls when an identity management system is already developed and in place. Moreover, these standards are primarily aligned with federated identity systems, and their utility for the decentralized identity management systems still needs to be explored.

3.2.6. Comparison of the proposed design with existing systems

As discussed previously, the ten principles that SSI represent an ideal system for building an SSI-based identity management system. In this section, these principles will be used as criteria in comparing the current blockchain-based systems for SSI with the proposed conceptual design for a blockchain-based decentralized identity management system.

All four SSI systems—namely, Sovrin, uPort, Civic, and Namecoin—provide the identity owner with full control over his or her identity and the ability to disclose claims and attributes selectively. They all also offer portability and persistence to a limited extent by utilizing established data formats and self-hosting of data. More specifically, uPort utilizes IPFS (InterPlanetary File System, a distributed file system) for storage, while storage and backup are facilitated by Sovrin with trusted network Agents. In the case of uPort and Civic, both of the systems store the identity information on the user device by using blockchain for verified and signed hashes of the data. Although these systems leverage decentralization to a limited extent, none of them is entirely decentralized. For example, Sovrin is running on a Hyperledger blockchain, and its consensus algorithm is based on approved nodes (also known as Stewards), which are run by organizations interested in maintaining the network health. In addition, Civic utilizes the verification providers and validators to verify the identity information of the users, therefore their role is centralized in the ecosystem. Similarly, Namecoin is also built on the network of Bitcoin, which makes it inherently bound to the underlying limitations of bitcoin, such as proof of work, network latency and other issues. Moreover, identity owners who want to use Namecoin for maintaining their identity need to buy Namecoins, which is an inherent built-in cost for the systems that use Namecoin as an identity provider. The portability of the identities that use Namecoins might also be an issue to consider. Moreover, other blockchain-based digital identity schemes such as identity-based encryption assume that there exists a setup of a trusted-third party provider. The primary role of this trusted-third party is to maintain the master private key securely so that any other party can generate a public key based on the identity value, which is a limitation for a fully decentralized identity management system.

This paper focuses primarily on examining blockchain-based decentralized identity management conforming to the SSI principles, especially in the context of public transportation, mainly aiming at offering interoperability among different transport service providers that spread across many countries. As described in the next section, the proposed conceptual design is based on decentralized identifiers and standard schemas defined by the respective stakeholders to generate credentials for an identity owner. These credentials can be shared between different stakeholders for the validation of transactions and claims (such as a student registered in a university gets discounted travel) made by the identity owner. Moreover, the proposed conceptual design for a decentralized identity management system took into consideration the requirements from different stakeholders that are involved in the decentralized identity management with the help of use-case scenarios. The feasibility of these requirements in sharing credentials among different stakeholders is validated by developing a simple prototype.

4. Research design

In this paper, we aim to elicit the requirements for and provide a conceptual design of a blockchain-based decentralized SSI management system that can be used for a pan-European public transportation system. We draw on the applied design science research approach [42] to identify the opportunities, define the objectives, elicit the requirements, and design a conceptual framework for the envisioned system.

We first identify the specific research problem and justify the value of the solution. In a second step, we define the objectives of the solution and knowledge of what is possible and feasible. The next step is concerned with designing and developing artifacts as well as evaluating how well the artifacts support the proposed solution [43–45]. The design science research process is based on three research cycles. The Relevance Cycle connects the requirements from the contextual environment of the research project with design science activities [46]. The Rigor Cycle links the design science activities to grounding theories and methods. It incorporates new knowledge into the knowledge base of scientific foundations, domain experience and expertise generated by the research. The Design Cycle loops over the core activities of developing and evaluating the produced artifacts and processes of the research [44,46].

Sonnenberg and vom Brocke [47] suggest that each design science research activity, including identification, design, construction, and use, shall be followed by an evaluation activity [44]. In a design science

[6] https://www.namecoin.org/.

[7] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[8] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

research process, an evaluation activity can occur ex-ante (i.e., before an artifact is constructed) or ex-post (i.e., after an artifact is constructed) [47]. The evaluation helps in demonstrating the utility and quality of the designed artifact. Though there are different evaluation methods, we used informed arguments as the descriptive evaluation method [48].

Collecting ex-ante feedback from external stakeholders like industry experts or potential end-users would not have been effective given the technological immaturity of decentralized systems and the unfamiliarity of the stakeholders with it. However, their ex-post feedback from interviews and user testing following the first design cycle could have been potentially incorporated into the final artifact.

Design science research projects typically are characterized by either more product-centric approaches or more process-oriented approaches [49]. In this project, a product-centric approach was followed to address the underlying objective—developing and testing a solution that facilitates digital identity management for public transportation providers. Furthermore, this paper places a greater focus on the usefulness of the situated artifact over its theoretical characteristics, since the latter has already been addressed in pertinent studies. Moreover, deductive or "theory-first" design science research is another approach to ensure that the solution fits the requirements [49]. Finally, this paper opens up new research possibilities based on the produced artifact that outlines an initial version of a self-sovereign decentralized identity management service that can be integrated into different systems that span across multiple jurisdictions.

5. Self-sovereign identity in public transportation

This section focuses on identifying the system objectives and requirements for a decentralized identity management system that can be implemented in the public transportation sector based on blockchain and SSI principles. The objectives are extracted from current implementations of identity management systems as well as requirements that can be derived from specific interactions and relationships between different stakeholders in the public transportation sector. Here decentralized identity concepts like Decentralized Identifiers, schemas, credentials, and the overall identity verification process are modeled in the context of public transportation.

5.1. Business context

The idea of a Single European Transport Area was first proposed in a white paper by the European Commission [50] to ease the movement of citizens and freight while making European transport more sustainable. According to the ITS Expert Group [2], one of the key issues to investigate is the concept of smart ticketing solutions, which provide a seamless ticketing experience for end-users and also covering multimodal transport fares. Smart ticketing solutions allow for the interoperability of fares and ticketing systems between different transportation providers. Several implementation options exist for smart ticketing solutions. One of these is smart ticketing based on secure identity and back-office processing. This option raises concerns about how user data is processed and how users are authenticated to use the system, thus emphasizing the need for trustworthy and secure data processing across different transportation systems.

Similarly, several initiatives promote cross-national travel using rail travel passes that allow people to travel across Europe. The Interrail, which was introduced in 1972, allows unlimited travel for a month across 30 countries in Europe [51]. Even though Interrail has been quite popular and served as a unified pass for travel across many countries in Europe, it has some intrinsic challenges. As pointed out by Jensen et al. [51], even though interrail tries to serve as "transport 'key' to a borderless Europe", it failed to assume such a status due to some inherent obstacles in the pan-European transportation system. For example, the existence of several operating systems and management systems hosted by the individual transport providers, transport zones of rail Europe, and the privatization of transport sectors. In addition, even in the interrail/Eurail pass, maintaining transparently the user-identity and user-credentials is a significant challenge as it lacks unified and interoperable identity management that is accepted by all the different public transportation providers across multiple jurisdictions.

5.2. System objectives and requirements

An inherent objective of a pan-European transportation ticketing system is its ability to take care of the different types of stakeholders, including their requirements, relationships and concerns, by using decentralized identity management. These relationships will form the foundation for trust among the various stakeholders of the system and ensure a seamless travel experience between different public transportation systems across Europe.

5.2.1. Stakeholders

The stakeholders involved in public transportation using decentralized identity management include 1) public transportation authorities and 2) passengers, public and private institutions, identity owners, and identity providers. Public transportation authorities provide access to specific transportation modes and are responsible for issuing and verifying tickets. They are considered the service-providing authority that is continuously requesting access rights from users to provide transportation services. Moreover, they also act as trusted partners in any country. They can issue certain types of verifiable credentials to users within the system—for example, eligibility for discounted fares for youth and students. Passengers, in turn, are the service-seeking entities who use their credentials to authenticate themselves to a public transportation authority. In the current system, passengers act as identity owners.

In addition to public transportation providers who request credentials from the users, we have also included public and private institutions into the prototype implementation with a key focus on providing verifiable attestations into the model. For example, a public institution like a university will issue a verifiable attestation saying that a student is currently enrolled at the university. Hence, a certain passenger is eligible for a student discount. Similarly, a private institution like a bank can issue a verifiable attestation saying that a student has a sufficient account balance, e.g., to purchase a ticket. Along these lines, public and private institutions are all stakeholders that can issue verifiable credentials, which attest to specific user attributes like age and student status, and thus institutions act as Identity Providers. For example, universities are responsible for providing attestations of student enrollment that can be used to claim discount fares on public transportation. Moreover, the stakeholders also include institutions, such as governments that issue national identities and banks that can attest to payment liquidity, which qualify users to pay for services.

A domain-specific trust framework must be established to institute trust between the different verifiers. For example, in order to function on a European level, each participating transport authority needs to know all the other respective authorities that provide similar services in the relevant countries. Here, the European Union Transportation Authority could act as a framework that pulls all domain-specific trust partners together. To ensure trust between stakeholders, it is important that each of them is uniquely identifiable in the system by using decentralized identifiers. These identifiers can be used to facilitate connections between the different stakeholders, which in turn can verify the credentials that were issued by each other.

5.2.2. General data protection regulation (GDPR) considerations

Personal data privacy through GDPR [52] is an important objective to be considered in the design of the system, as the system deals with personal information and therefore needs to account for privacy concerns and act in accordance with the guidelines of GDPR regulation. According to GDPR, any personal data of an individual shall be accessible by other entities only subject to the informed consent of the underlying person. In

Table 2
Schema registration by different entities.

Schema Designer	Credential Issuer	Purpose
European Transportation Authority	Public Transportation Provider (PTP)	Providing consistent proof to travel for users to enable seamless travel across different public transportation systems in Europe
European Banking Authority	Banking Provider (BP)	Providing consistent proof of liquidity for users to enable seamless pay for rides on public transportation across Europe
European Education Authority	University Office (UO)	Providing consistent proof of student status across European universities
National Government	National Office (NO)	Providing proof of national identity within a national jurisdiction

addition to this requirement, GDPR also strongly encourages to provide means that allow individuals to control and manage their given consent in a fine-grained manner. Consequently, a blockchain-based system can provide suitable functionality, such as smart contracts to grant and revoke consent, by recording such contracts on the ledger in an immutable fashion. Article 17 of GDPR, which states the right to erasure (or the so-called "right to be forgotten"), constitutes a major consideration for blockchain-based systems, as the blockchain maintains an immutable ledger. According to Article 17, any records of personal data owned by other entities shall be erased when requested by the subject. Therefore, the decentralized identity management system will not record any personal or other information that can identify the individuals explicitly on the blockchain. Alternatively, personal and other information that can identify the persons explicitly can be stored in off-chain storage repositories. Hash-pointers to the data storage location can be stored on the blockchain ledger, as suggested by Faber et al. [29], and using hash-pointers to the external data storage will make the process of storing data on the blockchain in compliance with GDPR. As the hash function is pre-image resistant, if the data are removed from the off-chain storage, there is no way to reconstruct the original data, such as personal information, using the hash pointers. Thus, it is GDPR-compliant to store only hash pointers to the personal information stored in off-chain repositories, as the right to be forgotten can be easily honored. To ensure secure peer-to-peer data exchange, the overall system's objective is to integrate with off-chain data storage solutions, such as cloud-based storage providers like Amazon Web Services and Microsoft Azure.

5.2.3. Schema registration

Schemas are an essential part of any decentralized identity system because they define the overall structure of credentials that allow users to issue and validate the system's credentials. In a broader sense, schemas should be created by an overarching authority (such as the European Transportation Authority) entrusted with defining a common structure for all the participants. For this reason, a fully functional system needs to maintain the schema definitions on the ledger so that they can be discovered and used by any participant. As shown in Table 2, three European agencies are responsible for registering a schema to achieve consistency across the system. These are the banking, education, and transportation industries that are currently managed at a European level. With regard to national identity, the system acknowledges the sovereignty of each state. Thus, each government is responsible for its schema design, which can be used by national institutions to issue their credential definitions on the ledger.

5.3. System functional and non-functional requirements

According to technical specifications of functional and non-functional requirements, the keywords used in the requirements are "MUST" and "SHOULD". More specifically, "MUST" keyword is used to indicate that the requirement is an absolute requirement, while "SHOULD" is used to describe an optional requirement that may not need to be fulfilled in the full implementation of the system, but the implications for choosing not to implement must be understood. As an example, the core functionalities of the system have been identified and are viewed as a MUST. Moreover, the requirements have been separated into functional requirements (FR) and non-functional requirements (NFR) [53].

5.3.1. Establishing a digital identity

The identity subjects need to be able to register an identifier in order to participate in the decentralized system. Thus, the Identity Owner needs to be in control of the identifier to ensure that data can be associated with a specific identifier.

- FR1: The system MUST allow any natural person to create a decentralized identifier.
- FR2: The system MUST allow the subject to create as many decentralized identifiers as needed.
- FR3: Users MUST be able to control their data associated with the corresponding identifier.
- NFR1: The system MUST provide a public-private key pair to the user.
- NFR2: The system MUST operate on a decentralized information system to issue identifiers.

5.3.2. Establishing relationships

Managing different relationships and interactions between stakeholders requires a way to establish connections between the actors. Thus, the system needs to provide a way to discover the users based on their decentralized identifiers to allow for a connection to be established. This ensures a secure data exchange without leaking data to any outside relationship.

- FR4: Users MUST be able to connect with each other using decentralized identifiers.
- FR5: Users SHOULD be able to accept and reject connections.
- NFR3: The system MUST support secure data exchanges.
- NFR4: The system SHOULD display relationships in a human-readable way.

5.3.3. Issuing credentials

In order to prove claims to other stakeholders, it needs to be possible to issue verifiable credentials or self-issued credentials.

- FR6: The system MUST allow entities to act as Identity Providers to issue verifiable claims to a subject.
- FR7: Users SHOULD be able to create self-issued credentials.
- FR8: Users SHOULD be able to approve and reject Verifiable Credentials.
- FR9: Users MUST be able to register Schema definitions in a non-programmable way.
- NFR5: The system MUST issue claims in a human-readable format with standard semantics.
- NFR6: The system SHOULD be able to integrate with external databases.

5.3.4. Credential management

Identity subjects need to have access to their credentials in order to manage them. The system should be able to connect to user-defined identity hubs so that it can securely access all issued credentials. Thus, data need to be stored in an encrypted form and decrypted on request by the identity subject.

- FR10: Users MUST be able to manage and store credentials securely.
- FR11: Users SHOULD be able to decide where to store credentials.
- FR12: Users SHOULD be able to revoke claims or attestations to claims that have been issued.
- NFR7: The system MUST enable data encryption.
- NFR8: The system MUST expose authentication methods with Identity Hubs and Registries.

5.3.5. Proving/asserting claims

In order to prove claims from certain credentials, the system needs to be able to ask the identity subject to give consent in order to share specific claims. Thus, the user always needs to be informed regarding what type of claims are requested by outside parties and what data is presented to the requested stakeholders. This aspect will increase the transparency of the system and aligns it with the overall principles of self-sovereign identity.

- FR11: Users MUST be able to prove claims.
- FR12: Users MUST be able to give consent to request proof of claim.
- FR13: Users MUST be able to request Verifiable Credentials.
- FR14: Users MUST be able to disclose requested data selectively.
- NFR9: The system MUST handle claims in a transparent manner.
- NFR10: The system SHOULD enable data minimization through Zero-Knowledge proofs.

5.4. User scenarios and use cases

For illustrative purposes, the following use cases involve stakeholders from a domestic country system that are required to apply for a travel credential. A university office, a banking provider, and a public transport provider are used to model a domestic system and thereby showcase the overall functionality of the system in a Europe-wide context. Any instance in the system such as a university office could be replaced through a stakeholder within the same institutional context. The following section describes two scenarios that might occur when a user engages with the system. The scenarios assume that the user who is the identity holder is already in control of his or her decentralized identity. Use cases are described using Unified Modeling Language (UML) to present how core functionalities could be facilitated in the system [54].

5.4.1. Scenario 1: Requesting travel credentials

After a student has gone through gathering all necessary base credentials to apply for a travel credential, she must approach their local transportation authority. If all the documents presented by the student are valid, then the student receives a travel credential that can be used for public transportation all over Europe at a discounted price. As shown in Fig. 2, the student and the Identity Provider (in this case, the transportation authority) establish a trusted relationship. The student presents a set of claims that are needed for successfully issuing the travel credential.

The identity provider then validates the correctness of the provided claims through cryptographic proofs. After the successful validation by the system that the transportation authority can issue a new credential, the travel credential will become an authoritative digital document like any other verifiable credential. Finally, the student stores the credential for future use in her digital wallet or Identity Hub.

5.4.2. Scenario 2: Using the travel credential across europe

After successfully obtaining a travel credential, suppose the student wants to travel from one European country to another and uses the card to travel from A to B via the metro. She uses her digital wallet and presents the travel credential to the validator machine, and it checks the validity of the credential. Following the verification, the validator calculates the student fees and passes them on to the digital wallet. This information can be treated as a transaction credential as well as a receipt for a specific journey, which entails price, location, and time after the check-in and check-out. In parallel to this process, a payment request is issued to the bank account, which is referenced in the travel credential. As shown in Fig. 3, the use case diagram depicts the process that occurs when the student uses her card. After establishing the trust relationship, the proof needs to be presented by the student through the system. After validating the proof issued by the service provider, another transportation authority can give access to the system. While providing access to the service, the system treats the service offered as a credential. This credential can be used as a receipt for a journey to prove to anyone else that a particular check-in or check-out has happened. Moreover, the system can engage with any off-chain solution to trigger additional events (e.g., a charging request).

5.5. Sequence diagrams

After defining the most important use cases in the system, a sequence

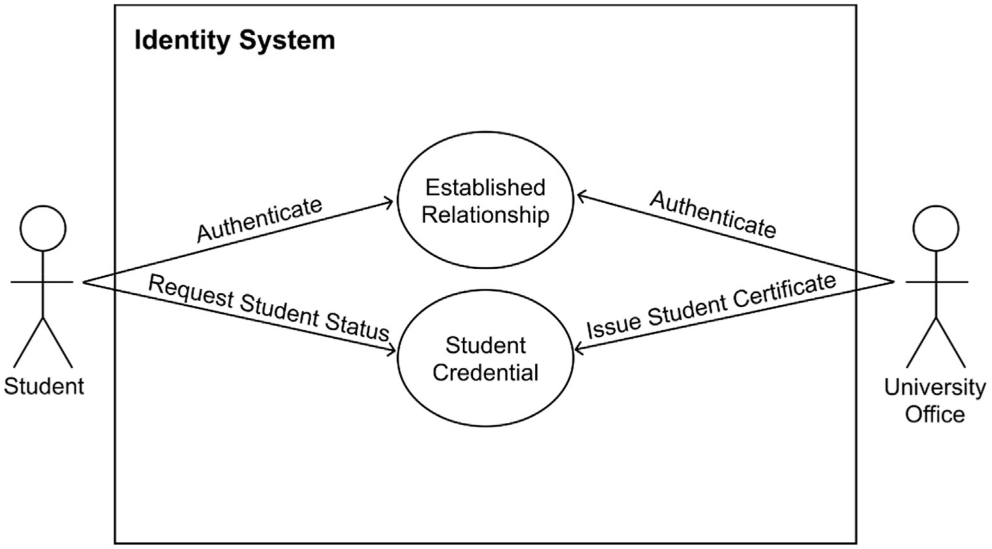


Fig. 2. Use-case diagram for requesting a discounted travel credential.

diagram can be designed to showcase the different interaction flows between the different stakeholders in the system. The interactions between stakeholders can be clustered as actions on a national and European level.

5.5.1. Sequence diagram 1: Travel credentials

The sequence diagram in Fig. 4 describes the process the user needs to go through to acquire all the necessary base credentials in order to satisfy the requirements of applying for a travel credential. The system assumes that the user first acquires a government ID. This happens through the attestation by the government, which is requested by the user. Following a successful attestation by the government, the user receives a government credential. The same process is used to request attestation for a university transcript at a university office or a bank account statement by a banking provider. Every time a new credential is issued, the user stores these credentials in a personal wallet, and these credentials are referred to as base credentials.

5.5.2. Sequence diagram 2: Using the travel credential to travel

As shown in Fig. 5, after receiving all the necessary credentials for applying for a travel credential, the users continue with the application process at the local transportation authority. Here the public transport provider asks the user to present the required attestations in order to issue a travel credential. After requesting the attestation, the user presents all three acquired attestations. These attestations are processed by the public transport provider and checked for validity through cryptographic proofs which are encoded inside the credential. After the proofs have been validated and confirmed, a travel credential is issued and is saved in the user's personal wallet. In the last step, the user uses the travel credential to travel to a European country (PTP2). The user presents the travel credential to the transport provider in the country where he intends to travel, then the transport provider validates the travel credential and allows the user to use the service. This is achieved through cryptographic proofs and the general understanding between the transportation service providers in Europe. Therefore, the validity and usage of travel credentials across borders can be ensured (see Fig. 6).

5.6. Prototype implementation

After outlining the overall system design of a decentralized identity application in the forms of requirement specifications, use cases and sequence diagrams, in this section, we outline how a simple prototype implementation can be developed to check the feasibility of a decentralized solution for identity management in the context of public transportation in Europe. As part of the prototype, a specially designed travel credential for the public transportation sector is defined and issued to passengers for their travel in European countries. We call this a Euro Mobility Card (EMC). The EMC allows passengers to travel across different public transportation systems in Europe, where the card replicates a verifiable credential that can be issued by any Public Transport Agency (PTA) in Europe. By providing this card, the traveler can prove that he or she is eligible for certain discounts and has sufficient bank liquidity to pay for transportation on the go. The EMC is a digital card that users can access from their mobile device and present whenever there is a need for proof of credentials. Such credentials can be requested programmatically by validator machines on entry/exit systems or by a manual request using ticket inspectors' handheld devices while traveling.

Table 3 describes the issuing and usage of the EMC, where each stakeholder is mapped to a real-world entity in the Danish context. In a decentralized system, the roles of certain stakeholders can overlap with each other when compared to the roles in any traditional identity management system (e.g., the roles of a service provider and issuer). This is because credentials are stored with the user by default, and thereby eliminating the need for any third party to act as the identity-providing authority. However, since there is a one-to-one validation process between the verifier and issuer, the issuer plays a role similar to an identity provider in a centralized system. Without the cryptographic proof encoded into the credential by the issuer, the validation process would not be possible without an intermediary.

Thus, the stakeholders within the system roles are not mutually exclusive, allowing certain stakeholders to play multiple roles. To create a secure communication channel between the two stakeholders, a relationship first needs to be formed. For this reason, each party creates and exchanges with its counterpart a unique pairwise decentralized identifier. The created pairwise identities are unique to the relationship and cannot be reused across other relationships. Depending on the design choice, the decentralized identifiers are either registered on the ledger or stored inside the wallet. In the developed prototype, the pairwise decentralized identifiers are registered on the ledger. Thus, a student forms relationships with all parties with which he wants to securely exchange information. In the prototype, the student establishes relationships with the government, Danske Bank, Copenhagen Business School (CBS), and Danske Statsbaner (DSB), which are four pairwise identifiers with a unique relationship. The creation of isolated identifiers for each relationship helps to defeat the correlation between the student and each stakeholder, thus increasing the level of privacy within the system and

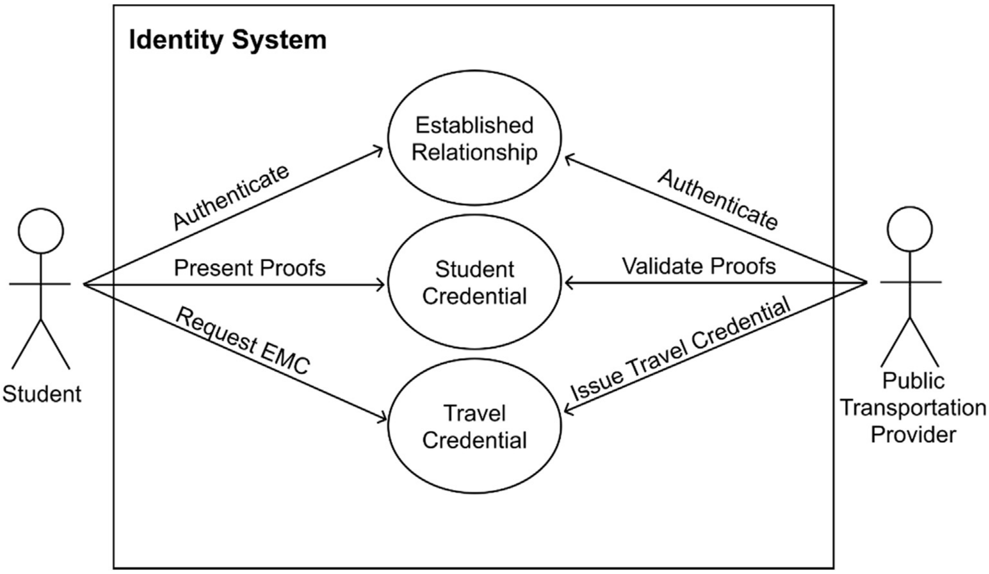


Fig. 3. Use-case diagram of requesting a discounted travel credential.

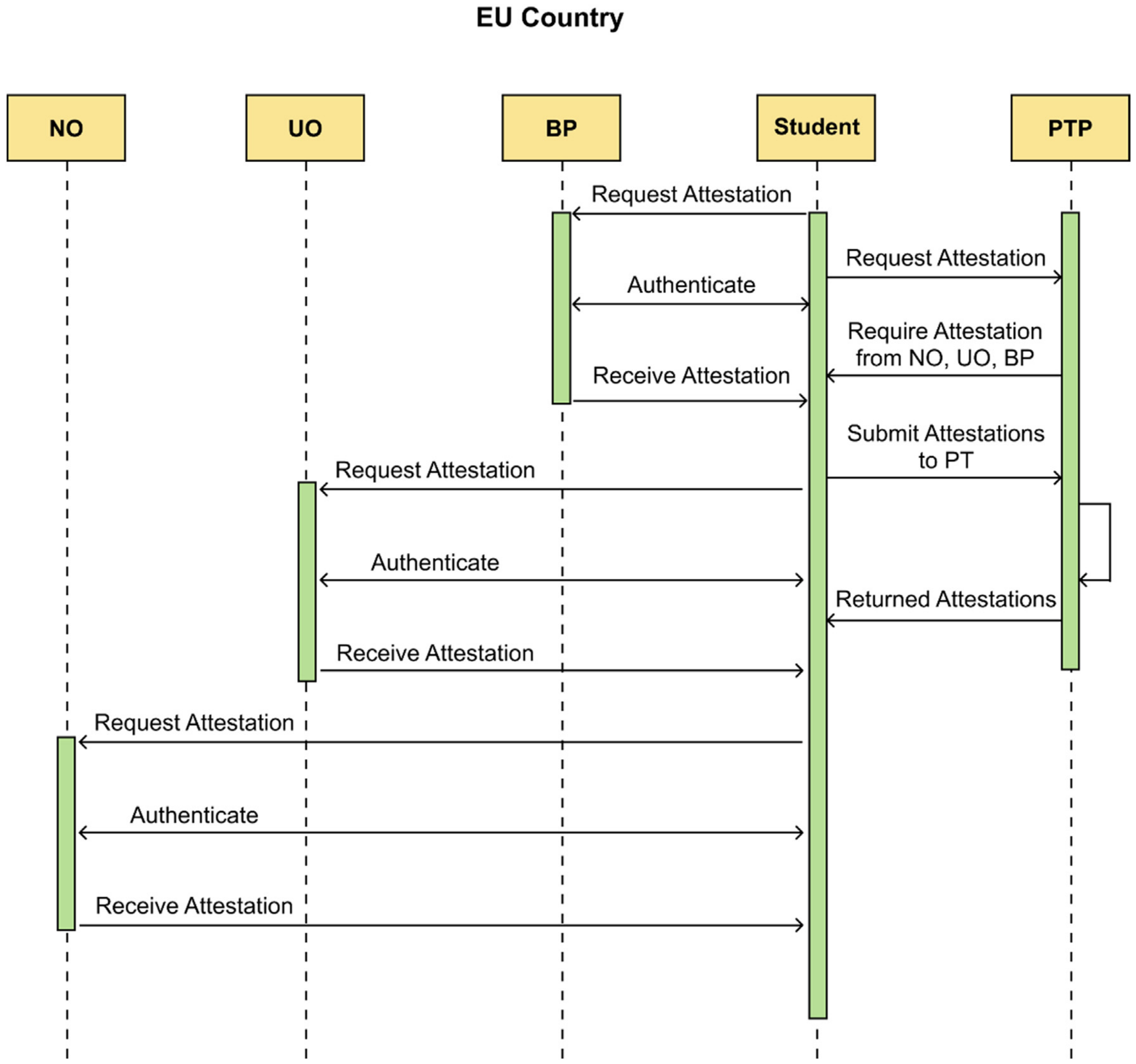


Fig. 4. Sequence diagram of base credentials between stakeholders: Public Transportation Provider (PTP), Banking Provider (BP), University Office (UO), and National Office (NO).

helping to create a multidimensional identity that is able to control multiple decentralized identifiers. Screenshots of the prototype implementation for a decentralized identity management showing various operations, such as sending relationship requests (Fig. A1), accepting relationship requests (Fig. A2), an overview of the accepted relationships (Fig. A3) are presented in the appendix.

5.6.1. *Schema definitions*

Schema design is an essential aspect of decentralized identity management and the identity management system allows for system-wide schema discovery and enables the different stakeholders to create their own schema definitions based on existing schema designs. This is particularly useful with regard to issuing the EMC from different transportation authorities in Europe. Fig. 7 presents schema definitions, where each schema has an overarching authority (e.g., transport, banking) to standardize the schema definitions. Moreover, the prototype assumes that a national government is responsible for its own identity card schema, which can vary on a European level. However, we assume that banking, transportation, and education can be overseen on a European level. For an authority to issue a schema definition to the ledger, the prototype allows for adding attributes through an input form. For example, the EMC schema could be added to the system by adding the following array to the input [“first_name”, “last_name”, “photo”, “is_student”, “card_number”, “bank_account”] and submitting the form. At the current stage, the prototype issues schema definitions on the ledger.

5.7. *Other business considerations and challenges*

This section explores various business considerations and the context under which the prototype can be extended further. First of all, we have used the train as the primary transportation mode in the prototype implementation. The train/rail is the primary public transportation mode used in the European region [55]. Moreover, many European countries already implemented an integrated multimodal single ticketing system at the national level that covers different transportation modes such as busses, metros, and ferries. Therefore, even though we have used the train as a public transportation mode explicitly in the prototype, handling multiple modes of transportations will not significantly change the prototype's design. Additionally, several country-level national public transportation providers such as Deutsche Bahn also offer international travel tickets that cover multiple countries to provide passengers with further ease of travel. Similarly, there are also other initiatives at the European level, such as Interrail and Eurail, that offer international travel tickets and a seamless travel approach. As pointed out in the EU report [55], there are several challenges in implementing such systems. For

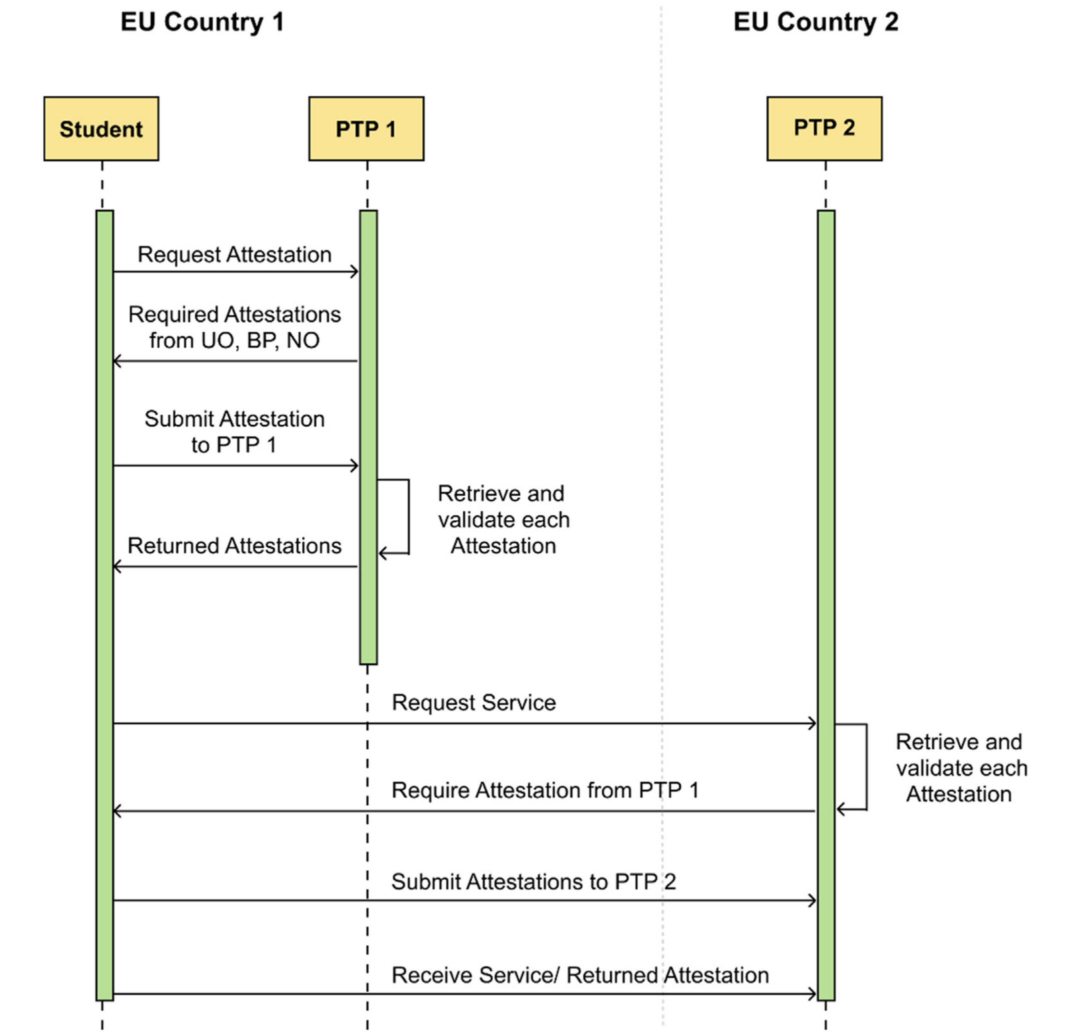

EU Country 1
EU Country 2
Student
PTP 1
PTP 2
Request Attestation
Required Attestations from UO, BP, NO
Submit Attestation to PTP 1
Retrieve and validate each Attestation
Returned Attestations
Request Service
Retrieve and validate each Attestation
Require Attestation from PTP 1
Submit Attestations to PTP 2
Receive Service/ Returned Attestation

Fig. 5. Sequence diagram of using the travel credentials between the student and different public transportation providers (PTP).

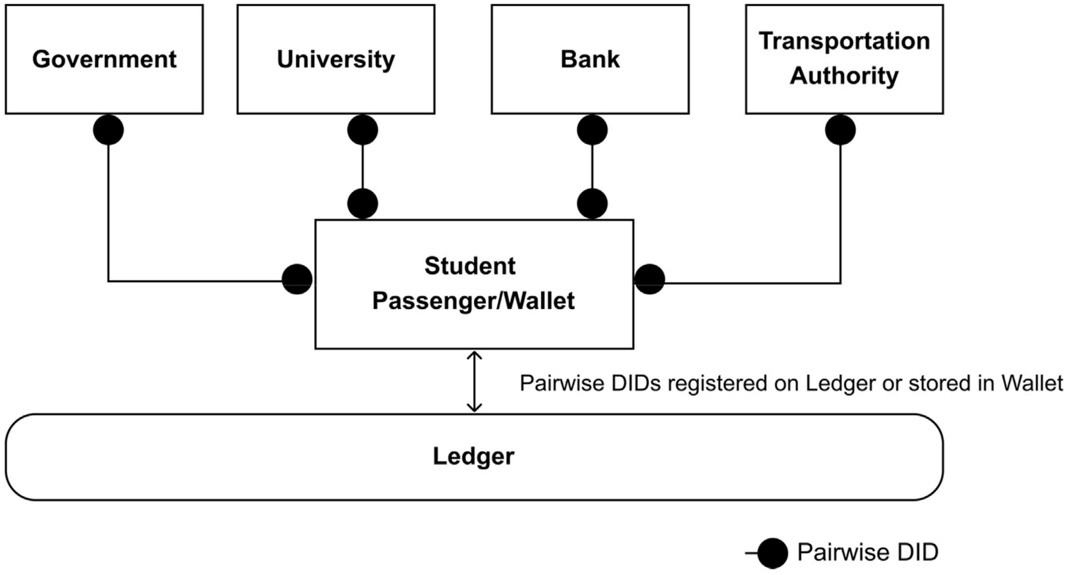


Fig. 6. Forming relationships and creating pairwise decentralized identifiers.

example, ensuring proper access to traffic, travel, and fare data among the service providers is essential due to a lack of trust between the operators. Also, the lack of common and interoperable standards in the data formats is a significant challenge for implementing technical

Table 3
Role definitions of actors in the system.

Institution	Overall role	Identity Management Role
Danske Bank	Bank	Identity Provider/Issuer
Danske Statsbaner (DSB)	Transportation Authority	Service Provider/Identity Provider/Issuer
Copenhagen Business School	University	Identity Provider/Issuer
Danish Government/NemID	Government	Identity Provider/Issuer
Student	Passenger	Identity Holder

solutions for handling such integrated international ticketing systems. In that context, the proposed prototype implementation uses common and interoperable standards such as schema registrations and decentralized identifiers, more in the direction of the development of common standards.

In the prototype implementation, we have modeled different stakeholders such as public transportation providers, passengers, public and private institutions to display their own specific stakeholder requirements. For example, a transportation provider might want to make sure that the credentials provided by the identity provider are valid and the attestations provided by institutions can be verifiable. Similarly, the institutions might have their own requirements that the attestations provided by them are not easily falsifiable. In the prototype, we included different stakeholders, but we have not conducted a detailed stakeholder analysis, which we propose as part of our future work.

Another critical challenge in the proposed system might be the validation of the user credentials as part of the passenger ticket's verification. In checking the tickets, the user credentials need to be validated, which will put additional constraints on the handheld mobile devices used to verify the tickets. Typically, these handheld mobile devices have limited network connectivity, especially when trains/busses/ferries travel through remote areas. As the validation of the user credentials and attestations provided by public/private institutions (e.g., university certifying that the passenger is currently enrolled as a student) needs interactions with the backend blockchain, those handheld ticket-checking mobile devices need to have an internet connection. Therefore, validation of user credentials during the offline ticket checking process is a significant challenge that should be addressed before implementing a decentralized identity management system. A solution might be based on using a cached version of information related to user credentials based on the passengers' reservations or else to perform the ticket checking only when the network connectivity is available. However, it is evident that this challenge should be explored further in search for a suitable pragmatic solution that can support the offline ticket checking process.

In our prototype, we propose decentralized identity management, where the decentralization aspect is achieved through blockchain. In this design, the transactions related to users' identity credentials must be verified and mined into blocks, which is the typical job of miners in a decentralized application. Depending on the type of mining scheme chosen in a decentralized system, sometimes it can lead to high transactional costs. For example, public blockchain and cryptocurrencies like Bitcoin use an expensive mining scheme like proof-of-work; thereby, transactions and mining costs are pretty high. In the case of decentralized identity management, if it is designed as a private blockchain with appropriate permissions, where specific stakeholders, like public transportation providers, have permission and take responsibility to mine the transactions. Then the costs of the transactions are very low.

In contrast, if blockchain is designed as a public blockchain, then the permission to mine the transaction will be decided by some method like proof-of-work or proof-of-stake, then the cost of the transactions will be significantly higher. Similarly, the performance of the transactions is also entirely dependent on the type of blockchain. In the case of public blockchains, the transactions' performance will be constrained by the choice of the mining scheme, e.g., proof-of-work offers low transaction performance. Alternatively, if the blockchain is designed with permissions, then the performance of the transactions is, in general, relatively high, unlike the public blockchains. However, a further detailed study should be done regarding which type of blockchain and mining scheme will be suitable based on stakeholders and their roles in implementing a decentralized identity management application as the cost and performance of the transactions are heavily dependent on them.

6. Discussion

In this paper, we have explored how blockchain-based decentralized identity management conforming to self-sovereign identity principles could help to achieve interoperability across different public transportation authorities. In the following sections, we discuss the need for decentralization of user identity in public transportation and the entailed particulars of the proposed system.

6.1. Decentralization of user identity in public transportation

There is limited research on using blockchain technology for public transportation. A literature review on blockchain applications [56] stated that the usage of blockchain in the transportation sector is still in the early phases of development. However, a reputation-based system for intelligent transportation was proposed by Hîrţan et al. [57]; in this system, users share their data in a secure manner using crowd-sourcing and collective validation. In the genre of intelligent transportation, dynamic key management using blockchain was proposed [58] to enhance security in vehicular communication networks. A blockchain-based mobility-as-a-service [59] using Edge computing was proposed to enhance trust and transparency among all stakeholders. Moreover, a conceptual design for intelligent transportation based on blockchain [60] was proposed for real-time ride-sharing services. In the European Union, the current public transportation system across Europe is highly scattered and needs to be further developed into a coherent transportation solution. In order to achieve the goal of a single European transport market by 2050, the way user accounts are managed needs to be adapted and to adhere to a common format. This means that systems that are currently implemented must use common standards in order to create an interoperable solution that can be used by all existing services and any upcoming services. The implementation of a decentralized identity management solution will be a crucial turning point for driving a new paradigm in public transportation. The conceptual design for the proposed new system is focused on user control, privacy, and interoperability. However, the state of the current systems is characterized by many different standards and a high dependency on different vendors. This dependency leads to vendor lock-in, wherein the private software solutions lock the services into their own exclusive software architectures and proprietary data formats, thereby creating hurdles for integration and interoperability among various transport operators. This phenomenon causes high switching costs and results in isolation between the different transportation management systems. In order to arrive at a combined public transportation solution, standardized common data formats and system architectures need to be developed and adopted among all the participating countries in Europe.

However, designing a one-size-fits-all solution for identity management could lead to the centralization of power, resulting in a monopolized access management landscape in the public transportation sector. Public transportation is a public good, and the underlying identity architecture should not be managed similarly to structures that have been seen by social

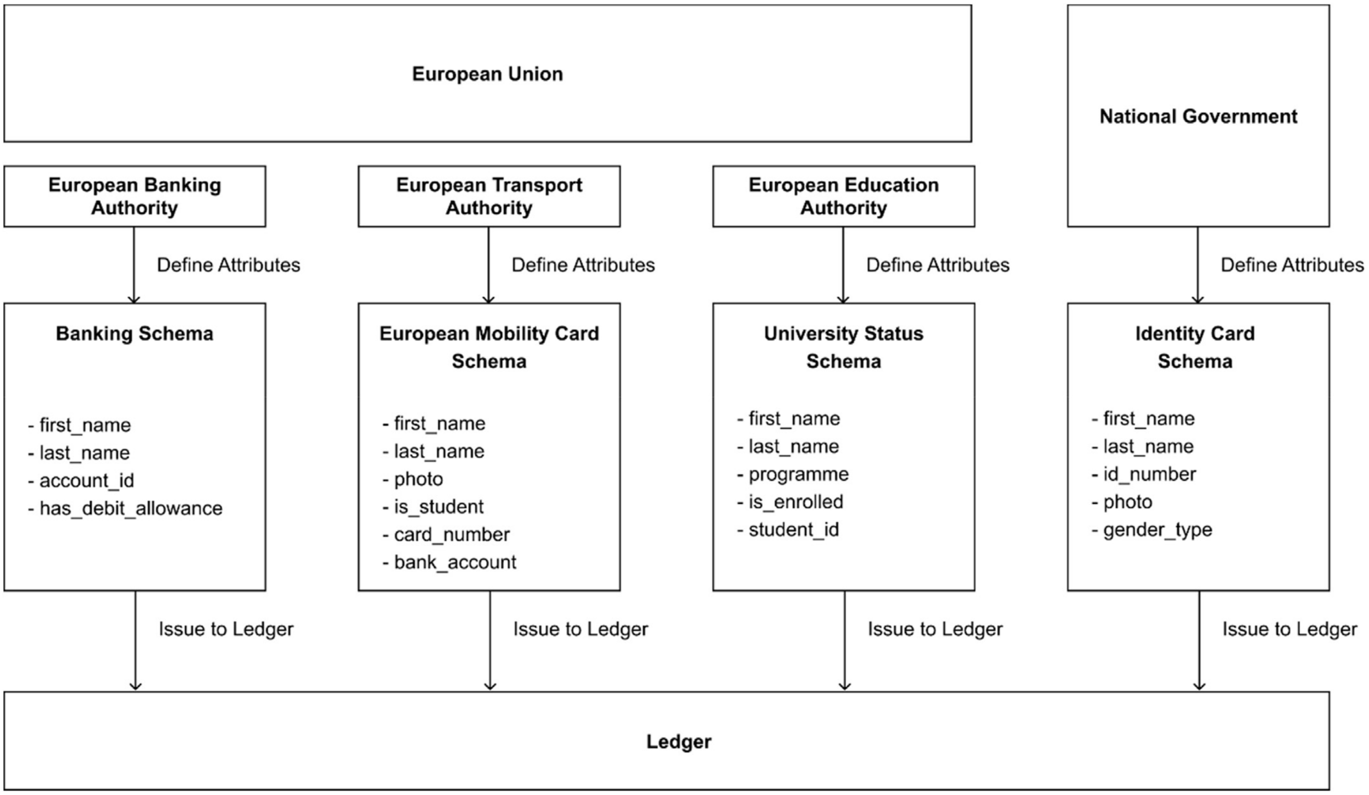


Fig. 7. Schema definition.

media services and other data harvesters. Moreover, a self-sovereign identity-based solution for user management in public transportation not only can enforce privacy by design and user control but also can improve the efficiency of the overall system. The reuse of existing information leads to faster service integration, higher efficiency, better interoperability, and a better user experience across the entire public transportation sector. Moreover, the focus on privacy improves the overall security and reduces costs for public transportation agencies with regard to storing and managing private data. The improved user experience that adheres to an ever-growing need for privacy will incentivize more and more users over time to shift their mobility habits. To profit from the benefits of decentralized identity management in transportation, the European Union must come together not only as a political and fiscal union but also as a transportation union that engages all public transportation stakeholders.

6.2. Relevance to intelligent transportation system

The notion of a cyber-physical-social system integrates interactions among cyber space, physical space, and social space [61]. Cyber-physical-social systems focus on coordinating and integrating human-machine interactions in cyberspace with human and social characteristics so that management and control of such complex socio-technical systems can be achieved efficiently [62,63]. In the context of cyber-physical-social systems, an intelligent transportation system is a typical use case that demonstrates two types of complexities: 1) engineering complexity that arises from transportation infrastructural elements and 2) social complexity that arises from traffic participants, climate, culture, and management [61]. Due to the emergence of social media, it has become easier to obtain and share user-generated information, which contains users' opinions, preferences, and sentiments. As part of the intelligent transportation system, individuals' travel preferences and travel-related information can be integrated by combining information from multiple sources from cyber, physical, and social spaces for traffic behavior analysis and control, thereby offering a better-customized experience to the traffic participants.

The concept of self-sovereign identity can be considered one of the drivers that help to achieve an intelligent transportation system in the long run. Due to its user-centric nature and fine-grained control over access to the user's identity credentials, self-sovereign identity can be shared in a transparent way across different sectors (e.g., transportation, energy) and layers (e.g., cyber, physical, social) using various devices (e.g., sensors, IoT nodes). In fact, the concept of decentralized identity management is not limited to the transportation sector; rather, it can be applied to any industry and public governance sector where there is a need for maintaining user identity, which should be shared across different entities in a self-sovereign manner. The concept of decentralized identity provides necessary privacy for the users among these transactions since a set of decentralized identifiers can be created for each transaction among the stakeholders, while at the same time only revealing the bare minimum of user information that is needed to complete the transactions. As mentioned before, since the decentralized identifiers and claims are not reused across different relationships/transactions, isolated identifiers provide necessary security and privacy for the users as well as enable self-sovereign identity management that is wholly controlled by the identity owners. Moreover, institutional actors, such as banks and healthcare, can potentially allow clients to use their identity management systems for third-party applications. However, the reuse of these systems in a wider context poses security risks due to the inherent link of the user identity to confidential data (e.g., financial records in a bank). Therefore, institutional actors would prefer to use a common decentralized identity management system, like the one proposed in this paper, to exchange credentials with third-parties rather than providing access to their internal identity management systems.

6.3. Towards unified mobility

The low-fidelity prototype developed in this paper models the process of issuing an EMC based on the principles of decentralization using blockchain technology, which can be assessed according to two core principles of self-sovereign identity—namely, user control and portability. The EMC allows for a high level of user control due to its nature as a verifiable credential that is under the full control of the user and stored in the user's personal wallet. Moreover, the EMC is part of the user's identity, which will consist of many different credentials, such as an identity card. Thus, issuing a card is only dependent on its direct verification by the issuer, but it is not reliant on the goodwill of any identity provider. The independence from the identity providers allows the user to gain full control over his or her identity. With regards to portability, the prototype also scores high, mainly because of the underlying technology. The prototype follows the guidelines of the W3C working group on decentralized identity that advocates application-agnostic utilization of credentials. The users can easily restore any of the acquired credentials by using their private keys.

To assess the practicality of the proposed system, an assessment of the process of validating the technical capabilities could be conducted. This would shed light on the technological challenges that the integration of the proposed system into existing ticketing systems brings in order to be a fully operational unified transportation. The developed prototype constitutes a small subset in the solution space for the identified problem, which entails a lot of technical effort on the side of identity and service providers. In the context of public transportation, these initiatives would require advancements in upgrading the current ticketing system and terminals to support the final solution. Specifically, the identities provided to passengers, such as the EMC card, need to be presented in a form that is recognizable by the ticketing terminals to check-in and check-out on a journey in a seamless manner. Additionally, the infrastructure needs to be upgraded in such a way that the inspection devices can successfully read the presented mobility card. Therefore, a more exhaustive technical feasibility study is required to assess the full implementation of an identity management system that facilitates cross-border travel at a European level.

Another pillar of feasibility for this project is operational feasibility. This involves the legal aspects of the system as well as the organizational conflicts and policies that the system entails. Since the underlying technology of the proposed system does not rely on a central authority, a governance trust framework needs to be in place to support the use case of identity management for the public transportation sector. Following how the Sovrin network is operated by its Stewards organizations, few governmental bodies should be formed to take care of the responsibility of governing and maintaining the network. This would help to mitigate any concerns regarding the credibility of the system as well as enable individuals and service providers to join the network. Since the parties cannot trust anyone to assert claims, the governing bodies should be present and have their own identity on the network through which they implement the functionality of issuing verifiable credentials. Several bodies need to be defined via a consortium by the European Commission such as one for transportation, one for banking, and another for educational institutions. Another benefit of establishing a more regulated and governed ledger is that in this way the legal aspects of data privacy can be addressed by the involved entities, which can ensure that the data processing within the system conforms to legislation such as GDPR.

7. Conclusion

Based on the self-sovereign principles of identity, in this paper, we proposed a decentralized identity management system that can eliminate the need to use multiple travel cards when people travel with several transportation providers across multiple jurisdictions. Accordingly, we derived the key requirements and developed a low-fidelity prototype using the Hyperledger Indy blockchain as a proof-of-concept, and we demonstrated how individuals can have better control over the use of their identities while using interoperable ticketing systems across Europe. The proposed system is aligned with the EU goal of achieving a single transportation market among the member countries by 2050. Finally, we presented a low-fidelity prototype version of the decentralized identity management system in the public transportation sector that utilizes the building blocks of self-sovereign identity and blockchain technologies. This paper provides insight into designing a decentralized identity management system in the public transportation sector that is based on the self-sovereign identity principles.

In most of the prevailing identity management solutions, users delegate the control of their identity to the identity providers. To give users full control over their own identity, a direct identity layer between a verifier, an issuer, and an identity holder needs to be established based on the principles of decentralization using a blockchain-based identity management system, where trust is delegated to a network instead of a single party. Thus, a trusted, reliable, transparent, and immutable network, as well as cryptographic proofs, are the fundamental layers needed to grant full control to users. In terms of the practical implications of our research, the prototype introduces a verifiable credential, the EMC, which can act as an identity card throughout the public transportation network in Europe. The design and requirements of the EMC are built upon a set of global technical standards defined by the W3C. Through standardized issuing and validation processes, the overall market would benefit from reduced costs of identity management. Finally, a decentralized system would improve the overall landscape of the market and break free from vendor lock-in by third parties. Through self-sovereign identity-embedded principles, users could simply port their data to the next-best solution without leaving the underlying system architecture. A self-sovereign identity-based solution for public transportation is therefore seamlessly compatible with any other type of service that builds on W3C identity standards. The proposed system design acts as a first step towards implementing decentralized identity management in public transportation.

Future related research could work towards building more thorough and robust prototypes by taking into consideration more real-world use-case scenarios from the transportation sector. In addition, one could also take the cyber-physical-social system and intelligent transportation system perspectives to explore the complexities, challenges, and opportunities in integrating the data from cyber, physical, and social spaces for offering a better-customized experience to traffic participants using traffic behavior analysis and other methods. Finally, future work could explore the challenges associated with adopting such decentralized and self-sovereign-based identity management systems by the respective stakeholders in a multi-transport provider environment by taking the European single transportation market as a use case. For example, the proposed prototype implementation can benefit from involving stakeholders such as Deutsche Bahn and other public transport providers from various European countries to explore how self-sovereign-based identity may help share user credentials data among various transport providers. Furthermore, the proposed prototype can benefit from conducting a comprehensive stakeholder analysis to assess the system from the respective requirements of different stakeholders.

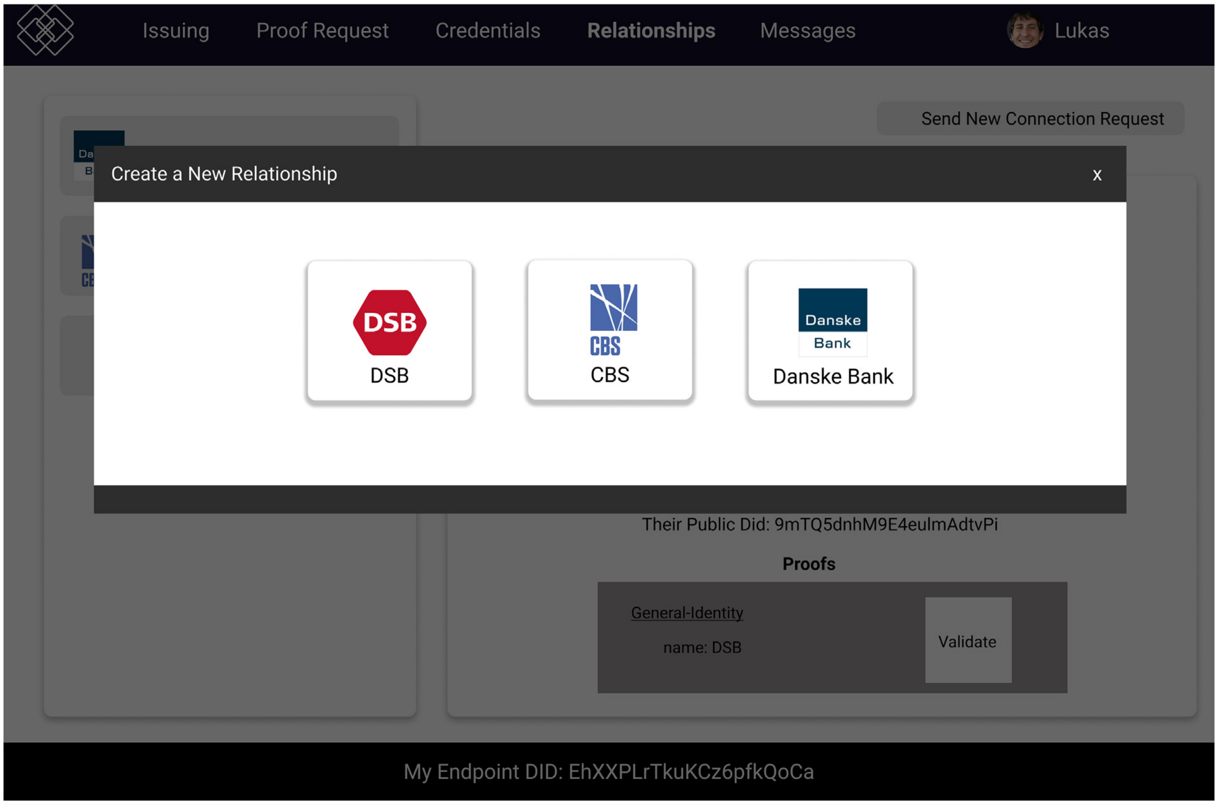
Author contributions

Lukas Stockburger: Conceptualization, methodology, software, validation, writing (original draft); **Georgios Kokosioulis:** Conceptualization, methodology, software, validation, writing (original draft); **Alivelu Mukkamala:** Visualization, writing (review & editing); **Raghava Rao Mukkamala:** Supervision, conceptualization, methodology, writing (review & editing); **Michel Avital:** Supervision, conceptualization, methodology, writing (review & editing).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix. Exemplary Prototype Screenshots



Create a New Relationship

Their Public Did: 9mTQ5dnhM9E4eulmAdtvPi

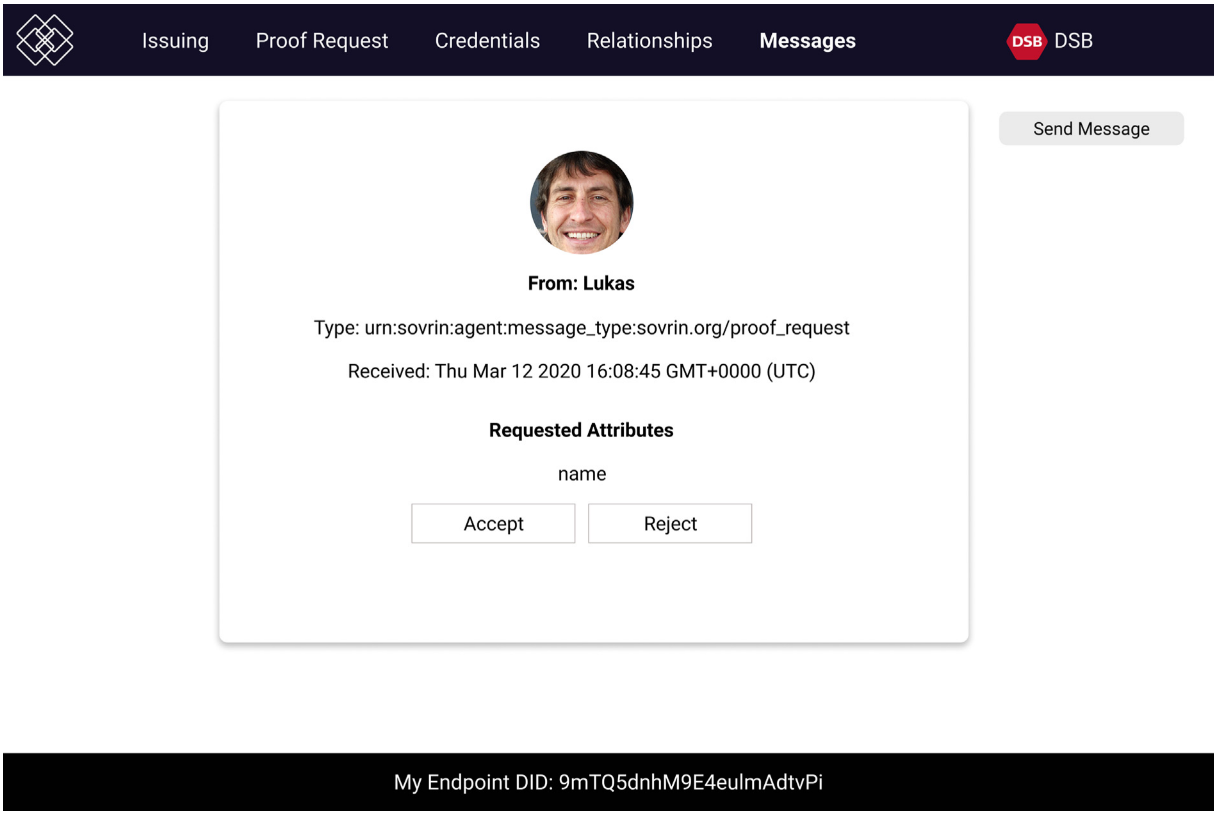
Proofs

General-Identity

name: DSB

My Endpoint DID: EhXXPLrTkuKCz6pfkQoCa

Fig. A1. Sending Relationship Requests.



From: Lukas

Type: urn:sovrin:agent:message_type:sovrin.org/proof_request

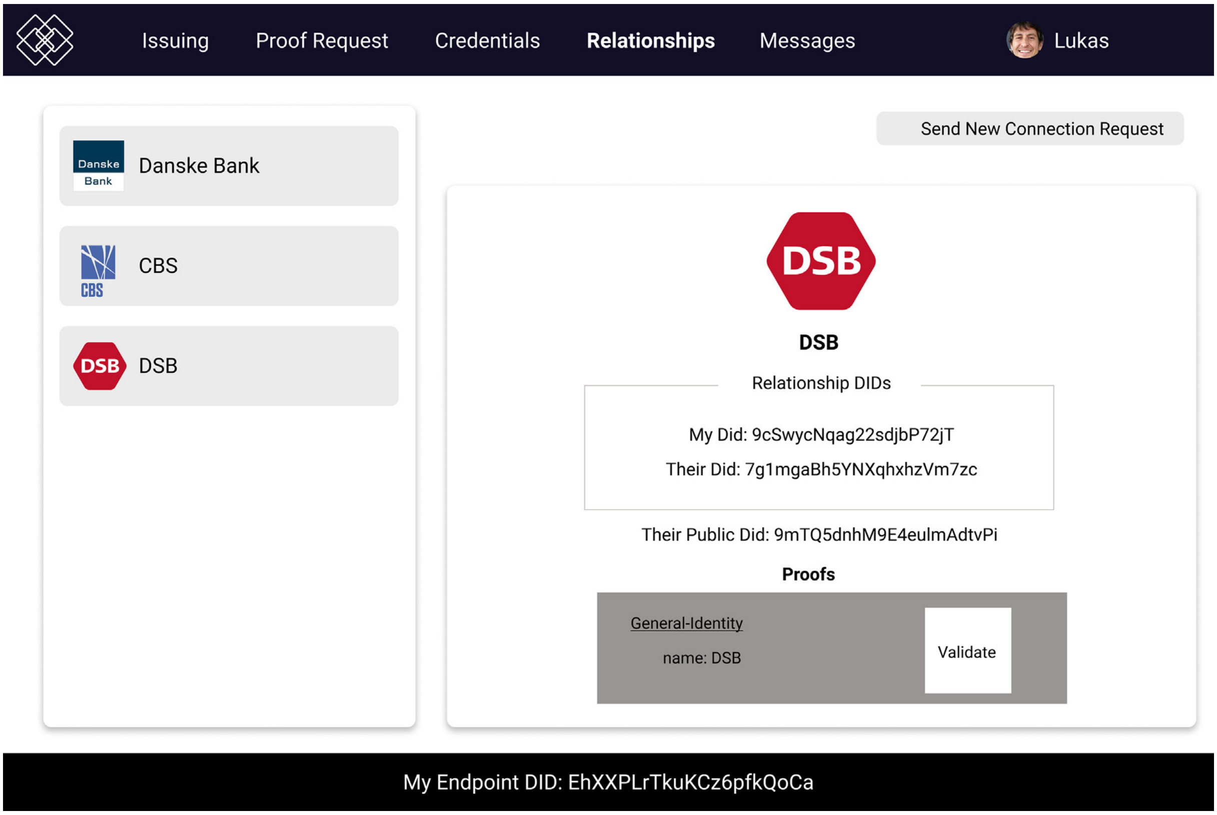
Received: Thu Mar 12 2020 16:08:45 GMT+0000 (UTC)

Requested Attributes

name

My Endpoint DID: 9mTQ5dnhM9E4eulmAdtvPi

Fig. A2. Accepting a Relationship Request.



DSB

Relationship DIDs

My Did: 9cSwycNqag22sdjbP72jT

Their Did: 7g1mgaBh5YNXqhxhzVm7zc

Their Public Did: 9mTQ5dnhM9E4eulmAdtvPi

Proofs

General-Identity

name: DSB

My Endpoint DID: EhXXPLrTkuKCz6pfkQoCa

Fig. A3. Overview of Accepted Relationships.

References

[1] P. Holmberg, M. Collado, S. Sarasini, et al., Mobility as a service-MAAS: describing the framework, 2016, Available online: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1043942&amp;dswid=-3273.

[2] ITS Expert Group, Smart Ticketing Guidelines for ITS Deployment in Urban Areas, Urban ITS Expert Group, 2013. Technical Report, https://ec.europa.eu/transport/sites/transport/files/themes/its/road/action_plan/doc/2013-urban-its-expert_group-guidelines-on-smart-ticketing.pdf.

[3] M. Carter, S. Petter, V. Grover, J.B. Thatcher, Information technology identity: a key determinant of IT feature and exploratory usage, MIS Q. 44 (3) (2020) 983–1021.

[4] M. Carter, V. Grover, Me, my self, and I(T): conceptualizing information technology identity and its implications, MIS Q. 39 (4) (2015) 931–958.

[5] P. Seltsikas, R.M. O'keefe, Expectations and outcomes in electronic identity management: the role of trust and public value, Eur. J. Inf. Syst. 19 (1) (2010) 93–103.

[6] E.A. Whitley, U. Gal, A. Kjaergaard, Who do you think you are? A review of the complex interplay between information systems, identification and identity, Eur. J. Inf. Syst. 23 (1) (2014) 17–35.

[7] H. Tajfel, J.C. Turner, The social identity theory of intergroup behavior, in: J.T. Jost, J. Sidanius (Eds.), Political Psychology, Psychology Press, 2004.

[8] P.J. Windley, Digital Identity: Unmasking Identity Management Architecture (IMA), O'Reilly Media, Inc, 2005.

[9] C. Allen, The path to self-sovereign identity. Life with Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html, 2016.

[10] A. Tobin, D. Reed, The Inevitable Rise of Self-Sovereign Identity, The Sovrin Foundation, 2017. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

[11] T. Lyons, L. Courcelas, K. Timsit, Thematic Report: Blockchain and Digital Identity, The European Union Blockchain Observatory & Forum, 2019. https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf.

[12] M. Laurent, J. Denouël, C. Levallois-Barth, P. Waelbroeck, Digital identity, in: M. Laurent, S. Bouzefrane (Eds.), Digital Identity Management, Elsevier, 2015, pp. 1–45.

[13] D. Recordon, D. Reed, OpenID 2.0: a platform for user-centric identity management, Proc. Second ACM Worksh. Digital Ident. Manag. (2006) 11–16.

[14] D. Fett, R. Küsters, G. Schmitz, A comprehensive formal security analysis of OAuth 2.0, Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (2016) 1204–1215.

[15] K. Wagner, B. Némethi, E. Renieris, P. Lang, E. Brunet, E. Holst, Self-sovereign identity: a position paper on blockchain enabled identity and the road ahead, in: Identity Working Group of the German Blockchain Association, 2018. https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf.

[16] K.C. Toth, A. Anderson-Priddy, Self-sovereign digital identity: a paradigm shift for identity, IEEE Secur. & Priv. 17 (3) (2019) 17–27.

[17] J.P. Moyano, O. Ross, KYC optimization using distributed ledger technology, Bus. & Inform. Syst. Eng. 59 (6) (2017) 411–423.

[18] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, 2008.

[19] A. Bakre, N. Patil, S. Gupta, Implementing decentralized digital identity using blockchain, Int. J. Eng. Technol. Sci. Res. 4 (10) (2017) 379–385.

[20] D. Fiorello, A. Martino, L. Zani, P. Christidis, E. Navajas-Cawood, Mobility data across the EU 28 member states: results from an extensive CAWI survey, Transport. Res. Procedia 14 (2016) 1104–1113. https://ec.europa.eu/transport/sites/transport/files/studies/2019-remaining-challenges-for-eu-wide-integrated-ticketing-and-payment-systems-final-report.pdf.

[21] A. Tobin, Sovrin: what goes on the ledger? Evernym. https://sovrin.org/wp-content/uploads/2017/04/What-Goes-On-The-Ledger.pdf, 2018.

[22] Y. Liu, D. He, M.S. Obaidat, N. Kumar, M.K. Khan, K.K.R. Choo, Blockchain-based identity management systems: a review, J. Netw. Comput. Appl. 166 (2020) 1–11, 102731.

[23] K. Cameron, The Laws of Identity, Microsoft Corp, 2005. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[24] J.B. Bernabe, J.L. Canovas, J.L. Hernandez-Ramos, R.T. Moreno, A. Skarmeta, Privacy-preserving solutions for Blockchain: review and challenges, IEEE Access 7 (2019) 164908–164940.

[25] M. Kuperberg, Blockchain-based identity management: a survey from the enterprise and ecosystem perspective, IEEE Trans. Eng. Manag. 67 (4) (2020) 1008–1027.

[26] X.C. Zheng, S.J. Sun, R.R. Mukkamala, et al., Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies, J. Med. Internet Res. 21 (6) (2019) 1–12.

[27] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, K. Dahal, DNS-IdM: a blockchain identity management system to secure personal data sharing in a network, Appl. Sci. 9 (15) (2019) 1–19, 2953.

[28] B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494.

[29] B. Faber, G.C. Michelet, N. Weidmann, R.R. Mukkamala, R. Vatrapu, BPDIMS: a blockchain-based personal data and identity management system, Proc. 52nd Hawaii Int. Conf. Syst. Sci. (2019) 6855–6864.

[30] L. Soltanisehat, R. Alizadeh, H. Hao, K.K.R. Choo, Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: a systematic literature review, IEEE Trans. Eng. Manag. (2020) 1–16.

[31] M. Kamargianni, M. Matyas, The business ecosystem of mobility-as-a-service, Proc. Transport. Res. Board Annu. Meet. (2017) 1–14.

[32] E. Bothos, B. Magoutas, K. Arnaoutaki, G. Mentzas, Leveraging blockchain for open mobility-as-a-service ecosystems, Proc. IEEE/WIC/ACM Int. Conf. Web Intellig. (2019) 292–296.

[33] B. Bhushan, A. Khamparia, K.M. Sagayam, S.K. Sharma, M.A. Ahad, N.C. Debnath, Blockchain for smart cities: a review of architectures, integration trends and future research directions, Sustain. Cities Soc. 61 (2020), 102360.

[34] J. Xu, K. Xue, H. Tian, J. Hong, D.S. Wei, P. Hong, An identity management and authentication scheme based on redactable Blockchain for mobile networks, IEEE Trans. Veh. Technol. 69 (6) (2020) 6688–6698.

[35] G. Ateniese, B. Magri, D. Venturi, E. Andrade, Redactable blockchain–or–rewriting history in bitcoin and friends, Proc. IEEE Eur. Sympos. Secur. Priv. (2017) 111–126.

[36] D. Derler, K. Samelin, D. Slamanig, C. Striecks, Fine-grained and controlled rewriting in blockchains: chameleon-hashing gone attribute-based, Proc. Netw. Distr. Syst. Secur. Symp. (2019) 1–15.

[37] F. Buccafurri, L. Fotia, G. Lax, R. Mammoliti, Enhancing public digital identity system (SPID) to prevent information leakage, in: Proceedings of International Conference on Electronic Government and the Information Systems Perspective vols. 57–70, Springer, Cham, 2015.

[38] F. Buccafurri, G. Lax, A. Russo, G. Zunino, Integrating digital identity and blockchain, in: Proceedings of OTM Confederated International Conferences on the Move to Meaningful Internet Systems, Springer, Cham, 2018, pp. 568–585.

[39] H.H.S. Yin, K. Langenheldt, M. Harlev, R.R. Mukkamala, R. Vatrapu, Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain, J. Manag. Inf. Syst. 36 (1) (2019) 37–73.

[40] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, M. Sena, uPort: a platform for self-sovereign identity. https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf, 2017.

[41] Civic, Civic. Civic technologies. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf, 2017.

[42] K. Peffers, T. Tuunanen, M.A. Rothenberger, S. Chatterjee, A design science research methodology for information systems research, J. Manag. Inf. Syst. 24 (3) (2007) 45–77.

[43] R. Baskerville, A. Baiyere, S. Gregor, A. Hevner, M. Rossi, Design science research contributions: finding a balance between artifact and theory, J. Assoc. Inf. Syst. Online 19 (5) (2018) 358–376.

[44] A.R. Hevner, S.T. March, J. Park, S. Ram, Design science in information systems research, MIS Q. 28 (1) (2004) 75–105.

[45] J. Pries-Heje, R. Baskerville, The design theory nexus, MIS Q. 32 (4) (2008) 731–755.

[46] A.R. Hevner, A three-cycle view of design science research, Scand. J. Inf. Syst. 19 (2) (2007) 87–92.

[47] C. Sonnenberg, J. Vom Brocke, Evaluation patterns for design science research artefacts, in: Proceedings of European Design Science Symposium, Springer, Berlin, Heidelberg, 2012, pp. 71–83.

[48] J. Venable, J. Pries-Heje, R. Baskerville, A comprehensive framework for evaluation in design science research, in: Proceedings of International Conference on Design Science Research in Information Systems, Springer, Berlin, Heidelberg, 2012, pp. 423–438.

[49] R. Gleasure, When is a problem a design science problem? Syst. Signs Actions 9 (1) (2015) 9–25.

[50] European Commission, Roadmap to a Single European Transport Area: towards a Competitive and Resource Efficient Transport System: White Paper, Publications Office of the European Union, 2011. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0144&amp;from=EN.

[51] M.T. Jensen, S. Gyimothy, O.B. Jensen, Staging interrail mobilities, Tour. Stud. 16 (2) (2016) 111–132.

[52] C. Tankard, What the GDPR means for businesses, Netw. Secur. *2016* (6) (2016) 5–8.

[53] S. Bradner, RFC-2119: Key Words for Use in RFCs to Indicate Requirement Levels, Network Working Group, 1997. https://tools.ietf.org/html/rfc2119.

[54] J. Rumbaugh, I. Jacobson, G. Booch, The Unified Modeling Language Reference Manual, second ed., Addison Wesley Educational Publishers, 2010.

[55] S. Frazzani, I. Taranic, M. Jensen, A. Zamboni, K. Noti, M. Piantoni, Remaining challenges for EU-wide integrated ticketing and payment systems (No. Ref. Ares (2019) 5698356). https://op.europa.eu/en/publication-detail/-/publication/af05b3eb-df43-11e9-9c4e-01aa75ed71a1, 2019.

[56] V. Astarita, V.P. Giofrè, G. Mirabelli, V. Solina, A review of blockchain-based systems in transportation, Information 11 (1) (2020) 1–24, 21.

[57] L.A. Hîrţan, C. Dobre, H. González-Vélez, Blockchain-based reputation for intelligent transportation systems, Sensors 20 (3) (2020) 791.

[58] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P.A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Inter. Things J. 4 (6) (2017) 1832–1843.

[59] T.H. Nguyen, J. Partala, S. Pirttikangas, Blockchain-based mobility-as-a-service, Proc. 28th Int. Conf. Comput. Commun. Netw. (2019) 1–16.

[60] Y. Yuan, F.Y. Wang, Towards blockchain-based intelligent transportation systems, Proc. IEEE 19th Int. Conf. Intellig. Transport. Syst. (2016) 2663–2668.

[61] G. Xiong, F. Zhu, X. Liu, X. Dong, W. Huang, S. Chen, K. Zhao, Cyber-physical-social system in intelligent transportation, IEEE/CAA J. Autom. Sinica 2 (3) (2015) 320–333.

[62] F.Y. Wang, The emergence of intelligent enterprises: from CPS to CPSS, IEEE Intell. Syst. 25 (4) (2010) 85–88.

[63] J.J. Zhang, F.Y. Wang, X. Wang, G. Xiong, F. Zhu, Y. Lv, J. Hou, S. Han, Y. Yuan, Q. Lu, Y. Lee, Cyber-physical-social systems: the state of the art and perspectives, IEEE Trans. Comput. Social Syst. 5 (3) (2018) 829–840.