UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Blockchain based Identity Management and Ticketing for MaaS

Paulo Catalão Querido

Mestrado em Engenharia Informática
Especialização em Engenharia de Software

Versão Pública

Trabalho de Projeto orientado por:
Prof. Doutor Naercio David Pedro Magaia

2020

Acknowledgments

I would like to thank Card4B Systems for the opportunity of integrating a revolutionary project within the public transport industry, which greatly enhanced my technical knowledge and sharpened my professional experience.

Furthermore, I could not dismiss the university Faculdade de Ciências da Universidade de Lisboa for providing all the knowledge, throughout my graduation years, required for my professional career.

To conclude, I'm thankful to all my family members for their continuous support over the years. In particular, to my parents for their wise counselling and for investing in my education. Secondly, a significant thank you to Inês Soares for all her love and support during this last step of my education. And lastly, I would like to thank all the friends that I made during this chapter of my life.

To my parents

Resumo

À medida que avançamos no século XXI, o mundo torna-se progressivamente mais sofisticado e a nossa capacidade de prever o futuro diminui à mesma proporção. Os problemas globais emergentes exigem novos tipos de ferramentas, e permitem fornecer uma imagem holística dos sistemas atuais e complexos, possibilitando o avanço tecnológico. São vários os problemas que assombram o futuro da humanidade, adjacente aos recursos escassos e às questões ambientais, surge assim a necessidade de uma exploração mais eficiente das infraestruturas existentes.

Nos últimos anos, evidências científicas de degradação ambiental são um problema reconhecido que a humanidade enfrenta e, devido a isso, organizações conscientes começam a adotar a visão de "desenvolvimento sustentável". A Comissão Mundial sobre Meio Ambiente e Desenvolvimento define tal visão como a capacidade de as gerações atuais atenderem as suas necessidades sem comprometerem a capacidade das gerações futuras atenderem as deles. Apesar do desenvolvimento sustentável ser desejável, mudanças significativas, se não radicais, às premissas básicas por trás dos modelos de negócios modernos são necessárias para atingir o "desenvolvimento sustentável".

Servicising refere-se a um fenômeno em que os fornecedores podem mudar o foco dos seus modelos de negócios da venda direta de produtos para a prestação de serviços, aumentando a eficiência operacional, e produtos e processos mais ecológicos. Assim, *servicising* é a solução que melhor atende à procura e às expectativas dos consumidores. O sucesso de *servicising* é principalmente uma consequência dos indivíduos se poderem demarcar da manutenção, armazenamento e outras responsabilidades associadas à propriedade de certos itens.

Atualmente existem diversos exemplos de serviços prósperos. No entanto, a organização atual do sistema de transportes públicos, não contribui de forma adequada para um ecossistema de serviços de mobilidade funcional e conveniente. Sabe-se ainda que o fenómeno da urbanização está a concentrar a população nas cidades, aumentando a poluição e o congestionamento nos centros urbanos. Considerando o papel substancial dos transportes na vida quotidiana nas zonas urbanas, a pressão para melhorar a indústria dos transportes intensifica-se.

Na Europa, os sistemas de transporte público privatizados são frequentemente desenvolvidos individualmente por cada operador, resultando numa fragmentação e falta

de uniformidade da informação. Estes operadores implementam os seus sistemas independentemente uns dos outros, analogamente originando sistemas legados e soluções de bilhética proprietárias, o que significa que os passageiros que viajam por múltiplos operadores são forçados a utilizar as soluções individuais dos vários fornecedores de serviços e comprar bilhetes separados.

O conceito de *Mobility-as-a-Service (MaaS)* promete a resolução dos problemas existentes na indústria dos transportes, uma vez que, permite a integração de diferentes serviços de mobilidade, como partilha de carros e bicicletas, estacionamentos, táxis, entre outros, com o transporte público tradicional. Para planear uma viagem, os passageiros contam com diversas opções de mobilidade, conectadas entre si, com uma escolha aberta de alternativas de acordo com as suas preferências. A base do *MaaS* é a disponibilização de informação multimodal a qualquer hora e em qualquer lugar, com acesso direto e irrestrito de um fornecedor de serviço para outro. Considerada como a solução ideal, o *MaaS* incorpora o planeamento de viagens, bilhetes eletrónicos, vários métodos de pagamento como "*pay-as-you-go*" e pacotes mensais, bem como um esquema de validação de bilhetes. Os sistemas modernos de *MaaS* foram desenvolvidos como uma camada intermediária e centralizada entre os operadores e os passageiros. No entanto, revela-se um enorme desafio ampliar a rede de *MaaS* que englobe várias operadoras.

A *Blockchain* adota uma abordagem descentralizada e compreende um *Ledger* partilhado que regista e armazena todas as transações por ordem cronológica entre as várias partes que constituem uma rede. O resultado da descentralização de cada utilizador na rede, também chamado de nó, mantém uma cópia idêntica do *Ledger*, em vez de existir uma única autoridade no controlo do *Ledger*. Essencialmente, a *Blockchain* combina tecnologias já existentes, que quando acopladas, criam redes que garantem a confiança entre pessoas ou partes. Esta tecnologia emprega um *Distributed Ledger Technology (DLT)*, capaz de armazenar dados verificados por mecanismos criptográficos entre um grupo de utilizadores, que é primeiro acordado por meio de um protocolo de rede pré-estabelecido. Apesar de ser frequentemente associada às aplicações de ativos financeiros digitais, como a tecnologia de Bitcoin, a *Blockchain* tem o potencial de remodelar e afetar uma ampla gama de indústrias.

Com as inovações recentes em tecnologias de *Blockchain* e de *Ledger* distribuído, especialmente os desenvolvimentos atuais de *Smart Contracts*, espera-se que seja finalmente possível uma nova abordagem distribuída para o *MaaS*. Os sistemas *MaaS* beneficiam do poder da tecnologia disruptiva da *Blockchain*, melhorando a transparência e a confiança entre os provedores de serviço assim eliminando a camada intermediária. Além disso, a visão de uma experiência de viagem contínua entre vários fornecedores de transporte torna-se, finalmente, uma realidade para o utilizador, uma vez que todos os fornecedores de transporte cooperam no mesmo sistema.

O potencial de usar *Blockchain* permite abordagens mais eficientes para aproximar

os utilizadores e os provedores de serviço. Portanto, um serviço de *MaaS* baseado em *Blockchain* pode alcançar uma variedade de vantagens, incluindo a validação de títulos de viagem e identidades, pagamento único para títulos combinados. Notavelmente, a lógica de negócio relacionada com os bilhetes e os métodos de pagamento pode ser programada por meio de *Smart Contracts*. As transações, geradas por estes últimos, são posteriormente armazenadas e verificadas no *Ledger* distribuído, permitindo assim uma melhor gestão de dados, maior transparência e confiança.

Para implementar o novo conceito de *MaaS* e tirar partido dos elevados volumes de dados relativos aos passageiros e aos seus bilhetes, é fundamental que os operadores dos transportes tenham um sistema unificado, permitindo assim que cada participante crie, visualize e modifique a informação. Todavia, com um grande volume de informações, várias preocupações surgem em relação à disponibilidade e segurança do armazenamento, o que pode afetar a privacidade do utilizador.

Assim, este trabalho estuda e investiga a interseção entre *Blockchain* e *MaaS*, que estão na vanguarda da investigação para o setor de transportes. Os sistemas de transporte baseados em *Blockchain* criam uma abordagem de transporte sustentável, encontrando-se atualmente sob investigação a nível mundial. Em particular, este projeto tem como principal objetivo oferecer uma solução *MaaS* baseada em *Blockchain* que fornece aos usuários soluções de mobilidade envolvendo diferentes operadores de transporte e vários operadores *MaaS* no mesmo sistema.

O projeto possibilita o desenvolvimento de uma nova solução de bilhética baseada em *Blockchain*, com um módulo de Identity Managament capaz de gerir as identidades dos passageiros transversalmente a todo o sistema, bem como a criação de um mock-up para uma aplicação *MaaS* destinada ao passageiro. Por fim, este trabalho avalia o sistema desenvolvido em termos de funcionamento e desempenho, de acordo com casos de uso e requisitos.

O trabalho alcançou resultados no que diz respeito à colaboração entre múltiplos prestadores de serviços operando numa única plataforma, oferecendo assim uma solução unificada para as necessidades identificadas do passageiro. Além disso, a imutabilidade e as características de registo da *Blockchain* melhoram a transparência das operações do provedor de transporte com os dados do utilizador final. Esta tecnologia também aumenta a confiabilidade num ambiente descentralizado, resolvendo assim o problema da fragmentação de dados.

Palavras-chave: *Blockchain*; *Identity Management*; *Mobility-as-a-Service*; Bilhética; Descentralização

Abstract

As time moves further into the 21st century, the world is progressively becoming more sophisticated, and our capacity to forecast the future is decreasing at the same rate. The emerging global problems require new kinds of tools paving the way to move forward. Across Europe, privatised public transport systems are frequently conceived in separation by an operator resulting in legacy systems with proprietary ticketing solutions causing fragmentation and lack of uniformity of information.

The Mobility-as-a-Service (MaaS) concept promises to solve existing problems in the transport industry since it allows the integration of different mobility services, such as car and bicycle sharing, among others, with traditional public transport. To plan a trip, passengers have several mobility options, interconnected to each other, with a range of alternatives according to their preferences. However, it is a huge challenge to expand the MaaS network that includes several operators.

Recent innovations in Blockchain and distributed ledger technologies, especially the current developments of smart contracts, it is expected that a novel distributed approach to MaaS is finally feasible. MaaS systems benefit from the power of Blockchain disruptive technology, improving transparency and trust among service providers thereby eliminating the middle tier. In order to implement the new MaaS concept and take advantage of the high volumes of data relating to passengers and their tickets, it is essential that transport operators have a unified system, thus allowing each participant to create, view and modify the information.

This project enables the development of a new ticketing solution based on Blockchain, with an Identity Management module capable of managing the identities of passengers across the entire system, as well as the creation of a MaaS application mock-up for the passenger. Finally, the proposed system is evaluated in terms of operation and performance, according predefined use cases and requirements. Results are achieved in terms of the collaboration between multiple service providers operating on a single platform.

Keywords: Blockchain; Identity Management; Mobility-as-a-Service; Ticketing; Decentralisation

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ABT Account Based Ticketing. xviii, xxi, 20

BFT Byzantine Fault Tolerant. xviii, xxi

CA Certificate Authority. xviii, xxi

CCG Centro de Computação Gráfica. xviii, xxi

CNA Calypso Networks Association. xviii, xxi, 19

DApp Decentralised Application. xviii, xxi

DApps Decentralised Applications. xviii, xxi

DID Decentralised Identifier. xviii, xxi, 16

DIF Decentralized Identity Foundation. xviii, xxi, 17

DLT Distributed Ledger Technology. xviii, xxi, 2, 3, 16, 17, 27, 28, 29, 31, 32

DLTs Distributed Ledger Technologies. xviii, xxi, 3

DPOS Delegated Proof-of-Stake. xviii, xxi

FCUL Faculdade de Ciências da Universidade de Lisboa. xviii, xxi, 4

GDPR General Data Protection Regulation. xviii, xxi, 11

HLF Hyperledger Fabric. xviii, xxi

IdM Identity Management. xviii, xxi, 4, 14, 15, 16, 17, 28, 31

IDMS Identity Management System. xviii, xxi, 11, 12, 14, 16, 17, 30, 31

IDMSs Identity Management Systems. xviii, xxi, 11, 13, 18, 28, 31

IdP Identity Provider. xviii, xxi, 12, 13, 14

ITS Integrated Transport Services. xviii, xxi

MaaS Mobility-as-a-Service. xv, xviii, xxi, 2, 3, 4, 5, 21, 23, 24, 27, 32, 33

MSP Membership Service Provider. xviii, xxi

OASIS Organization for the Advancement of Structured Information Standards. xviii, xxi

Org Organisation. xviii, xxi

P2P Peer-to-Peer. xviii, xxi, 7

PBFT Practical Byzantine Fault Tolerance. xviii, xxi

PEI Projeto de Engenheria Informática. xviii, xxi

PKI Public Key Infrastructure. xviii, xxi

PoC Proof of Concept. xviii, xxi

PoS Proof-of-Stake. xviii, xxi

PoW Proof-of-Work. xviii, xxi, 8, 10, 29, 30

QR Quick Response. xviii, xxi, 17, 28

R&D Research and Development. xviii, xxi, 4

SAML Security Assertion Markup Language. xviii, xxi, 14

SP Service Provider. xviii, xxi, 12, 13, 14, 20, 21, 28, 32

SSI Self-Sovereign Identity. xviii, xxi, 17, 18, 30

SSO Single Sign-On. xviii, xxi, 13, 14

TO Transport Operator. xviii, xxi

UNL Unique Node List. xviii, xxi

W3C World Wide Web Consortia. xviii, xxi, 16

List of Definitions

Access Token Credentials used to access protected resources which is a string representing an authorisation issued to the client. The string is usually opaque to the client. Tokens represent specific scopes and durations of access, granted by the resource owner, and enforced by the resource server and authorisation server. – [5]. xviii, xxi

Research and Development (R&D) Research and development (R&D) includes activities that companies undertake to innovate and introduce new products and services. It is often the first stage in the development process. The goal is typically to take new products and services to market and add to the company's bottom line.. xviii, xxi

Single Sign-On (SSO) Property of access control of multiple related, yet independent, software systems. With this property, a user logs in a single ID and password to gain access to any of several related systems.. xviii, xxi

Software Development Kit (SDK) A software development toolkit (SDK) is a set of software tools and programs provided by hardware and software vendors that developers can use to build applications for specific platforms. These providers make their SDKs available to help developers easily integrate their apps with their services.. xviii, xxi

Transport Layer Security (TLS) Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP).. xviii, xxi

User Experience (UX) According to ISO 9241, user experience is defined as "a person's perceptions and responses that result from the use or anticipated use of a product, system or service". xviii, xxi, 31

Chapter 1

Introduction

Progressively the world is evolving and transforming into a more sophisticated environment that employes technology to enhance societies. As time moves further into the 21st century, our capacity to forecast the future is decreasing at a proportional rate. The emerging global problems demand innovative types of tools providing a holistic picture of the complex systems in place, paving the way to move forward.

Lately, scientific evidence of environmental degradation is an acknowledged problem that the humankind faces, and due to this, enlightened organisations commence adopting the vision of "sustainable development" [6]. Furthermore, the World Commission on Environment and Development [7] defines such vision as "the ability of current generations to meet their needs without compromising the ability of future generations to meet theirs." . Despite, sustainable development being desirable, Sandra Rothenberg [6] states that experts criticise the significant, if not radical, changes in the basic premises behind modern business models that are needed to accomplish it.

Servicising refers to a phenomenon in which customers acquire and merely receive the outcome of the organising and selection actions performed by another individual [8]. Hence, *servicising* is a solution that better satisfy consumers' demands and expectations. Since, suppliers shift the focus of their business models from selling products to providing services, therefore boosting their operational efficiency and better eco-friendly products and processes [8]. Thereby, and according to Heikkilä [8], organisations benefit from driving the demand for reduced material use, toward a strategic opportunity.

Services are present around the society, for instance, computer repair, car maintenance, parcel shipping, among others. Another example of a service is travelling by means of public transport, but the latter services as a unity are not [8]. In several industries, *servicising* has previously been adopted, in particular in freight transport and logistics, and it is strongly connected with the "sharing economy", which refers to sharing items and using services, rather than maintaining the entire machinery. As reported by Heikkilä [8], the success of *servicising* is mainly a consequence of characters highly seeking to discharge themselves from maintenance, storage, insurance, and other respon-

sibilities associated with the ownership of certain items. Accordingly, enterprises centre themselves on the activity and profit from the outcome.

Although prosperous services emerge nowadays, e.g. Netflix, the current organisation of the public transport system does not adequately contribute to a functional and convenient mobility service ecosystem. Mobility services regard individual transport services that are provided by simplistic interfaces of mobility operators.

Considering the substantial role of transportation in public financing, the pressure for enhancing the transport industry intensifies due to high user demand [8]. Simultaneously, urbanisation is leading individuals to cities, thus quickly increasing the population, pollution and congestion in the urban centres. Adjacent to the scarce resources and environmental issues, arises a necessity for more efficient exploitation of the existing infrastructure and transportation system instead of extending it [8].

The aforementioned issues correlate with the transportation industry empowering the necessity for a unified and single transport platform for all transport operators, and this is when Mobility-as-a-Service, also known as MaaS, intervenes. MaaS enables the integration of multiple mobility services such as car and bike sharing, car parks, taxis, and so forth with traditional public transport. To plan a trip, passengers are empowered with several mobility options, connected to one another, with an open choice of alternatives according to preference. Mobility-as-a-Service consists of multimodal information available at anytime and anywhere, with unconstrained and straightforward access from one service provider to another [9].

Considered as the perfect solution to the issues above, MaaS incorporates a trip planner, e-ticket, payment method for both “pay-as-you-go” and “mobility package”, and also a ticketing validation scheme. Modern MaaS systems have been developed as a centralised intermediate layer between providers and travellers. Having this in mind, MaaS system outcomes several benefits, like the easy management of two-sided parties (travellers and providers), and a shared database with different providers. Nevertheless, it is an enormous challenge to scale up the MaaS network with multiple and distinct operators.

Recent innovations in Blockchain and Distributed Ledger Technology (DLT), especially the current developments of smart contracts, it is expected that a novel distributed approach to MaaS is finally feasible. Mainly, Blockchain comprises a shared ledger of transactions between parties in a network, with a decentralised approach, which is not controlled by a sole central authority [10].

The Organisation for Economic Co-operation and Development (OECD) describes a ledger as a record book that records and stores all transactions between users in chronological order [10]. Decentralisation results from each user on the network, also called a node, holding an identical copy of the ledger, rather than one authority being in control of the ledger. Despite frequently associated with the digital financial asset applications, e.g., Bitcoin, the Blockchain technology has the potential to reshape and affect a wide range

of industries.

Essentially, Blockchain combines already existing technologies, and when coupled, these technologies create networks that secure trust amongst people or parties. Blockchain employs DLT to store data verified by cryptographic mechanisms amongst a group of users, which is first agreed through a pre-established network protocol and often outwardly the control of a central authority [10].

MaaS systems harness the power of the Blockchain disruptive technology, improving the transparency and trust between service providers by eliminating the intermediate layer. Moreover, the vision of a seamless public travelling experience for the end-user becomes a reality since all the participating transport providers cooperate in the same network.

The potential of using Blockchain enables more efficient approaches for approximating users and service providers, and therefore, a Blockchain-based MaaS can achieve a manifold of advantages including the validation of travel titles and identities, single payment for combined titles, and trust defined by smart contracts. Notably, the tickets and payment methods can be programmed as smart contracts stored and verified in the distributed ledger, thus enabling better data management.

1.1 Motivation

The intersection between DLT and MaaS are the bleeding edge of investigation within the transport sector as current solutions still present issues. On one hand, Blockchain based transportation systems create a novel approach of sustainable transportation. On the other hand, the MaaS concept can ease customer pain in using multiple solutions for daily travels.

The creation of a MaaS model within the current public transportation ecosystem is deemed impossible due to a myriad of problems. In a general overview, such problems are related to a heavy decentralisation of the information within the industry, the lack of communication and trust between the different service providers. Following the same philosophy towards a "new culture of mobility", the host organisation (i.e., Card4B) decided to explore the benefits of DLTs to best address the issues surrounding public transportation systems, specifically, in the context of creating a MaaS solution. The primary aim of using distributed ledgers is to increase collaboration, as well as to share trusted information, reduce costs, and decrease the risk of central storage or tampering with the data, via redundancy, whilst forging futuristic new business models in the transportation industry.

1.2 Objectives

The main goal of the project is to evaluate the applicability of Blockchain technology with the current ticketing solutions provided by Card4B - Systems S.A. along with envisioning

a novel platform of MaaS. Furthermore, the aim is the creation of a single platform, providing a cooperating ecosystem for partner organisations, thus, promoting a seamless travelling experience for a customer that requires the use of multiple service providers on a single journey.

Achieving such a goal requires building a ticketing system that is recognised by the service providers cooperating in the network for validation purposes. However, handling identity information about a user imposes liability for the system owner, hence being required a solution for granting trust and privacy for the end-user. A solution for the latter problem also relies on the Blockchain technology to grant the user ownership of its data. In case of travelling across multiple transportation providers, permission grants for accessing information are issued, helping the user knowing with whom his data is shared.

This dissertation is being carried out within the scope of the Innovation for a Mobility as a Service (i4MaaS) project that aims to create a research and development team dedicated to the study of seamless travelling solutions with a focus on MaaS and the exploration of Blockchain technologies. Moreover, the goal is to study and investigate the new MaaS paradigm and development of interoperability tools and platforms supported by Blockchain technology. Thus promoting the speed, security and immutability of the data transacted between all the players in the MaaS ecosystem and for the various stages of the trip, namely giving support for ticketing and Identity Management (IdM) paradigms. In particular, the project aims to offer a Blockchain-based MaaS solution that offers users mobility solutions involving different transport operators and several MaaS operators.

1.3 Host Organisation

This work is performed at Card4B - Systems S.A. in partnership with Faculdade de Ciências da Universidade de Lisboa (FCUL). Card4B originated from the necessity for solutions towards a "new culture of mobility" providing software solutions and expert services for Integrated Mobility solutions and city-services such as Public Transport, On-street and Off-street Parking, Tolls, Taxis, Car-sharing, Bike-sharing, On-demand transportation, Schools, Libraries, Pools, Stadium, Museum, among others.

Card4B's growth has enabled the development of Research and Development (R&D) projects, both at national and international level, enabling innovating the solutions currently on the market, and targeting future solutions on a mid-term vision [11].

1.4 Contributions

The work accomplished during this dissertation allowed the elaboration of a research article entitled "Blockchain Solutions of Identity Management and Ticketing for a Mobility-as-a-Service Ecosystem: A Survey, a Reference Model, and an Outlook" to be submitted

to an international journal.

1.5 Document Structure

The structure of this document is divided into seven chapters, organised as follows:

- Chapter 2 is comprised of the Background research conducted to each concept involved in this project where a thorough literature review was conducted to gather the necessary details for understanding the underlying technologies such as Blockchain, Identity Management, Ticketing and Mobility-as-a-Service;
- Chapter 3 uncovers the current Blockchain-based solutions for the mobility industry as well as for identities;
- Chapter 4 presents the use cases at the scope for this project, describing its stakeholders and requirements;
- Chapter 5 presents the proposed final architecture for the solution by analysing multiple platforms to accommodate the project use cases.
- Chapter 6 describes the implementation process of the envisioned solution described in the previous chapter. This chapter explores each chosen platform and how it was used to achieve the final goal of this project;
- Chapter 7 presents the performance evaluation conducted and, consequently, the results achieved by each component of the overall solution and also discusses tests results;
- Chapter 8 presents concluding remarks of the work, the problems faced during the development, and the project's future work.

Chapter 2

Background

This chapter presents the essential concepts regarding Blockchain, Identity Management, Ticketing, and Mobility-as-a-Service. Allowing to set a background of terminology required to comprehend the technologies used.

2.1 Blockchain

Contracts, transactions, and their records are amongst the characterising structures in our financial, legal, and political frameworks. Such mechanisms protect assets and set organisational boundaries, establish and verify identities, govern interactions among nations, organisations, communities, and individuals. Until now, these critical tools and bureaucracies formed to manage them have not kept pace with the economy's digital transformation [12].

In 2008, an individual or entity writing under the alias of *Satoshi Nakamoto* published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System". The vision of Bitcoin is a Peer-to-Peer (P2P) version of electronic cash that would allow online payments to be sent directly from one party to another without going through a trusted financial institution [13] who processes and mediates the transaction. At first, the exceptionally high volatility of bitcoin and the attitudes of many countries toward its complexity restrained its development somewhat. However, the benefits of Blockchain technology and Distributed Ledgers are attracting massive attention triggering novel applications far beyond finance.

The concept behind Blockchain is essentially a distributed database of records, or a public ledger of all transactions or digital events that have been executed and shared among participating parties [14] across an overlay peer-to-peer network, not controlled by a single central authority. Several technological advancements such as cryptographic hash, digital signature, and distributed consensus algorithms enabled the decentralised environment of Blockchain; hence, an exchange can occur in a decentralised manner.

Applications of the blockchain technology go far beyond the finance world, branching

out to different market sectors such as, Automotive, Government, Healthcare, Insurance, Media and Entertainment, Retail and Consumer Goods and Travel and Transportation [15]. Here, only applications within the sectors of interest of this project are presented.

From issuing identification and registering property to administering elections and enforcing laws, government services face considerable challenges that blockchain can overcome. For instance, we rely on the government to accurately record and track our assets as citizens of a country. Thus, rigorous and accessible registries are crucial to increase trust and transparency in government systems that suffer multiple problems. Linking ownership of an asset to a single distributed shared ledger, enables governments to increase the efficiency of disseminating publicly held records. Moreover, identity is undoubtedly essential for both citizens and government agencies who issue and verify such records. Blockchain mitigates this issue by providing a solution that shifts the control over identity from government agencies to the citizen.

In a world where cities are getting bigger, travel and transportation environments are complex systems with enormous amounts of moving components. Current solutions for handling identification, tickets and boarding passes cause frustration to users. Therefore, a blockchain system capable of generating a single token of identification, valid throughout the entirety of the trip, as the potential to streamline boarding. Therefore, it would reduce both congestion and the need of multiple travel documents, offering a seamless travelling experience to the passenger. Also, blockchain is capable of encourage the interoperability between transportation modes, offering a trustworthy and transparent system for all service providers involved.

It can become a compelling tool for improving business, conducting fair trade, democratising the global economy, and support the creation of open and fair societies, which are the common goals all these applications share.

2.1.1 Architecture

At the core of the economic logic of cryptocurrencies lies the problem of conquering a solution for the double-spending problem in which the same single digital token can be spent more than once. Since digital tokens are, in essence, digital documents that can be tampered-with by duplication or falsification, it creates a real threat to digital currencies [16]. Bitcoin solves this problem with a novel Proof-of-Work (PoW) system characterised as the computational effort of calculating hashes spent on accepting blocks of transactions. A transaction is considered final once sufficient work has gone into generating a valid PoW for a submitting block [17].

The term blockchain is often miss-understood as Bitcoin. However, it can be defined as a sequence of blocks interconnected by hash references, which holds a complete list of multiple transaction records. Each block points to the immediately previous block called *parent* block via a reference, thus forming a “chain”. Since all blocks in the blockchain

reference the previous block, the starting block suffers from not having such reference. Typically, this reference is hard-coded with the default value of zero, hence why it is labelled “Genesis Block”.

The structure of a single block is divided into two components the *block header* and *body* as shown in Figure 2.1. In particular, the *block header* contains:

- *Block version* - Describes the structure of the data inside the block required for a correct reading of the block;
- *Merkle tree root hash* - All of the transactions inside the block hashed together;
- *Timestamp* - Current time as seconds in universal time;
- *nBits* - The encoded form of the target threshold which a block header hash must be in order for the block to be valid [18];
- *Nonce* - A number, which usually starts with zero, that participants increment to try and add candidate block to the blockchain;
- *Parent block hash* - A reference to the previous block.

The *block body* contains merely the list of transactions, within a maximum determined by the block size and the transaction size, and a counter of the transactions submitted to the block.

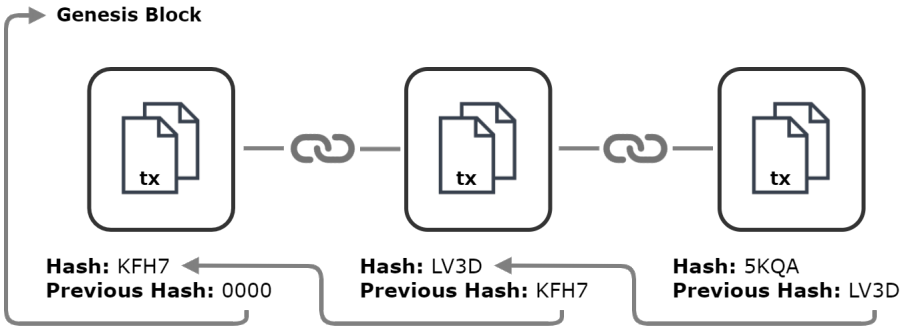

Figure 2.1: Blockchain and the block structure.

2.1.2 Key characteristics

As definied by Z. Zheng and colleagues [1, 2] blockchain has the following characteristics:

- *Decentralisation* - Centralised transactions require validation by a central trusted agency, coupled with the fact that conventional databases are owned and maintained by central trusted parties consequently generates performance bottlenecks. In contrast, one of the core characteristics of blockchain is its distributed ledger nature, which means that the database is maintained and held by all participants in the network. Once a new block of transactions is agreed within the network, each participant updates its own copy of the ledger.

- *Anonymity* - Users operating in a public ledger are identified by generated cryptographic addresses that do not reveal details about the identity of the user itself.
- *Immutable* - In traditional systems, the central server is a single point of failure as all the data is stored in one place. Also, if security gets compromised, it is possible to modify or permanently erase data. However, in a distributed ledger, once a transaction is added to the public ledger, it is nearly impossible to delete or rollback transactions. This immutability is secured through hashing of the blocks; therefore, the system is reliant on cryptography.
- *Auditability* - By being a public system, transparency of information is critical, therefore, everyone has access to the transactions.
- *Agreed by consensus* - Adding a block to the public ledger requires an agreement throughout all the participants (nodes) of the network. Consensus mechanisms are crucial in ensuring the integrity of the network since these protocols are the underlying rules for the consent collection regarding the ledger state.

2.1.3 Blockchain Types

Currently, blockchain systems are categorised into two main types , which define contrasting paradigms: public or *permissionless* and private or *permissioned* blockchains. This difference is based on three principles, namely, (i) who is allowed to participate in the network, (ii) execute the consensus protocol and (iii) maintain the shared ledger [19]. In a public blockchain network everyone can join and participate in the work which usually offers an incentive mechanism to attract more participants to join the network. The computational power of solving the PoW required to maintain the distributed ledger is one of the major drawbacks of public blockchains.

In contrast, a permissioned blockchain requires a permission to join. Generally, businesses who implement private blockchains, set a permissioned network which places restrictions to participants on who is allowed to participate in the network and in what transactions. This creates an added layer of privacy established by existing participants, a regulatory authority or a consortium. The comparison between these two types of blockchain is listed in Table 2.1.

2.2 Identity Management

Today, information systems are at the core of companies involved in increasingly complex value chains as well as on the Internet. Thereupon, the lines between users, service providers, and their competitors become blurred. Companies, therefore, need to implement flexible and efficient business processes focused on the electronic exchange of data

Table 2.1: Comparison between public and private Blockchain based on [1, 2].

Property	Public Blockchain	Private Blockchain
Read Permission	Public	Public or Restricted
Immutability	Nearly impossible [1]	Possible [2]
Efficiency	Low	High
Centralised	No	Yes
Consensus Process	Permissionless	Permissioned

[1] Nearly impossible to tamper since 51% of total network power is required
[2] Possible to tamper by having majority over the consortium or by the dominant organisation

and information. Such processes require reliable and secure identity and access management solutions. In the era of emerging threats of social engineering, phishing, and spoofing, the identity term becomes more complex, taking the answer to the question "Who are you?" to a whole other dimension [20].

There are many problems with the current state of identity systems. Digital identity is fragmented and siloed between various service providers, prohibiting a holistic view, and delivering poor user experience necessitating repetitive registrations and logins with usernames and passwords. This results in insecure systems where people use the same password for many of their sites. The centralised servers of identity providers like Google and Facebook are honeypots of data, so they are economically valuable for hackers to attempt to crack. The upcoming reliance on billions of internet-of-things devices makes it untenable to have all those devices controlled by a centralised identity provider, since a breach of the latter would prove catastrophic to not only digital but also physical infrastructure.

Identity management is a concept consisting of the processes, people, and technology used to create the assertion of unique identity for users or systems, based on a set of credentials, identifiers and attributes. Many private institutes or government organisations need personal information from users to provide them with the required services. A traditional Identity Management System (IDMS) usually store the credentials of each user they interact with in centralised databases hence creating concerns to the user. These concerns consists mainly of such databases being prone to breaches, and users not having control over their identity information. Due to the need for regulation, the General Data Protection Regulation (GDPR) was created to mitigate concerns of privacy of privileged information [21].

2.2.1 Identity Management Models

Identity Management Systems (IDMSs) are a fundamental foundation for cooperation between entities (i.e., people, associations, organisations or things) to support commerce,

education, health care, government services, and numerous different segments of society. An IDMS should allow entities to authenticate while simultaneously distribute information to enable the granting of access privileges by different levels or types [22].

According to [23], an IDMS usually involves multiple stakeholders that share interest in digital identities:

- Subject – Typically individuals also designated by users, whose identities are digitally recorded and used for numerous purposes;
- Service Provider (SP) – Provide different online services thus requiring the submission of proper credentials by users for granting access;
- Identity Provider (IdP) – Responsible for providing the users' identity data and related authentication results to the SP in a secure manner;
- Control party – Law enforcement agencies and regulatory bodies requiring access to identity information with auditing purposes for forensic processes.

An IDMS must strike the best balance between usability, security, privacy, and scalability. Therefore identity models evolved supporting these principles and were progressively modified for different use cases. Some leapt forward to enforce better scalability, others privacy or user control, consequently generating the following models, as stated by [3, 24].

Isolated Model

The isolated model is the traditional identity model in which the SP and IdP roles merge, hence identification and authentication are straightforwardly done at the SP itself. Furthermore, the functionalities of creating, maintaining, deleting and authenticating identities are implemented directly in the SP [24].

Simplicity is the crucial argument for implementing such a system model, although plenty of issues arise with the exponential growth of online services. Coupled with the fact that each SP requires registration by the user for granting access (Figure 2.2), assuredly, the diversity of credentials for accessing various service providers may become an unmanageable burden for users.

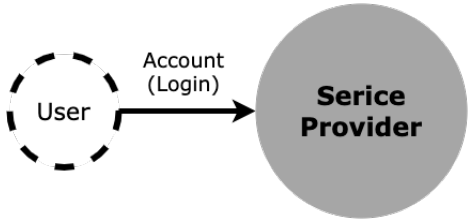

Figure 2.2: Traditional Identity Management.

Centralised Model

Central identity model mitigates the issue of diverse IDMSs where the user is required to register separately. Instead, user identity storage and user authentication is outsourced by several SPs to a central server called IdP, hence separating the roles of SP and IdP [3]. The IdP takes over all identity-related functionality for the SP, including credential issuance, storage, identification and authentication. Furthermore, all user's related identity data is transmitted to a single central authority (IdP), depriving the SP of holding the users information in their repositories. As shown in Figure 2.3, all the identities of every SP are stored in an IdP. When the SP needs to authenticate an user, a request is sent to the IdP which will send the solicited information by assembling a token to finish the process.

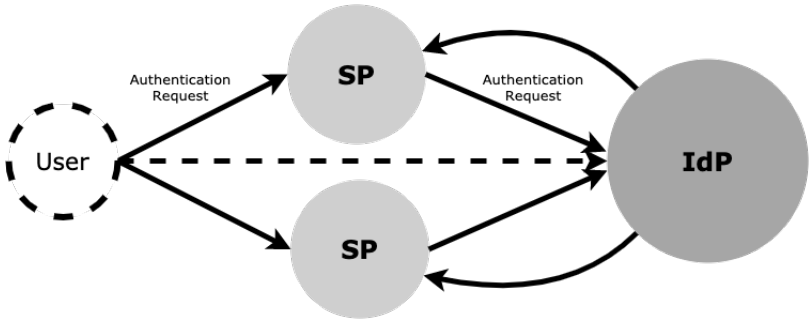

Figure 2.3: Centralised Identity Management.

Federated Model

The Federated Identity model represents the most modern and dominant model among the ones previously discussed. Although the centralised model requires the users in the same domain or network, in the federated model identity data is distributed across multiple IdPs and/or SPs making it a virtual global unique domain. Federation can be defined as the set of agreements, standards and technologies that enable a group of service providers to interoperate recognising users identity within a federated trust domain. The identity information of a particular user is distributed and linked usually by the help of a common identifier, thus no single entity is in full control of the identity.

A single identifier and credential are sufficient for the user to access all services in the federated domain. Therefore, this model provides the means to implement a Single Sign-On (SSO) solution with a significant drawback of requiring the management of multiple credentials by the user. The designation of SSO originated from the requirement of one single authentication to access all the services from different SPs.

User-Centric Model

The user-centric IdM model paradigm places the user in control of its own identifiers and credentials, thereby empowering it with total control over identity and authentication, and the attribute exchange process. Moreover, the user-centric identity model addresses the scalability problems of previous models and provides services similar to SSO. With an uncontrollable increasing number of identifiers and credentials, and supposing that the usability is inadequate, it leads to a weak authentication as users rapidly become unable to manage their credentials properly [25].

According to [26], digital identities can be achieved simply by letting the users store identifiers and credentials from different SPs in a single tamper resistant hardware device (e.g. Smart Card) or some other portable personal device. Figure 2.4 demonstrates that users can access services from any service provider accepting their credentials.

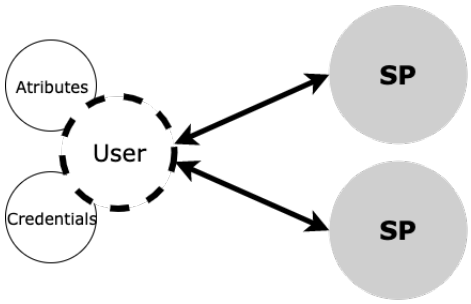

Figure 2.4: User-Centric Identity Management.

Comparison

Identity Management (IdM) models present characteristics such as SP type, IdP type, service composition, cross domain access, identity storage, user control over identity and privacy protection. Table 2.2 presents a comparison of the formal four models.

In summary, the isolated model merges SP with IdP for a single service. Therefore, it does not support cross domain access and identity control. Identities are stored in a local, isolated domain with insufficient security against attacks. However, the centralised model offers multiple SPs on a limited domain, yet only a single IdP. Cross domain access and user control over identity have little support and present a few mechanisms for protection. Lastly, federated models support numerous SPs, IdPs and services across multiple domains, offering users control over identities stored on SPs or IdPs.

2.2.2 Standards

The most relevant initiatives to standardise IDMSs are Security Assertion Markup Language (SAML) [27], OAuth 2.0 [5] and OpenID Connect [28]. All the standards men-

Model	SP Type	IdP Type	Service Composition	Cross Domain Access	Identity Storage	User Control over Identity	Privacy Protection
Isolated	SP acts as IdP	SP acts as IdP	Sole service	No support	On SP	No control	Low and very weak security
Centralised	Multi SPs	Single IdP	Multi services in the same domain	Limited support	On IdP	Few control	High but weak security
Federated	Multi SPs	Multi IdPs	Multi services across domains	Nearly fully supported	On both SPs and IdPs	Much control	High and strong security

Table 2.2: Comparison of IdM models based on [3].

tioned above were considered for later integration in the project, however, only the OpenID Connect standard was used, which is detailed below.

OpenID

Originally, OpenID was a visionary tool that never got much commercial adoption. However, it got industry leaders pondering what was conceivable. The successor OpenID 2.0 brought a more robust system, offering excellent security, and working well when appropriately implemented. However, it suffered from several design limitations such as relying on the XML format, and Relying Parties could not be applications, thus leading to some adoption problems. OpenID Connect 1.0 is the third generation of Open ID technology [28], which is a simple identity layer on top of the OAuth 2.0 protocol. Enabling clients to verify the identity of end-users based on the authentication performed by an OpenID Provider, and additionally obtains the user essential identity attributes using interoperable RESTful services [29]. Hence, this protocol adds IdM functionality to the OAuth 2.0 system.

A Client (i.e. Relying Party) aiming to authenticate a user receives the authentication information as an ID Token from the OpenID Provider (OP) in JSON Web Token (JWT) format. As shown in Figure 2.5, the OpenID Connect protocol, in abstract, follows the pictured flow to obtain to final ID Token. The relying party, sends a request of authentication to the OpenID Provider (OP) (1). Such request requires an authorisation by the user which is requested by the OP which authenticates the user (2). After user identity confirmation, the OP responds to the RP with an ID Token (3). From this point forward the RP, in possession of the user's ID Token, is able to request the OP about the user information (4)(5).

2.2.3 Blockchain Identity Management

Identity Management challenges are an inherent concept since the creation of the Internet with its ancient centralised identity systems. The problems with the current state of identity systems can be further explained as, an ever increasing number of credentials, lack of validated identity information, single points of failure, and vulnerability to attacks, that have plagued organisations for years as customer volumes increase. A possible solution

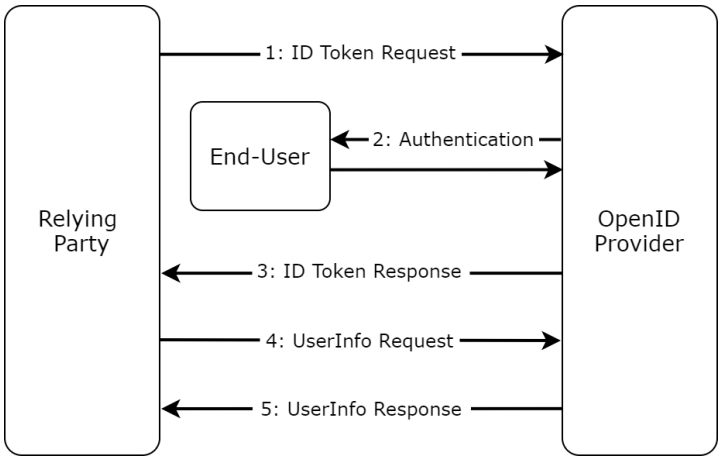

Figure 2.5: OpenID Connect Protocol Flow.

for these issues can be found with the use of the blockchain technology providing the opportunity for fully decentralised IdM system. The decentralised nature of DLT empowers people with control over their data and achieves greater security against unauthorised users. Furthermore, it enables a direct interaction between user and relying parties with verified information, therefore, making the sharing of identity information more seamless, safe and secure.

Standards

The novelty of blockchain-based IDMS led to a set of emerging standards including:

- **Decentralised Identifiers (W3C)** – Decentralised Identifier (DID) is a new type of identifier to provide verifiable, decentralised digital identity, thus, enabling the controller of a DID to prove control over it and to be implemented independently of any centralised registry, identity provider, or certificate authority [30]. Entities (e.g. person, organisation) are identified by DIDs which facilitates credential exchanges and authentication processes by using proofs for instance, digital signatures and privacy-preserving biometric protocols. An entity can have multiple DIDs representing relationships with other entities. Ownership of a DID is established by presenting the corresponding private key associated with the specific DID.

- **Verifiable Credentials (W3C)** – A Verifiable Credential is a digital document that can represent the same information as a physical credential. The addition of technologies, such as digital signatures, makes verifiable credentials, cryptographically signed by its issuer, more tamper-resistant than their physical counterparts. This specification defines a format for credential exchange between DIDs [31].

  Also, it defines the concept of Verifiable Presentation, which is a tamper-resistant presentation of a Verifiable Credential signed by the DID subject disclosing it.

- **Universal Resolver (Decentralized Identity Foundation (DIF))** – The vision of this standard is to develop an universal DID resolver by providing a unified interface for fetching DID Documents of different decentralised systems such as the Bitcoin blockchain, Sovrin, Ethereum, IPFS, and others. In order to support the Universal Resolver, a DID Driver must be implemented by DID-based blockchain IDMSs for linking the resolver with system-specific DID Method of DID Document reading. This allow applications to use a common interface for querying multiple decentralised IDMSs solving the pain of fetching the system-specific methods [32].

- **Identity Hubs (Decentralized Identity Foundation (DIF))** – An Identity Hub, which can be constituted by one or more Hub instances, is a set of encrypted personal off-chain datastores, interconnected by edge devices (e.g. mobile phones) and cloud storage. Moreover, Identity Hubs can run on personal devices or be hosted by a provider [33].

- **Open Badges (Mozilla, IMS Global)** – As another approach to digital credentials, Open Badges are visual tokens of achievement, affiliation, authorisation, or other trust relationship that is sharable across the web [34]. To improve the interoperability between the thousands of credential issuers around the world Open Badges are expressed in JSON-LD format, which can be encoded into Quick Response (QR) codes enabling easy integration into various applications. The specification identifies three core data classes used to instantiate a badge: *Assertions* which contain data about an awarded badge belonging to an entity, *BadgeClass* adds context to the type of credential and points to the issuer who defined it with its issuer properties, and *Profile* is a collection of information describing the entity or organisation using Open Badges.

Self-Sovereign Identity

Inheriting notions of user-centricity, Self-Sovereign Identity (SSI) is the latest emerging paradigm for IdM models supported by Blockchain, DLT and encryption technology to create immutable identity records. Moreover, this approach allows individuals to fully own and manage their lifetime portable digital identity without depending on a centralised authority for identifier origination or credential issuance, leading to the idea of "self-sovereign" identity systems (i.e., users exist independently from services).

The Sovrin Foundation [35] grouped Christopher Allen's "Ten Principles of Self-Sovereign Identity" [36] into the three categories, *security*, *controllability*, and *portability* presenting the requirements for implementing the SSI concept in a system (Table 2.3).

The main actors of SSI are presented in Figure 2.6 and can be described by the relations between them. The claim issuer issues the identity by attesting to specific attributes of the user, which is then stored and controlled in the user's domain. A relying party that

Security	Controllability	Portability
Protection	Existence	Interoperability
Persistance	Control	Transparency
Minimisation	Consent	Access

Table 2.3: Ten Principles of Self-Sovereign Identity

requires an identification is presented only with the relevant information. To accept and verify the validity of the information, the relying party must have a trustful relationship with the claim issuer.

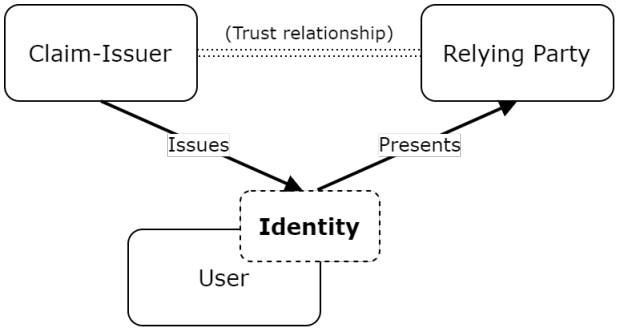

Figure 2.6: SSI Actors.

A general underlying architecture for these systems is described in Figure 2.7, where the relation between the four essential components needed in an SSI system is explained (i.e. identification, authentication, verifiable claims and attribute storage). The blockchain, referred to as identifier registry, acts as a replacement for the registration authority present in the most traditional IDMSs.

The identifier is unique for a specific user by use of an authentication method such as asymmetric cryptography. By generating a relationship between an identifier and public key on the blockchain, the identifier can be verified by anyone reading the blockchain by posing a challenge.

2.3 Ticketing

Initially, tickets were emitted on paper, passes or counter tickets, which were validated by punching holes on the card for each journey. The functionalities of paper tickets were particularly limited to counting the number of trips realised. Innovations took place in the public transport industry and paper tickets with magnetic stripes were introduced. This advancement allowed novel opportunities for transport operators since the functionality of reading and writing information from/to the magnetic stripe was finally a reality. The transfer rights could be granted automatically by a set of specific business rules on the validation process. Therefore, transferring between vehicles only by sliding the card on

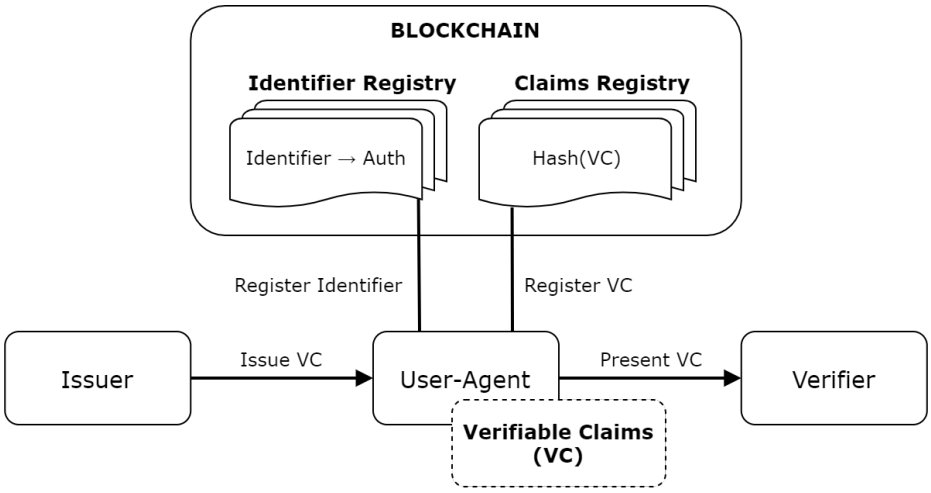

Figure 2.7: Self-Sovereign Identity Architecture.

the validator became a possibility. The latest innovation in this sector was the implementation of smart cards or smart tickets, which featured an extended memory and processing capabilities [37].

In a traditional card-centric ticketing system, tickets are stored in the customer media. Even if tickets are replicated on a central server, the content of the customer media is decisive. Real-time processing of tickets is generally carried out by front office terminals which require an individual and proprietary application software to obtain a certain level of intelligence. This application software necessitates comprehensive tariff schemes and processing on connected equipment leading to sophisticated software. Therefore, these systems require a high degree of setup of both software and hardware, thus presenting an elevated upfront, maintenance and upgrade cost [38]. However, card-centric systems are resilient to network failures since all the processing is executed offline.

Moreover, in card-centric approaches to ticketing, the rights/value available for use are stored on the card. Front-office systems must validate the information, and during such process, the validator checks that the card is genuine and that appropriate rights/-value are present. The process of validating requires consuming the rights/value present on the card, updating the data, producing feedback to the user regarding the validity of the transportation title, and sending this transaction to the back-office. Card-centric systems relying on front-office validators produce an instantaneous result without requiring accessing the back-office, mainly by the fact of card-terminal transactions being secure and immediate. One main drawback of this system is the synchronisation and management of data, thus resulting in limited flexibility and complex synchronisation processes.

The non-profit association Calypso Networks Association (CNA) [39] is a major player in developing standardised solutions suited to transport and mobility needs. Calypso is an international electronic ticketing standard for microprocessor contactless smart cards, ensuring interoperability between multiple transport operators in the same area.

The founding members of this project include OTLIS-Lisbon, ACTV-Venice, STIB-Brussels, LKRKN-Constance, and RATP & SNCF-Paris [40]. The previous information is based on Calypso's Whitepaper [37] which is a reference for Account Based Ticketing (ABT) further explained in the next subsection.

2.3.1 Account-based Ticketing

An ABT system is a ticketing system where the data on the travel rights and tickets are stored in a central server linked to a customer account. The portable object only serves as a mean of identifying the customer. The software processing of the fare media is then carried out by the central server [9]. In other words, ABT empowers the transport operators to relocate the fare calculation software and logic to the back office where the user accounts are present, thus approximating these cooperating systems.

ABT emerged as a result of an ever-increasing throughput, reliability and speed of data communications, coupled with an increment in processing speed of card technology. However, full online validation is not yet possible, hence why ABT often stays partially card-based. The latter means that a local validation can be processed without the need to connect with the back office.

The new approach to ticketing is particularly relevant for occasional users and new services since 80% of the journeys in public transport systems are done by people with passes. Thus, the creation of a solution that is both easy to understand and simple to use is the upmost priority. Notably, the main goal is not to replace existing passes, but to offer new services for occasional users or to offer complementary services to people with passes [37].

Card-centric vs. System-centric

ABT systems are system-centric approaches that distance themselves from legacy media centric ticketing solutions, and once in place offer a wide range of benefits. A system centric approach, with a better business case, provides new services which are not available today for customers due to the costs involved. There is a high adoption rate of ABT by new small ticketing schemes since they cannot afford to implement a card centric ticketing. For complex networks, ABT is a strong opportunity to improve the tariff possibilities with a dedicated target in mind, the occasional user. Therefore, this approach offers an architecture that enables multi modal and multi service approach, increasing the opportunity for greater interoperability between SPs.

2.3.2 Ticketing for MaaS

Currently, when designing or renewing a ticketing system, there is a plethora of technologies, architectures, customer media (e.g., NFC or QR Code, card-centric or server-centric,

prepaid or post-paid) to select that may become overwhelming for transport providers. However, the effectiveness of ticketing lies in its flexibility and the ability to meet new needs over the entire lifetime of a system. Several requirements arise throughout the life cycle of a single ticketing solution, such as new fare media, new services for customers, implementing interoperability schemes, fare updates, integrating new transport providers, and so on. Hence, it is essential to choose the right tools; otherwise, implementing the requirements above may become a huge burden or present high costs [9].

According the recommendatios of J. Eppe et al. [9], a ticketing system for MaaS must enable evolutions and upgrades throughout its life-cycle, which usually lasts up to 20 years. Therefore, it is essential to make the correct decisions right from the beginning of development and ensures the capability of the system to evolve to new technologies. All these recommendations converge towards a common goal of enabling interoperability amongst SPs regardless of the architecture model chosen (i.e., card-centric, ABT, Open Payment). Furthermore, the singular recommendations presented next highlight the best practices to help ticketing systems reach their target qualities and performance.

After often having been wrongly perceived as only a mean of payment for transport, MaaS takes advantage of ticketing as the access gateway of mobility for all. New ticketing systems must take advantage of new technologies such as contactless tickets delivering significant benefits to customers, operators, and transport authorities. This form of ticketing improves the customer experience by implementing a fluid and simple way for validation, facilitates network operations and implements fare policies thanks to the technical performance of the media, has mechanisms against fraud, and facilitates interoperability. Therefore, contactless ticketing promotes the implementation of a MaaS ecosystem due to its accessibleness and open nature. Hence, it offers a solution for facilitating a means to access all forms of mobility within this new system.

To implement a ticketing system is costly, meaning that it represents a significant investment for operators. Such investment must consider the system maintainability, ensuring that, the scalability of the system is not compromised, it stipulates a high level of security, and enable easily adapting fare policies, while minimising the total cost of ownership. Minimising the initial investment, neglecting the total cost of owning the system (i.e., maintenance and operation costs), is usually associated with a ”black box” design without any control. Furthermore, these ”black box” proprietary solutions tie the transport operator, and generally, the supplier of the system can practice an unfair price for changes. The best strategy is to follow implementations that rely on open and standardised solutions and open-source software. The latter is necessary when a network wants to become interoperable, facilitating the communication between contactless media and terminals. These ideas are illustrated below in Figure 2.8.

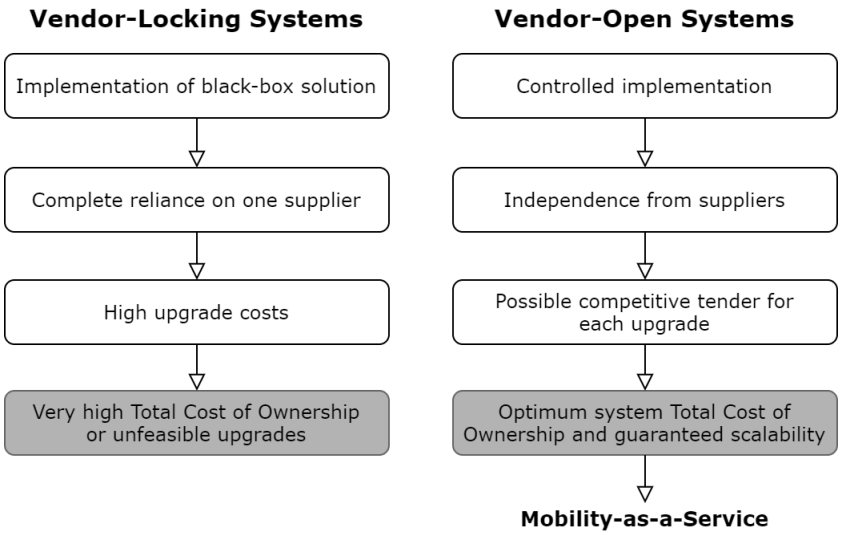

Figure 2.8: Proprietary vs Open Ticketing System.

2.4 Mobility-as-a-Service

In recent years mega-trends such as hyper urbanisation, climate change, globalisation, digitisation, and demographic shifts affected transportation as it is ([41]). Therefore, the current *modus operandi* in transport supply is deemed unsustainable. Such realisation has generated the need for innovative services that could better manage the existing fleet. A new paradigm shift emerges fuelled by a myriad of innovative new vehicle-sharing service providers and the anticipation of self-driving cars, especially in combination with public transport, paving the way for novel opportunities for new types of personal transport services. The fundamental objective is to merge private and public transportation to provide a sustainable and equally convenient alternative to personally owned modes of transportation.

The acknowledgement of such a shift in mobility has revolutionised the development of new concepts. Mobility-as-a-Service (MaaS) originated as a potential outcome of the union between the smartphone technology and shared autonomous electric vehicles. Heikkilä's master's thesis, "A Proposal for Action for the Public Administration, Case Helsinki" ([8]) promoted the widespread of the MaaS ideology. Since then, the term has rapidly gone from nowhere to nearly everywhere in the personal and public transport sector with new approaches emerging frequently. MaaS aims to bridge the gap between public and private transport service providers on a municipal, national, or even international level. It foresees the centralisation on a single digital platform the currently fragmented tools and services a traveller needs to conduct a trip (planning, booking, access to real-time information, payment, and ticketing). Is has the potential to eradicate the dependence on private vehicles and deliver seamless mobility through the bundling of transport services as one product since it allows integration and cooperation across multi-

ple transport service providers. Through MaaS, travellers could have access to accessible, flexible, reliable, price-worthy, and seamless everyday transit from A to B that includes combinations of public and on-demand transport, shared vehicles, and car leasing. MaaS triggers new concepts for mobility; e.g., users can buy either all the modes needed for a trip (pay-as-you-go) or monthly mobility plans based on their needs, through a single interface.

2.4.1 The MaaS Concept

The concept of MaaS is yet in its preliminary stages, which results in a high degree of ambiguity. According to Jittrapirom [42] "MaaS can be though as a concept (a new idea for conceiving mobility), a phenomenon (occurring with the emergence of new behaviours and technologies) or as a new transport solution (which merges the different available transport modes and mobility services)".

Currently, to find information and purchase a journey, the user is forced to navigate through multiple singular tools from different transport modes. Travellers often use numerous tools for journey planning. However, only a small number of journey planners offer information for intermodal trips (i.e., involve the use of more than one mode of transport for a journey) or either integrate a limited number of transport modes. Moreover, the user is bound to utilise multiple payment methods for each transport operator along with the generation of multiple travel titles, which might be overwhelming. These pain points represent a small portion of the pain points that deteriorate mobility and hinder intermodality, not promoting sustainable travel behaviours.

MaaS aims to reduce most of the aforementioned user-related pain points. The MaaS provider is the intermediary in the communication between transport operators and users. By using the data of services offered by the transport operator and buying capacity from them, the MaaS provider is capable of reselling the services to the customer at a fair price. Users are empowered with the use of one single interface to discover journey information by choosing the preferred modes of transportation. This solution enables the suggestion of the ideal combinations of transport modes for each trip by gathering real-time information and the preferences of the user, hence optimising the supply and demand at any time.

The core vision of MaaS is the aggregation of not only the transport operators in the same city yet also across different cities, shifting the paradigm towards a cooperative and interoperable ecosystem. Figure 2.9 demonstrates the current situation for urban and intercity trips from the user's usability standpoint and the innovation that a novel MaaS system by using a single solution for accessing multiple transport providers.

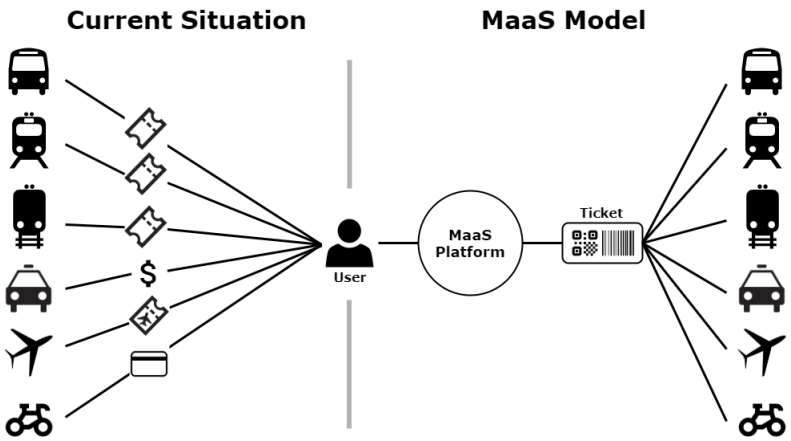

Figure 2.9: Comparison between traditional and Mobility-as-a-Service model.

2.4.2 MaaS Technology and Data Requirements

The MaaS paradigm relies heavily on the data exchanged between cooperating parties, hence data providers represent a key role in this type of system to ensure greater data interoperability. To accomplish this objective it is critical to consider every type of data standard (regional, national, international) and protocols need to be proposed on a central policy level and therefore, adopted by transport operators.

Accordingly, open data stores could adequately leverage the MaaS concept by conceiving policies and standards to support secure open data and sources, that would highly foster the scalability and operability of the MaaS system [43]. Gathering route, vehicle positioning, network conditions, ticketing and booking data from transport operators within the system it's essential to the development of MaaS platforms.

Chapter 3

Related Work

3.1 Blockchain in MaaS Solutions

As of the writing of this report, these are the concrete solutions found that seek to connect Blockchain and DLT with MaaS. Please note that innovations in the space of blockchain integration with public transportation come primarily from private ventures or individuals volunteering in working groups.

3.1.1 TSio Protocol

The TSio Protocol is a solution by TravelSpirit Foundation which aims to enable both private and public mobility providers to compete in a transparent MaaS marketplace that is focused on providing personalised user-centric services to anyone and everyone [44]. Furthermore, TSio Protocol enforces contractual agreements with smart contract mechanisms in order to establish an equitable and open market. The design objectives for the TSio Protocol are empower the user to access multiple transport services through a single interface, enable interoperability and roaming capability between transport operators, reduce costs of low-value payments for transport providers, provide low latency network with fast verification, prevent fraud and attacks, and manage personal data.

3.1.2 Tesseract

EY OpsChain Tesseract is a blockchain-powered platform supporting new mobility businesses built around fractional ownership of vehicles, multimodal transportation integration and new investment models. Tesseract envisions a single blockchain-based platform where single vehicles, fleets and other transport services are available to support an integrated and autonomous future of mobility. Vehicles and trips are digitally stored in a blockchain ledger hence promoting an automatic settlement between owners, operators and service providers, through a single payment system. By using blockchain assets such as cryptocurrency, asset tokens, and smart contracts, enables a system where in-

stantaneous and immutable occur without an intermediary, a transparent record of digital ownership with tokens, and automation of the transaction process with smart contracts [45].

3.1.3 IoMob

IoMob's open platform moves mobility beyond traditional MaaS, into a world of fully connected mobility marketplaces. That is, any provider, app, anywhere and anytime [46]. At the core of the IoMob architecture is the IoMob Protocol, which is used by mobility providers to announce the services they offer on the platform. The protocol supports a wide variety of transportation modes, aiming to build a system general and permissionless enough that any organisation or individual can participate on the network.

Announcements of services by messages through the protocol is standardised. These messages are redirected to mobility hubs, which store the information from multiple services providers, and provide a standardised API for end-user applications to request the required information for a specific journey. If the end-user purchases the services through the app, that information is sent back to the hub which relays the specific information of the corresponding SP. The revenue sharing among players is coordinated by the smart contracts of IoMob which enforce specific agreed terms. Furthermore, this allows participants to trust the network for agreements instead of establishing explicit partnerships [47].

3.1.4 Transit Protocol

Transit Protocol aims to transform mass public transportation to provide a seamless commuting experience for urban environments. Furthermore, this multi-modal transport protocol on the blockchain enables the aggregation of different mobility services into one platform [48]. Transit Protocol is the blockchain platform of the end user solution TransitLink. A single app brings every mode of transport together handling the full experience of journey planning, single payments, and dynamic journey adjustments. The project is focused on city transport companies in China to provide an infrastructure for QR Code acceptance and contactless payments.

3.2 Blockchain-based Identity Management Solutions

The current state of traditional identity management presents a wide range of problems described in Section 2.2.3. Hence, a possible solution for these issues may be present in the use of blockchain and DLT for IdM, accomplished by removing the need for traditional credential service providers and enabling direct interaction between user and relying party. Blockchain-based IDMSs have the potential to greatly enhance security and

privacy and enable built-in control and consent capabilities for both users and relying parties.

Although more solutions are emerging, the following are the most prevalent throughout the literature as being individually key exemplars of the current design decisions.

3.2.1 uPort

uPort [49] is an open source framework, built on top of the Ethereum Blockchain, that aims to provide decentralised identity for specific services such as emailing and banking. Considering the chosen platform, Ethereum Smart Contracts form the core of the identity underpinned by the interactions of contracts. In case of losing the mobile device, the underlying logic of contracts enable the user with methods for recovery of identity. Smart contracts are uniquely addressed in the system by a 20-byte hexadecimal token acting as a globally unique, persistent identifier. The main system components are two smart contract templates, namely *controller* and *proxy*, that comprise each uPort identity.

Figure 3.1 provides an overview of the general architecture of uPort, illustrating an interaction between a uPortID and the smart contract of a decentralised application on Ethereum. In order to create a new identity on the uPort platform, a user's mobile application generates a new asymmetric key pair and sends that information as a transaction to Ethereum.

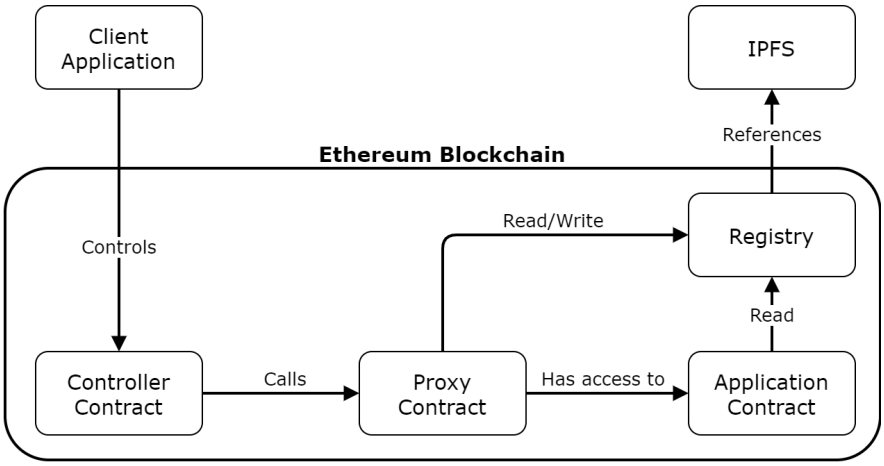

Figure 3.1: An overview of key elements of uPort architecture.

3.2.2 Sovrin

Sovrin is an open-source, decentralised identity network [35]. Since only trusted institutions, called *stewards*, operate Sovrin ledger nodes for consensus purposes, this approach is built on permissioned DLT. Two premises are behind the choice of a permissioned ledger: eradicate expensive PoW and trust relies on both people and code. Firstly, using

Plenum, i.e., a Byzantine fault tolerant consensus protocol with no PoW, reduces the energy cost of running a node and improves transaction throughput. Secondly, the vision is a "web of trust" starting by the common root-of-trust, the distributed ledger. However, new organisations can become "trust anchors" allowing them to add more users. The Sovrin Foundation sole purpose is the proper governance of the ledger by approving trusted institutions, who support the goals of Sovrin Foundation, to operate Sovrin ledger nodes. Sovrin is directly tied with the Hyperledger Indy project, providing its code base for developers.

The Sovrin architecture presented in Figure 3.2 summarises the main components of this IDMS. Moreover, the Sovrin legder contains transactions associated with specific identifiers, which are distributed and replicated among all *stewards*. The identifiers follow the DID standard, explained in Section 2.2.3. A single user is allowed to create and manage multiple identifiers as one pleases to increase privacy by separating identities as each identifier has a different asymmetric key pair.

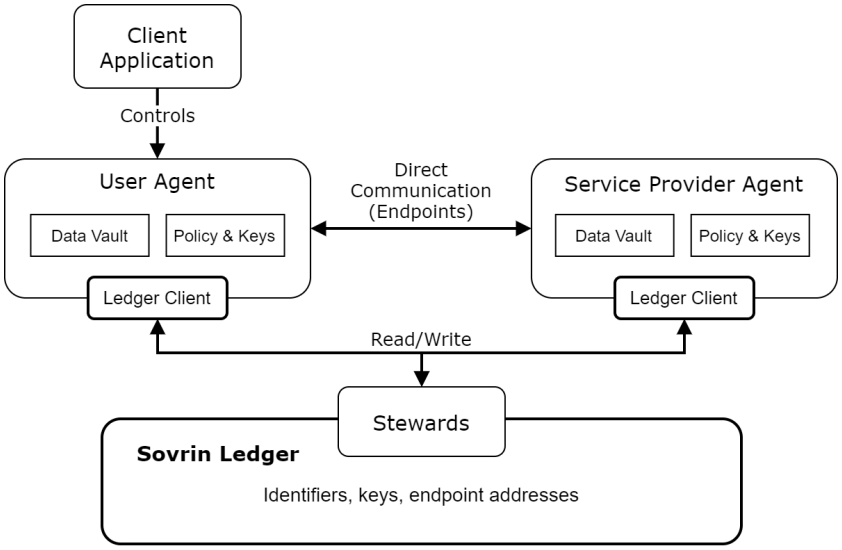

Figure 3.2: An overview of key elements of Sovrin architecture

3.2.3 ShoCard

ShoCard is an identity ecosystem supporting the concept of SSI, which lets the user decide with whom to share personal data and allows third parties to validate the authenticity of data [50]. It aims to combine a user identifier with an existing trusted credential (e.g., identification Card, passport, driver's license), and additional user attributes together. ShoCard handles storage by using the Bitcoin platform for timestamping signed cryptographic hashes of user's identity information.

ShoCard is a blockchain-based identity authentication platform supporting the concept of SSI, enabling the user to decide with whom to share personal data and allows

third parties to validate the authenticity of data. It aims to combine a user identifier with an existing trusted credential (e.g., identification Card, passport, driver's license), and additional user attributes together [51]. ShoCard handles storage by using the Bitcoin platform for timestamping signed cryptographic hashes of user's identity information, which are mined into the Bitcoin ledger. The ShoCard server acts purely as an intermediary for storing certifications exchanged between users and a relying party, thus generating an EnvelopeID for each certification as future reference. As stated by S. E. Haddouti et al. [4], the scheme relies on three phases: bootstrapping, certification, and validation. Figure 3.3 demonstrates the flow of processing transactions in a ShoCard system.

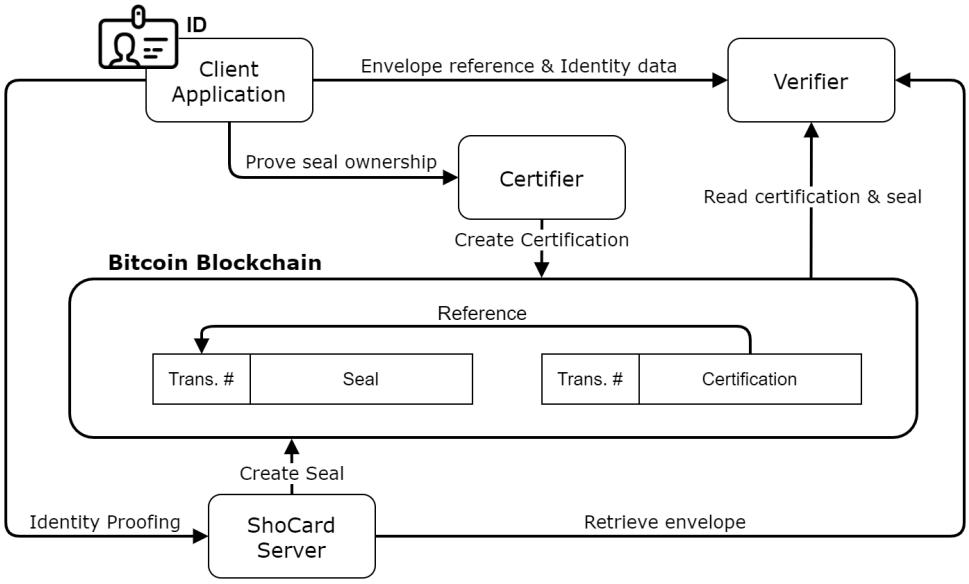

Figure 3.3: An overview of key elements of ShoCard architecture.

3.2.4 Comparison

Table 3.1, presents a comparative analysis of the aforementioned Decentralised IDMSs. The previously described solutions are all unique in their way. Hence no single solution is perfect, presenting both benefits and downsides. The advantages of integrating DLT in IdM are prevalent throughout the table, however, regarding Cameron's Human Integration premise [52], there is a noticeable lack of understanding by these systems in the department of User Experience (UX). Moreover, in the case of uPort and ShoCard, both deliver a mobile application, yet the usability is unclear, coupled with a scarcity of information about the user's privacy implications. Sovrin's solution is still under development, therefore an interface for the end-user is still missing. Additionally, even when the primary goal of such a system is the decentralisation of the authority for identities, a significant problem arises due to the profound demand for trust in every IDMS. Consequently, creating a challenge for designing immutable public ledgers that reference users' data, and at

the same time providing the required transparency over the data stored publicly.

Requirements	uPort	Sovrin	ShoCard
User control and consent	✗	✓	✓
Minimal disclosure for a constrained use	✓	✓	✗
Justifiable parties	✗	✓	✗
Directed identity	✓	✓	✓
Design for a pluralism of operators and technology	✓	✓	✗
Human integration	✗	✗	✗
Consistent experience across contexts	✓	✗	✓

Table 3.1: Comparison of Decentralised Identity Management Solutions based on [4]

3.3 Blockchain-based Ticketing Solutions

Currently, only a single solution was found regarding the interconnection of DLT and public transport ticketing systems. The focus of this solution is mainly the ticket creation and the consequent revenue distribution of multiple service providers operating in a MaaS ecosystem.

3.3.1 Planar Network

Planar Network is a platform for public transport tickets that integrates operators from different geographical regions and different modes of transport onto a single network [53]. By using DLT and smart contracts, the platform aims to provide a single source of truth for all tickets created, real time financial settlement between retailers and operators, and a single platform for customers to buy tickets from multiple SPs in a single transaction.

Only a set of trusted transport operators is permitted to offer contracts for transport between specific geographical regions of the broader network. A single operator has permission to create Fares on a set of Flows, therefore, defining a region in which they operate. A Flow is a subsection of the network, including an origin and destination station and a route code which determines the intermediate stops. Fare is an asset created by Operators consisting of a flow, validity duration, and price, in order for Retailers to offer travel tickets. A ticket creation contract is executed, requiring a Fare and money as input, to produce a final Ticket on the Blockchain. Figure 3.4 describes the connection between all the components for generating a ticket. This ticket gets associated with a wallet with a public and private key, that is required in a Blockchain environment for ownership of assets. Only the owner of a wallet can sign transactions using its private key for transactions involving the wallet.

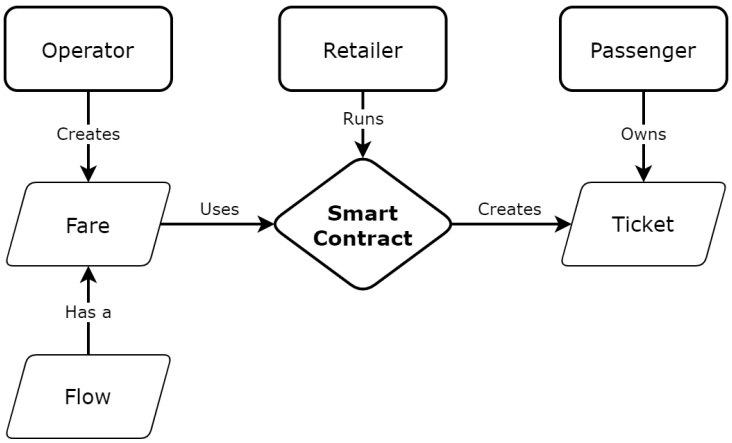

Figure 3.4: The Ticket Creation Smart Contract.

3.4 Discussion

Blockchain technology enables many processes and transaction services to be more transparent, decentralised, democratic, and secure without the need of a third-party organisation in the middle. It is possible to conclude that a vision of a Blockchain-based MaaS solution is indeed a reality, ensuring greater cooperation between transport providers and personalised user-centric service.

The closest approximations to the project's final goal are TSio Protocol, Tesseract, IoMob, and Transit Protocol solutions, which aim to build a Blockchain-based MaaS system. Each individual solution tries to create the MaaS concept based on the Blockchain technology with support for both transport providers and end-users, offering identity management solutions for users and companies with a single source of truth for ticket generation and financial settlement. However, the lack of technical documentation of such solutions hinders innovation in public transportation systems globally since every solution is, currently, being developed in a siloed manner.

Blockchain-based Identity Management solutions are still in its infancy, however still present some issues. In the case of uPort, the centralisation of JSON registries represents a single point of failure to the system facilitating the leak of attributes' meta-data. Sorvin's solution presents a significant limitation of locking users to this solution, and a missing client application makes the user experience an aspect left out for consideration. Finally, in spite of ShoCard supporting a multitude of identity providers, it is still unknown the users' willingness to use such a system and the implications of storing and managing their identity on the Blockchain.

As for public transport ticketing implementations in Blockchain, a single solution was found throughout the research process. Planar Network leverages the use of smart contracts to achieve a single source of trust for all created tickets. Such implementation allows excluding intermediaries in the business process, increasing profit margins, and

enabling real-time financial settlement. Also, smart contracts provide speed, safety, and confidentiality for business-to-business interactions by eradicating the need for paperwork and storing encrypted data in the distributed ledger.

Bibliography

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, June 2017, pp. 557–564.

[2] H. Wang, Z. Zheng, S. Xie, H.-N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, pp. 352 – 375, 10 2018.

[3] Y. Cao and L. Yang, "A survey of identity management technology," in *2010 IEEE International Conference on Information Theory and Information Security*. IEEE, 2010, pp. 287–293.

[4] S. E. Haddouti and M. D. Ech-Cherif El Kettani, "Analysis of identity management systems using blockchain technology," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, April 2019, pp. 1–7.

[5] D. Hardt, "The oauth 2.0 authorization framework," Internet Requests for Comments, RFC Editor, RFC 6749, October 2012, http://www.rfc-editor.org/rfc/rfc6749.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6749.txt

[6] S. Rothenberg, "Sustainability through servicizing," *MIT Sloan Management Review*, vol. 48, 12 2007.

[7] World Commission on Environment and Development, "Our common future," Oxford University Press, Oslo, Report 019282080X, mar 1987.

[8] S. Heikkilä *et al.*, "Mobility as a service-a proposal for action for the public administration, case helsinki," 2014.

[9] J. Eppe, R. Gambetta, N. Generali, P. Guillaumin, S. Merzouk, J. Rubel, F. Sykes, L. T. Costa, P. Vappereau, and V. Zajackowski, "Ticketing for maas," Calypso Networks Association, 76 rue Royale - 1000 Brussels, Whitepaper, jun 2019.

[10] OECD, "OECD Blockchain Primer," https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf, Organisation for Economic Co-operation and Development (OECD), Tech. Rep., 2018, (Accessed on 01/13/2020).

[11] Card4B - Systems S.A., "About us," https://www.card4b.pt/about.html, 2018, (Accessed on 11/07/2019).

[12] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.

[13] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[14] M. Crosby, P. Pattanayak, S. Verma *et al.*, "Blockchain technology: Beyond bitcoin," 2016.

[15] IBM, "Blockchain industry applications — ibm," https://www.ibm.com/blockchain/industries, (Accessed on 12/03/2019).

[16] U. W. Chohan, "The double spending problem and cryptocurrencies," *Available at SSRN 3090174*, 2017.

[17] M. Rosenfeld, "Analysis of hashrate-based double spending," 2014.

[18] Bitcoin.org, "nbits, target threshold - bitcoin glossary," https://bitcoin.org/en/glossary/nbits, (Accessed on 11/27/2019).

[19] IBM, "The difference between public and private blockchain - blockchain pulse: Ibm blockchain blog," https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/, (Accessed on 12/03/2019).

[20] T. J. Smedinghoff, "Introduction to online identity management," 2008.

[21] European Parliament, Council of the European Union, "Regulation (EU) no 2016/679," 2016, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG.

[22] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," *arXiv preprint arXiv:1908.00929*, 2019.

[23] E. Bertino and K. Takahashi, *Identity management: Concepts, technologies, and systems*. Artech House, 2010.

[24] B. Zwattendorfer, T. Zefferer, and K. Stranacher, "An overview of cloud identity management-models." in *WEBIST (1)*, 2014, pp. 82–92.

[25] R. Sánchez-Guerrero, F. Almenárez, D. Díaz-Sánchez, A. Marín, P. Arias, and F. Sanvido, "An event driven hybrid identity management approach to privacy enhanced e-health," *Sensors*, vol. 12, no. 5, pp. 6129–6154, 2012.

[26] A. Jøsang and S. Pope, "User centric identity management," in *AusCERT Asia Pacific Information Technology Security Conference*. Citeseer, 2005, p. 77.

[27] OASIS, "Security assertion markup language (saml) v2.0 technical overview," OASIS, Technical Overview, mar 2008.

[28] The OpenID Foundation, "Openid connect faq and q&as," https://openid.net/connect/faq/, (Accessed on 12/23/2019).

[29] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, "Openid connect core 1.0," The OpenID Foundation, techreport, Nov. 2014.

[30] D. Longley, C. Allen, M. Sabadello, M. Sporny, and D. Reed, "Decentralized identifiers (DIDs) v1.0," W3C, W3C Working Draft, Dec. 2019, https://www.w3.org/TR/2019/WD-did-core-20191209/.

[31] D. Longley, M. Sporny, G. Noble, D. Burnett, and B. Zundel, "Verifiable credentials data model 1.0," W3C, W3C Recommendation, Nov. 2019, https://www.w3.org/TR/2019/REC-vc-data-model-20191119/.

[32] M. Sabadello, "A universal resolver for self-sovereign identifiers," https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c, nov 2017, accessed on 12/26/2019.

[33] DIF, "Identity hubs," https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md, accessed on 01/16/2020.

[34] I. G. L. Consortium, "Open badges v2.0," https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/index.html, April 2018, (Accessed on 01/16/2020).

[35] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," The Sovrin Foundation, Whitepaper, mar 2017.

[36] C. Allen, "The path to self-sovereign identity," https://github.com/ChristopherA/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md, mar 2017, accessed on 12/28/2019.

[37] Calypso, "Account based ticketing with calypso," Calypso Networks Association, 185 Rue de Bercy, 75012 Paris, France, Whitepaper 170529-CalypsoWhitePaperABT, aug 2017, https://www.calypsonet-asso.org/sites/default/files/170529-CalypsoWhitePaperABT_%20v2.3.pdf.

[38] P. Vappereau, "Open payment and account-based ticketing: Is it back to the future or a genuine step forward?" https://www.linkedin.com/pulse/open-payment-account-based-ticketing-back-future-step-vappereau/, nov 2017, accessed on 01/08/2020.

[39] "Calypso," https://www.calypsonet-asso.org/, (Accessed on 11/02/2020).

[40] Calypso, "Objectives," https://www.calypsonet-asso.org/content/objectives, accessed on 01/16/2020.

[41] C. Mulley, "Mobility as a services (maas)–does it have critical mass?" 2017.

[42] P. Jittrapirom, V. Caiati, A.-M. Feneri, S. Ebrahimigharehbaghi, M. J. Alonso González, and J. Narayan, "Mobility as a service: A critical review of definitions, assessments of schemes, and key challenges," 2017.

[43] Kamargianni, M., Matyas, M., Li, W., Muscat, J., Yfantis, L., "The MaaS Dictionary," MaaSLab, Energy Institute, University College London, Tech. Rep., 2018.

[44] S. Ho, "Tsio protocol: The internet of mobility (whitepaper)," https://planar.network/assets/docs/whitepaper.pdf, 2017, accessed on 01/02/2020.

[45] EY, "Tesseract: Blockchain integrated mobility platform," https://www.ey.com/en_au/automotive-transportation/tesseract-blockchain-integrated-mobility-platform, (Accessed on 01/05/2020).

[46] IoMob, "About – iomob," https://www.iomob.net/about/, (Accessed on 01/05/2020).

[47] ——, "Introducing the iomob blockchain protocol — an open protocol for the future of mobility," https://medium.com/iomob/introducing-the-iomob-blockchain-protocol-an-open-protocol-for-the-future-of-mobility-e2d1898a 4 2018, (Accessed on 01/05/2020).

[48] T. Protocol, "Transit protocol," https://www.transitprotocol.com/, (Accessed on 01/05/2020).

[49] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, "uPort: A Platform for Self-Sovereign Identity,"

http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf, October 2016, accessed on 12/30/2019.

[50] ShoCard, "Shocard whitepaper," http://shocard.com/wp-content/uploads/2018/01/ShoCard-Whitepaper-Dec13-2.pdf, 2017, accessed on 12/30/2019.

[51] ShoCard and SITA, "Travel identity of the future - whitepaper," https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf, 2016, accessed on 01/2/2020.

[52] K. Cameron, "The laws of identity," *Microsoft Corp*, vol. 12, pp. 8–11, 2005.

[53] Planar Network, "The planar network - blockchain transport (whitepaper)," https://planar.network/assets/docs/whitepaper.pdf, 2017, accessed on 01/02/2020.

[54] M. Kamargianni and M. Matyas, "The business ecosystem of mobility-as-a-service," in *transportation research board*, vol. 96. Transportation Research Board, 2017.

[55] M. Matyas and M. Kamargianni, "The potential of mobility as a service bundles as a mobility management tool," *Transportation*, vol. 46, no. 5, pp. 1951–1968, 2019.

[56] I. M. Karlsson, J. Sochor, and H. Strömberg, "Developing the 'service' in mobility as a service: Experiences from a field trial of an innovative travel brokerage," *Transportation Research Procedia*, vol. 14, pp. 3265 – 3273, 2016, transport Research Arena TRA2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2352146516302794

[57] MaaS Aliance, "The alliance — maas alliance," https://maas-alliance.eu/the-alliance/, 2019, (Accessed on 11/07/2019).

[58] S. Hietanen, "CEO, ITS Finland. "Mobility as a service" - the new transport model?" Technical report, MaaS Finland, Tech. Rep., 2014.

[59] ——, ""mobility as a service" - the new transport model?" *Eurotransport*, vol. 12, no. 2, pp. 2 – 4, 2014.

[60] K. Salah and M. Khan, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, 11 2017.

[61] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[62] Bitcoin Wiki, "Sha-256 - bitcoin wiki," https://en.bitcoin.it/wiki/SHA-256, (Accessed on 12/02/2019).

[63] Z. Cheng, "Design and evaluation of a bitcoin miner systemc model with thread and data-level parallelism," Ph.D. dissertation, UC Irvine, 2017.

[64] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain." *Journal of Information processing systems*, vol. 14, no. 1, 2018.

[65] NxtCoin, "What is nxt? — nxtcoin," http://www.nxtcrypto.org/nxt-technology/what-nxt, (Accessed on 12/03/2019).

[66] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[67] P. Vasin, "Blackcoin's proof-of-stake protocol v2," *URL: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper. pdf*, vol. 71, 2014.

[68] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, no. 1999, 1999, pp. 173–186.

[69] D. Larimer, "Delegated proof-of-stake (dpos)," *Bitshare whitepaper*, 2014.

[70] Bitshares Docs, "Delegated proof of stake (dpos) — bitshares documentation documentation," https://docs.bitshares.org/en/master/technology/dpos.html, (Accessed on 12/03/2019).

[71] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 2016, p. 4.

[72] K. Lei, Q. Zhang, L. Xu, and Z. Qi, "Reputation-based byzantine fault-tolerance for consortium blockchain," 12 2018.

[73] Symbiont.io, "Technology — symbiont.io," https://symbiont.io/technology, (Accessed on 12/03/2019).

[74] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: an introduction," *R3 CEV, August*, vol. 1, p. 15, 2016.

[75] A. Bessani, J. Sousa, and E. E. Alchieri, "State machine replication for the masses with bft-smart," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, 2014, pp. 355–362.

[76] D. Schwartz, N. Youngs, A. Britto *et al.*, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, p. 8, 2014.

[77] iFour Technolab Pvt. Ldt., "The blockchain evolution, history and it's implementation in blockchain consulting," https://www.ifourtechnolab.com/blog/blockchain-history-and-evolution, (Accessed on 12/03/2019).

[78] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[79] Blockgeeks, "What are dapps? the new decentralized future - blockgeeks," https://blockgeeks.com/guides/dapps/, (Accessed on 12/03/2019).

[80] A. Slomovic, "Privacy issues in identity verification," *IEEE Security & Privacy*, vol. 12, no. 3, pp. 71–73, 2014.

[81] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile," 2002.

[82] D. Hardt, "The oauth 2.0 authorization framework," 2012.

[83] W. Li and C. Mitchell, *Addressing Threats to Real-World Identity Management Systems*, 01 2015, pp. 251–259.

[84] The OpenID Foundation, "Thank you too apple," https://openid.net/2019/10/22/thank-you-too-apple/, oct 2019, (Accessed on 12/23/2019).

[85] A. Hughes, M. Sporny, and D. Reed, "A primer for decentralized identifiers," W3C, Draft Community Group Report, Jan. 2019, https://w3c-ccg.github.io/did-primer/#did-methods-0.

[86] C. Allen and S. Appelcline, "A primer on self-sovereign identity," https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/topics-and-advance-readings/self-sovereign-identity-primer.md, sep 2017, accessed on 12/27/2019.

[87] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80 – 86, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574013718301217

[88] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[89] TravelSpirit, "TSio Protocol - TravelSpirit Foundation," https://travelspirit.foundation/tsio-protocol/, (Accessed on 01/05/2020).

[90] M. Tan, "Transit protocol and what we do - medium," https://medium.com/@SupaDynaMike/transit-protocol-and-what-we-do-363f5bdc8dd9, 2019, (Accessed on 01/05/2020).

[91] IDChainz, "Idchainz - chainzy," https://www.chainzy.com/products/idchainz/, (Accessed on 01/06/2020).

[92] Blockstack, "Github - blockstack-core: The reference implementation of blockstack," https://github.com/blockstack/blockstack-core, (Accessed on 01/06/2020).

[93] Deloitte, "Github - deloitte's smart id contracts," https://github.com/SmartIdentity/smartId-contracts, (Accessed on 01/06/2020).

[94] E. Larcheveque, "Bitcoin address authentication protocol (bitid)," https://github.com/bitid/bitid/blob/master/BIP_draft.md, 2016, (Accessed on 01/06/2020).

[95] Civic, "Civic - token behavior model (whitepaper)," https://www.civic.com/wp-content/uploads/2018/05/Token-Behavior-Model-May-16-2018.pdf, 2018, accessed on 01/06/2019.

[96] "Intelligent transport system - Public Transport - Account-based ticketing state of the art report (Working document: ISO/TC 204/WG 8 N 000)," International Organization for Standardization, Geneva, CH, Techinical Report, Oct. 2016.

[97] C. C. Group, "A primer for decentralized identifiers," W3C, Draft Community Group Report, jan 2019, accessed on 01/09/2020.

[98] "Node.js - wikipedia," https://en.wikipedia.org/wiki/Node.js, (Accessed on 09/30/2020).

[99] "Express.js - wikipedia," https://en.wikipedia.org/wiki/Express.js, (Accessed on 09/30/2020).

[100] "A docker tutorial for beginners," https://docker-curriculum.com/, (Accessed on 09/30/2020).

[101] "Introduction — handlebars," https://handlebarsjs.com/guide/#what-is-handlebars, (Accessed on 10/02/2020).

[102] "Json," https://www.json.org/json-en.html, (Accessed on 10/03/2020).

[103] "Getting started with ibm blockchain platform," https://cloud.ibm.com/docs/blockchain/index.html, (Accessed on 10/03/2020).

[104] "Go tutorial - tutorialspoint," https://www.tutorialspoint.com/go/index.htm, (Accessed on 10/04/2020).

[105] "1. introduction — apache couchdb® 3.1 documentation," https://docs.couchdb.com/en/latest/intro/index.html, (Accessed on 10/07/2020).

[106] "Yaml - wikipedia," https://en.wikipedia.org/wiki/YAML, (Accessed on 10/07/2020).

[107] "Prometheus - monitoring system & time series database," https://prometheus.io/, (Accessed on 11/02/2020).

[108] D. Lang, M. Friesen, M. Ehrlich, L. Wisniewski, and J. Jasperneite, "Pursuing the vision of industrie 4.0: Secure plug-and-produce by means of the asset administration shell and blockchain technology," in *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, July 2018, pp. 1092–1097.

[109] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, p. 95–102, Jun. 2018. [Online]. Available: https://doi.org/10.1145/3212998

[110] A. Baliga, "Understanding blockchain consensus models," 2017.

[111] T. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 1–1, 12 2019.

[112] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Oct 2017, pp. 2567–2572.

[113] T.-T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples," *Journal of the American Medical Informatics Association*, vol. 26, no. 5, pp. 462–478, 03 2019. [Online]. Available: https://doi.org/10.1093/jamia/ocy185

[114] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[115] D. Vujičić, D. Jagodić, and S. Ranđić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2018, pp. 1–6.

[116] A. Baliga, "The blockchain landscape," *Persistent Systems*, vol. 3, no. 5, 2016.

[117] T. L. Foundation. (2020, mar) Hyperledger. [Online]. Available: https://www.hyperledger.org/

[118] ——, "Hyperledger architecture, volume 1," https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, aug 2017, accessed on 05/04/2020.

[119] ——. (2020) Hyperledger fabric documentation v2.0. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.0/whatis.html

[120] "Gluu documentation," https://gluu.org/docs/, (Accessed on 11/03/2020).

[121] E. S. Stefan Thomas, "Codius -white paper," Ripple Labs, White Paper, jul 2018, https://github.com/codius/codius-wiki/wiki/White-Paper.

[122] G. Greenspan, "Multichain private blockchain — white paper," MultiChain, White Paper, 2015, https://www.multichain.com/download/MultiChain-White-Paper.pdf.

[123] Blockstack. (2020) Overview of blockstack. [Online]. Available: https://docs.blockstack.org/org/overview.html

[124] A. B. Muneeb Ali, Jude Nelson *et al.*, "Blockstack technical whitepaper v2.0," Blockstack PBC, Whitepaper, may 2019.

[125] J. Nielsen, *Usability Engineering*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1993.