ISSN 1831-9424

European Commission

JRC SCIENCE FOR POLICY REPORT

Final Report of the Exploratory Research Project, Blockchain for Transport (BC4T)

The Application of Secure and Privacy-Centric Road Vehicle Identity and Emissions Monitoring Systems

O'Brien, D.; Christaras V.; Kounelis I.; Nai-Fovino I.; Fontaras G.

2022

Joint Research Centre

EUR 31161 EN

Contact Information
Name: Georgios Fontaras
Address: Joint Research Centre, Via Enrico Fermi 2749, TP-230 21027 Ispra (VA), Italy
Email: Fontaras.Georgios@ec.europa.eu
Tel.: +39 0332 786425

EU Science Hub
https://ec.europa.eu/jrc

JRC130260

EUR 31161 EN

PDF	ISBN 978-92-76-55143-0	ISSN 1831-9424	doi:10.2760/309745	KJ-NA-31161-EN-N
Print	ISBN 978-92-76-55773-9	ISSN 1018-5593	doi:10.2760/491939	KJ-NA-31161-EN-C

Luxembourg: Publications Office of the European Union, 2022

How to cite this report: O'Brien, D., Christaras, V., Kounelis, I., Nai Fovino, I., Fontaras, G., *Final Report of the Exploratory Research Project, Blockchain for Transport (BC4T)*, Publications Office of the European Union, Luxembourg, 2022, doi:10.2760/309745, JRC130260.

Contents

Abstract

The objective of the BC4T project is to investigate possible applications of blockchain (BC) technology on road transport, focusing on topics of interest to the European Commission's policy agenda. BC is a technology that enables data exchange and storage in a transparent and traceable way giving additional security while maintaining data provenance and identity ownership. Pilot studies have shown that it is possible to connect entities such as vehicles, people, and authorities via BC technology while preserving data privacy in line with the General Data Protection Regulation (GDPR), electronic IDentification, Authentication, and trust Services Regulation (eIDAS) and the ePrivacy Directive. The study also showed that sharing vehicle information such as fuel consumption or emissions to a fully BC-based monitoring system would be technically feasible. Simulations also indicated that it is possible to connect a vehicle fleet of 280 million vehicles, the EC and 27 Member States via two heterogeneous BCs communicating in tandem at a pilot level. Data such as those recorded by On-board Fuel Consumption Monitoring Devices (OBFCM) can be stored and reported via the tamper-resistant BC and could reduce administrative/cost burdens whilst facilitating compulsory monitoring of CO_2 and energy consumption. Adopting a European Digital Identity could open up a range of diverse applications within the connected mobility ecosystem linking users and regulators while protecting personal data and privacy. The benefits of the adoption and testing of BC could create a significant and transparent interlinking of public and private data and enable interoperability across different transport systems.

Acknowledgements

The authors would like to acknowledge the support of

— The JRC exploratory research programme for funding the study.

— Mr Massimiliano Gusmini for his continuous support in the graphics design and editing of the report.

— Mr Panagiotis Christias, Epic's Admin, for helping with setting up Epic experiments, help with linux administration.

— And to thank the following reviewers for helping to ensure the quality of this Science for Policy Report:

- Harmen Vander Kooj from the Dutch BC Coalition,
- Iordanis Papoutsoglou from the Centre for Research and Technology Hellas,
- Saki Gerassis Davite from DG MOVE,
- Raphael Lemaihieu from DG FISMA,

Authors
O' Brien Dermot
Christaras Vasileios
Kounelis Ioannis
Nai Fovino Igor
Fontaras Georgios

With contributions from:

— Section 4.1

- Andreas Freund
- Tram Vo
- Umed Khudoiberdiev
- Matt Shi
- Grace Pulliam
- Rajat Rajbhandari
- Parth Bhatt
- Chris Ballinger

— Section 4.3:

- Christos Patsonakis
- Charalampos Savvaidis
- Kostantinos Votis

— Section 5.1:

- Tsoniotis Nikolaos

Executive summary

The Blockchain for Transport BC4T project investigated possible applications of BC([1]) technology in the road transport sector, focusing on topics relevant to the European Commission's policy agenda. BC technology allows for permanent and immutable information storage and the digitisation of trust. The EU has embraced the BC, considering it a technology where Europe can be a global leader in the future. Many stakeholders recognise the potential of BC to change the paradigm for transport. BC4T aimed to enhance the JRC's know-how on applied BC technology relevant to road vehicles, attempting a first review on the topic, developing, and demonstrating prototypes linked to vehicle self-sovereign identity (SSI) and emissions monitoring and analysing possible links to future policy in the domain.

The project objectives were:

1. To gather know-how on BC technology for the automotive and road transport sectors.
2. To provide a policy-relevant overview of the status in the development and deployment of BC implementations regarding road vehicles.
3. To conceptualise prototypes linked to ongoing JRC policy support activities (i.e. digital identity, vehicle fuel consumption and emissions monitoring) serving as the basis for future research on these topics.
4. To develop computer simulation and analysis tools necessary to test BC systems' applicability and likely performance for the above-mentioned and possibly other future implementations.

Given the broadness of the road vehicle sector and the significant number of BC applications appearing, the BC4T project focused on two primary case studies:

1. the application of BC technology for vehicle identity attribution and
2. real-world vehicle CO_2 emissions and energy consumption monitoring

These two indicative first implementations helped guide the realisation of actual pilot implementations and allowed a first stress test of the available BC technology. In general, a broader BC-based ecosystem established around the vehicle and its use could spur a vast number of novel applications spanning from topics related to policy and governance, such as emissions monitoring, pollutants-based taxation and tolling, verification of roadworthiness, to user-oriented solutions that utilise SSI frameworks, and third-party utilities such as vehicle charging infrastructure, vehicle sharing, vehicle rental, vehicle insurance and others.

BC4T investigated in depth the following four activities to support the project objectives:

1. Pilot 1: Simulation of an EU-based vehicle identity management system based on Self-Sovereign Identity (SSI) and MS Vehicle Registration Authorities interacting with the European Commission (EC). The implementation was performed in collaboration with a non-profit consortium focusing on BC for mobility, Mobility Open BC Initiative (MOBI).
2. Pilot 2: Simulation of a data exchange BC-based monitoring mechanism (vehicle fuel consumption/CO_2 emissions monitoring used as an example) guaranteeing the provenance of emissions data and its integrity for monitoring and other possible purposes; the simulation assumed vehicles interacting with the EC and Member State (MS) Vehicle Registration Authorities. The BC4T study team performed the implementation.
3. Pilot 3: Integration of the previous two BC systems to achieve interoperability, a different possible SSI framework was investigated. This activity was performed in collaboration with Informatics and Telematics Institute (ITI) an emerging technology research group within the Centre for Research and Technology Hellas (CERTH).
4. A desktop review of the current state of road tolling, taxation, and emissions trading rules and obligations that could potentially serve as first implementations to be rolled out on BC technology for road vehicles. The study attempted to outline how BC technology can help reshape them and establish possible future applications of relevance to the EU and end-users.

([1]) A BC is a ledger for storing digital information operating on a network where each node maintains an identical copy of the stored data. New information is grouped into "blocks" that are timestamped and linked to previous ones via cryptography. New blocks are appended periodically to the structure creating a historical "chain" of information that is virtually impossible to tamper.

The first pilot was chosen to demonstrate that BC can enable an eco-system of self-sovereign applications at the vehicle level. In addition, the use of SSI frameworks will be important as many future transport applications will require a digital twin of the: vehicle, user, transportation-related entities, governmental bodies or even could include digitisation of the components of the vehicles. For an entity to interact with the digital world, it will require a digital representation, i.e. a digital twin or digital identity. As stated in the proposal to amend the eIDAS regulation (EC, 2021), the essential features of the technology used must have privacy, security, and users in control of their own data and identity at heart.

From a demonstrative point of view, the second pilot was an excellent choice to show a simple identity management system, using the same certificates as most of the web services one would typically access and use. These X.509 certificates (with more details in the next section) can be used in conjunction with a private BC network and store data off-chain to increase privacy and security. The emissions monitoring scenario was chosen as a starting use-case even though the vehicle would only need to communicate at a maximum rate of once a month. Therefore, the Transactions Per Second (TPS) required to implement such a use-case successfully is relatively low compared to a use-case like traffic monitoring, which would necessitate sub-second communication intervals, requiring magnitudes of order higher TPS. The fuel consumption use-case was also relevant from a regulatory perspective. It directly links to a policy priority and would allow a series of applications related to the abatement of greenhouse gas emissions from road vehicles. The use-case builds on the communication of onboard fuel consumption monitoring (OBFCM) data reporting requirements described later in subsection 3.2.1.

Pilot 3 intends to demonstrate how adding complexity may affect the BC systems and showcase the plausibility of their interaction. In research and software development projects starting with simple scenarios and then adding complexity is the best practice. Connecting the BC system (second use-case) developed at the JRC on Hyperledger Fabric to another heterogeneous BC system built on Hyperledger Indy that deals with the SSI management (first use-case) is challenging. Hyperledger has no native way to connect these BC systems. As such, a gateway was needed to translate the messages communicated between the two systems to understand each other. As the task of developing such a gateway could take more time than the duration of the BC4T project to develop, it was decided to seek outside collaboration with researchers who had already developed such a gateway. The development and deployment of this system was undertaken as the third pilot use-case in cooperation with the CERTH.

Finally, identifying likely policy-related candidate cases for a possible first roll-out of such a system, the topics of taxation, tolling and emissions trading in transport were reviewed with a high-level description of the application of BC technology, followed by an outline of a possible implementation path. The EC is working on policies and directives related to adopting interoperable electronic road toll systems and enabling cross-border information exchange. In addition, considerations of extending the European Emission Trading System (ETS) to include transport emissions by 2030 could influence national taxing schemes.

Policy context

The European Union (EU) is committed to reducing Green House Gas (GHG) emissions and has a longstanding policy for achieving significant reductions in the contributions to transport greenhouse gas emissions. This push to reduce GHGs from the Transport sector, comes from data showing that domestic transport within the EU accounts for a 23% share of the total net emissions within the EU as of 2018. Most of these emissions originate from the road transport sector, particularly light-duty vehicles. As stipulated by 2019/631/EU (EC, 2019h), the European Commission (EC) explores methods for monitoring the real-world CO_2 emissions derived from real-world fuel and energy consumption of road vehicles in the EU. For this purpose, EU regulation has already introduced OBFCM systems in all new vehicles entering circulation as of 2021. Regulation (EU) 2018/1832 (EC, 2018) of November 2018 decreed, starting from January 2021, OBFCM devices as compulsory devices in all newly produced commercial and light passenger vehicles. The collecting and analysing OBFCM data will enable regulators to monitor and confirm that the objective of decreasing emissions derived from road transport is reflected in the real-world activity of road vehicles. However, since it is already accessible on the vehicle, these data could be used to support other applications, public or private, subject to the vehicle owner's willingness to share them.

Regulation (EU) 910/2014 (eIDAS) (EC, 2014b) is the only EU framework for trusted cross-border electronic identification (eID) of a natural person. Following its enactment in 2014, it was based on the nation eID systems that are conditional to diverse standards and only facilitate the electronic identification needs of a small segment of EU citizens and businesses. The COVID-19 pandemic has had a dramatic effect on the rate of digitalisation leading to both the public and private sectors transitioning to digital services. Now it is becoming an expectation of EU citizens and businesses that activities such as enrolling at a foreign university, tax declarations, banking,

car rental, loans and insurances, authentication over the internet for payments or services, and more should be digital and with a high level of assurance of security, privacy and with convenience for the user.

The increased rate of digitisation from the COVID-19 pandemic created a demand for means to authenticate and identify online, including the need to exchange information relating to one's identity digitally, such as certificates, attributes and qualifications one holds (which could include ID number, residence address, age, qualifications, driving license and other permits or payment information). The need to authenticate and identify online has sparked a new paradigm, with the adoption of "advanced and convenient solutions that can integrate different verifiable data and certificates of the user" (EC, 2021). "Users expect a self-determined environment where various credentials and attributes can be carried and shared, such as your national eID, professional certificates, and public transport passes. These are so-called self-sovereign app-based wallets managed through the user's mobile device, allowing for secure and easy access to different public and private services under their full control" (EC, 2021).

The Proposal for a European Digital Identity Framework echoes the need for a more harmonised approach to digital identification to that of divergent national methods and the vitality this will give to the EU digital Market by enabling citizens, businesses and public services to identify online conveniently and uniformly while facilitating data subjects control over what personal data is shared and when. All EU citizens should benefit from secure access to public and private services provisioned by an ecosystem at the EU level that enables trust between participants relying on verified proofs of identity and attestations of attributes and verifiable claims. The reliability of digital identity solutions will support competition within the EU by benefiting "from a harmonised European approach to trust, security and interoperability" (EC, 2021).

It is, therefore, necessary to in addition lay out the conditions to be included in a harmonised framework for European Digital Identity Wallets:

- Enable users to access a large scope of cross-border private and public services through electronic identification and authentication, both online and offline.
- Benefit from the potential delivered by tamperproof solutions to provide a high level of assurance.
- When adopted or issued by the Member States, use a common standard to allow seamless interoperability and a high level of security.
- Permit the issuance and handling of trustworthy digital attributes and support the decline in administrative strain, enabling citizens to use the verifiable credentials and claims in their private and public interactions. For example, EU citizens should be capable of proofing digital ownership of a valid driving licence issued by a Member State Vehicle Registration Authority, "which can be verified and relied upon by the authorities in the other Member States" (EC, 2021).
- "Qualified electronic ledgers record data in a manner that ensures the uniqueness, authenticity, and correct sequencing of data entries in a tamper-proof manner. For example, it creates a reliable audit trail for the provenance of commodities in cross border trade and provides for the basis of advanced solutions for self-sovereign identity and supports more efficient and transformative public services" (EC, 2021).

Main findings

The project contributes to the know-how on potential applications of BC technology for the road transport sector. The pilots investigated by the project team demonstrate that it is possible to connect entities such as vehicles, people, and authorities via BC technology while preserving data privacy in line with the General Data Protection Regulation (GDPR) (EC, 2008), eIDAS (EC, 2014b), the ePrivacy Directive (EC, 2002). The project also showed that sharing vehicle operation data such as fuel consumption or CO_2 emissions to a fully BC-based monitoring system would be technically feasible.

By the very nature of SSI frameworks, users are fully controlling the generation of their own decentralised identity. Helping to demonstrate that the recommendations laid out by the proposal for a Regulation amending eIDAS (EC, 2021) and extending it to include a European Digital Identity and Wallet, is feasible. It also offers the benefits of putting a user in control of one's identity and data with increased levels of privacy when using SSI frameworks. In addition, this report further demonstrated the capabilities of using a tamper-resistant ledger for data integrity and provenance, leading to increased security and removing single points of failure.

The three pilot studies also demonstrated that the approach chosen was technically feasible. Connecting

the BC system developed at the JRC on Hyperledger Fabric to simulate vehicle monitoring to another heterogeneous BC system built using Hyperledger Indy, that deals with the SSI management aspect was a significant success as Hyperledger has no native way to connect these BC systems.

The analysis from this report further supports the necessity of adopting the European Digital Identity and Wallet amendment of eIDAS. To smoothly and efficiently interact in a digital world, a digital identity is required whether you are a person, a device or an institution (EC, 2021).

Validating the use of BC for transport applications would be one step toward achieving full interoperability across heterogenous systems across EU27.

Key conclusions

Pilot 1, SSI Vehicle Management System for Emissions Monitoring:

The first pilot investigated the use of an identity management system built employing a Self-Sovereign Identity Framework, which is either using standards already largely accepted and adopted by industry or, in the case where there is no clear standard, implementing their own standard. Pilot 1 was done in collaboration with MOBI; it demonstrated the performance of an Amazon Web Services (AWS) cloud computing cluster used and alluded to the hardware requirements and cost for 280 million vehicles. This pilot was purely exploring the performance of the identity management system and did not include the data integrity and provenance system developed in the following use-case.

It was demonstrated that for 1 million vehicles, the resulting performance for the slowest process flow had a number of process flows that can be executed per second that was a magnitude of order faster than needed for the emissions monitoring scenario, with reporting taking place on an annual basis. It is expected that for the scaling from 1 million to 280 million vehicles, that the results will not deviate significantly from the current ones, although this is not guaranteed.

Pilot 2, Emission Data Integrity and Provenance:

The second pilot, deployed purely by the JRC, implemented a system that can ensure the integrity and provenance of emissions data from vehicles and implements a simple identity management system based on certificates commonly used in web services (X.509 certificates), while increasing the levels of privacy through storing certain data off-chain and through use of private channels. This research was purely a JRC activity and performed on High-Performance Clusters (HPCs) at the JRC.

Pilot 2 aimed to evaluate if sharing vehicle data such as CO_2 emissions or fuel consumption from vehicles to a BC-based system would be technically feasible with current technological solutions. The performed research was formulated in this direction, using the current real-world values in the EU as parameters. As a result, a vehicle fleet of 280 million vehicles was considered, interacting with 27 Member States, having the legal obligation to transmit once per year their CO_2 emissions to the EC. A maximum throughput of 257 transactions per second was achieved with these parameters, with the system being steady and responsive. This result shows that it is feasible with the current technology to meet the obligation of one transaction per vehicle per year and even more to have better outcomes when increasing the hardware resources.

Finally, the experiment setups provided valuable knowledge and practical know-how on deploying and using a BC infrastructure, Hyperledger Fabric. This domain was still undiscovered when the project started, and the study team had to create its own custom solution. This process had not only helped the project team to better understand the internal BC mechanisms, but it also led us to automate the deployment procedure completely, thus facilitating the execution of many experiments with different parameters.

Pilot 3, SSI Vehicle Management System with Data Integrity and Provenance of Emission Reporting Data.

The third pilot then added complexity by combining the first BC network architecture built on Hyperledger Fabric developed in the first pilot with that of another BC network, Hyperledger Indy. This was combined with a library for peer-to-peer interactions, Hyperledger Aries. HLI and HLA are used for running the SSI operations within the vehicle identity management system. Allowing for all the benefits of using a SSI framework along with the data integrity and provenance features provided by the first pilot.

The implementation and deployment of such as system is by far the most technically challenging part of

such a study, where just the gateway dealing with the communication between the heterogenous BCs can take considerable time and effort to develop, as it does not exist natively. Hence, this research was done in collaboration with CERTH, a research institution that had already published work detailing the SSI implementation they had performed using Hyperledger Aries and Indy; specifically of interest was a gateway they developed to allow communication between Hyperledger Fabric (used for data provenance and integrity) with Hyperledger Aries and Indy (used for SSI).

Now the system for pilot 3 has been deployed on the JRC infrastructure, the next step is to run the performance simulations to give an idea of how feasible this system is in normal operating situations, what infrastructure resources would be required to run such as system and what the associate cost would be. These results will be published in a peer reviewed journal in collaboration with ITI.

Exploration of applicability of BC technology to tolling, taxation and the ETS:

The three pilot studies undertaken were just a start in terms of investigating different combinations of complex systems using BC4T and how they would fit into a regulatory and societal framework. Technological advances together with the need to comply with legislation can lead to future innovation and stimulate new ideas about future research scenarios however, there must be cohesion across the EU and adopted transportation systems, together with tolling and taxation, in the different countries. In fact, the pilot studies could spur a broad number of applications both of policy relevance, such as pollutant-based taxation and tolling, and user-oriented utilities based on self-sovereign identity solutions.

Other areas investigated in this report include use of BC for Tolling and Taxation, namely use of taxation and tolling systems in relation to road usage, vehicle types and congestion with a view to spurring on possible future research scenarios. Details in this chapter include, Vehicles as Identities and BC for Tolling followed by an indication of what the next steps could be in BC for Tolling and some conclusions are drawn (see following section).

Tolling and taxation of vehicles is undergoing a major shift in technologies and processes. The new EETS framework drives cross-border interoperability and leads the way to regulatory and technological harmonisation among EU Member states. In parallel the Green Deal imperatives are extending the European Emissions Trading System to incorporate more market players and address more sectors, among which the road transport. Secondary efforts include the shift from time-based to distance-based tolling, which affects heavy and lightweight vehicles and paves the way to more equitable tolling and taxation policies.

Although the technological substrates are there, they are disjointed and do not foster an all-encompassing regulated environment at both EU and national levels. New paradigms are needed to showcase interoperability at large, reduce infrastructural needs and support standardisation. EETS, EU ETS and European BC Services Infrastructure (EBSI) can work in tandem to regulate standard interfacing between disparate actors and value chain stakeholders. Distributed Ledger technologies could provide this standard interface under a privacy-preserving prism. This report is part of the work conducted to identify the potential of and pilot BC-based implementations as an additional enabler to the ecosystem of solutions proposed for the transport sector.

1 Introduction

The present Science for Policy Report summarises the findings of the BC4T project launched under the European Commission (EC) Joint Research Centre's (JRC) exploratory research program.

BC([2]) technology is a breakthrough of the past decade with great potential for development and implementation across different industries and research fields. BC allows large groups of people and entities to reach an agreement, permanently store immutable information and thus digitise trust. By creating trust online, BC provides the infrastructure for a more fair, inclusive, secure and democratic digital economy; this characteristic of BC technology has significant implications on how people think about many of our economic, social and political institutions (Dal Mas et al., 2020b), including Transportation (Observatory, 2018).

The next phase of change of the Internet will be the development and adoption of a common identity layer, enabling people, devices, and organisations to create and use their own self-sovereign identity, which they own and control (Sovrin, 2017, Alupotha, 2018). A study by McKinsey (Institute, 2019), cited by the World Economic Forum (WEF, 2021b), predicted that countries adopting digital IDs could boost their economies between 3-13% of their Gross Domestic Product (GDP) by 2030.

Many stakeholders recognise the potential of BC to shift the paradigms in transport-related industries. With regards to road transport, some examples of emerging trends are:

- **The Sharing Economy:** Within the transport sector, this includes e-scooters, bike or car-sharing, providers for personal transportation, parking spaces, and more. Players within the auto industry have been exploring and looking to grow within the sharing economy movement (Forbes, 2019, WEF, 2017). These include Toyota investing in Getaround (Reuters, 2016), General Motors' car-sharing program Maven (Rincon, 2018), Daimler's car-sharing app called CROOVE (Times, 2018) and Fords bike-sharing program in San Francisco (Sutton, 2017). By adopting BC technology, the sharing economy is also advanced by allowing decentralised communities to own and share transportation assets while rewarding good actors within the community and disincentivising bad actors.
- **The Internet of Things (IoT):** *"The new rule for the future is going to be, "Anything that can be connected, will be connected"* (Buck, 2017). IoT will transform the transport industry from helping traffic management (Forbes, 2020, WEF, 2021a, Dziuba, 2020) with access to accurate, trusted, real-time data. Improve safety with inter-vehicle communication and safety responses to emergencies (Enterprise, 2020). Generally improving the volume, quality and granularity of transport data and the use-cases and applications that this entails. Authenticating and verifying which devices have access can share data, to who and when will require the security that comes with BC technology and the need for SSI solutions so that the IoT devices can control their identity and associated data.
- **Artificial Intelligence (AI):** AI will give rise to a vast improvement in transportation capabilities, not to mention being the crucial technology for autonomous vehicles, traffic management, and performing analytics related to the functions of transportation (Forbes, 2020, WEF, 2021a, Dziuba, 2020). In addition, BC helps to enable data marketplaces, where data can be bought, sold, with access rights only given to those who have been given consent by the data owner. Even more exciting is the possibility to combine BC and AI using Federated Learning, where ML models gain experience from different data sets located in a variety of sites without sharing the training data (**?**, Unal et al., 2021, Ma et al., 2020).
- **5G networks:** Will significantly increase connectivity and speed, reduce latency of devices within vehicles and transport infrastructure, allowing for improved and novel applications of other technologies (IoT, Autonomous Vehicles, etc.) and services. Services such as real-time monitoring and management of traffic become possible with the increased network capabilities provisioned by 5G, among a vast number of new possible products that can be developed and delivered (Ericsson, 2020).
- **Big Data:** Access to Big Data will lead to cost reductions, smart decision making, new services and products, and improved services that are more efficient and take less time. An example of transport applications that can be achieved with Big Data are as follows: Real-time Route Optimisation, Strategic Network Planning, Product Innovation,Service Improvement, Resilience Planning, Risk Evaluation, Supply Chain Analytics, Environmental Monitoring and Forecasting, Traffic Monitoring and Control (Forum, 2015, GlobalTranz, 2016).

([2]) A BC is a structure for storing digital information operating on a network where each node maintains an identical copy of the stored data (ledger). New information is grouped into "blocks" that are timestamped and linked to previous ones via cryptography. New blocks are appended periodically to the structure creating a historical "chain" of information that is virtually impossible to tamper.

- **Connected and Autonomous Vehicles:** Depend on various technologies such as AI, 5G, Big Data, and one of the most common IoT devices on the Road. The adoption of autonomous vehicles will provide newfound road safety and free citizens to perform other tasks while travelling in comfort and increased travel time (IBM, 2021, Forbes, 2021a, Deloitte, 2021).
- **Mobility-as-a-Service (MaaS):** Facilitate the movement of people with packages consisting of either monthly or pay-as-you-go plans for the use of any mode of transport anytime (Forbes, 2021c).
- **Digital Identity:** Has been cited as one of the key drivers for the success of the EU digital Economy (TransUnion, 2018), with having attributes relating to a traveller or vehicles identity can unlock the potential of seamless and secure travel (et Accenture, 2018), Digital Identity and SSI is becoming highly attractive technology to invest in, with countries like India aiming towards a digital-first future, with smart cities and digital identity being a key enabler (Services, 2018). To access and life in the digital world, one needs digital identities in the form of digital twins.
- **Electric Vehicles:** BC-based applications can help EV manufacturers to keep tabs on the materials as they are being brought into factories for EV production. In addition, from a charging infrastructure perspective, BC applications could allow vehicle owners to trade energy power by sharing their EV battery with the grid via the charging infrastructure (i.e., vehicle-to-grid or V2G). Thus, through specialized digital P2P charging platforms, owners can make their batteries available to the grid during the times when they are not using them (Forbes, 2021b, Okwuibe et al., 2020, Mckinsey, 2018, Jones, 2018).
- **Smart Cities (Intelligent Communities):** In general, most of the technologies above when combined in a harmonized way with all transportation networks and services with public services, along with an open economy; will form the backbone of the smart cities of the future, each component vital for the overall ecosystem (for Business Inovation & Skills, 2013, Commission, 2018).

The US Department of Transport Volpe Centre, in its 2018 report (US Department of Transportation, 2018), identifies different use-cases of BC in transportation: freight logistics and proof of delivery, toll payments, car/ride sharing, autonomous vehicle security, and aviation. Major automotive manufacturers such as Renault, Ford, GM and BMW established the Mobility Open BC Initiative (MOBI) to research and develop future BC-based solutions and services (IBM, 2018, Eyerys, 2018).

The potential of BC to revolutionise the transport sector has been a topic discussed extensively within the industry and has seen a large volume of investments by businesses aiming to position themselves for the future.

Massamba Thioye, the lead of the project exploring the use of Distributed Ledger Technology (DLT) and BC under the United Nations (UNs) Climate Change work functions, said *"The UN Climate Change secretariat recognises the potential of BC technology to contribute to enhanced climate action and sustainability"* (Nations, 2018, Dal Mas et al., 2020a). It was then further detailed that BC and DLT would:

- "Strengthen monitoring, reporting and verification of the impacts of climate action."
- "Improve transparency, traceability and cost-effectiveness of climate action."
- "Build trust among climate actors."
- "Make incentive mechanisms for climate action accessible to the poorest."
- "Support mobilisation of green finance." (Nations, 2018, Dal Mas et al., 2020a, Nations, 2017)

The EU has embraced BC technology through different activities and initiatives. The Commission established the EU BC Observatory and Forum (EuBOF), which aims to accelerate BC innovation and the development of the BC ecosystem within the EU to help cement Europe's position as a global leader in BC (Observatory, 2017). Other EU initiatives include the European BC Service Infrastructure who are setting standards and incorporating EU regulation compliance into BC frameworks (EBSI, 2017), which will be described in detail in Section 2.6.1. The CHAISE project is providing the required training and education to employees across sectors (CHAISE, 2022). The International Association for Trusted BC Applications (INATBA) is dedicated to providing users, public and private developers a forum to interact with regulators and policy makes on the global stage and help to bring BC technology to the next level (INATBA, 2022). Finally the Gaia-X Association is a multi-national non-profit organisation whose aim it is to develop technical frameworks and standards in order to create "an open, transparent, and secure digital ecosystem", "based on the values of openness, transparency, sovereignty, and interoperability, to enable trust" (Gaia-X, 2022). Of particular interest is the Gaia-X 4 ROMS project which is to support the remote operation of autonomous and linked Mobility Services, looking into many transport use-cases, such as, decentralised vehicle management, remote operation, predictive distribution and integration of autonomous car

fleets into city areas; to name a few.

BC4T investigated in depth the following four activities to support the project objectives:

1. **Pilot 1:** Simulation of an EU-based vehicle identity management system based on SSI and MS Vehicle Registration Authorities interacting with the European Commission (EC). The implementation was performed in collaboration with a non-profit consortium focusing on BC for mobility, MOBI.

2. **Pilot 2:** Simulation of a data exchange BC-based monitoring mechanism (vehicle fuel consumption/CO_2 emissions monitoring used as an example) guaranteeing the provenance of emissions data and its integrity for monitoring and other possible purposes; the simulation assumed vehicles interacting with the EC and MS Vehicle Registration Authorities. The BC4T study team performed the implementation.

3. **Pilot 3:** Integration of the previous two BC systems to achieve interoperability, a different possible SSI framework was investigated. This activity was performed in collaboration with Informatics and Telematics Institute (ITI) an emerging technology research group within the Centre for Research and Technology Hellas (CERTH).

4. **A desktop review of the current state of road tolling, taxation, and emissions trading** rules and obligations **that could serve as first implementations to be rolled out on BC technology for road vehicles**. The study attempted to outline how BC technology can help reshape them and establish possible future applications of relevance to the EU and end-users.

The first pilot was chosen to demonstrate that BC can enable an eco-system of self-sovereign applications at the vehicle level. In addition, the use of SSI frameworks will be important as many future transport applications will require a digital twin of the: vehicle, user, transportation-related entities, governmental bodies or even could include digitisation of the components of the vehicles. For an entity to interact with the digital world, it will require a digital representation, i.e. a digital twin or digital identity. As stated in the proposal to amend the eIDAS regulation (EC, 2021), the essential features of the technology used must have privacy, security, and users in control of their own data and identity at heart.

From a demonstrative point of view, the second pilot was an excellent choice to show a simple identity management system, using the same certificates as most of the web services one would typically access and use. These X.509 certificates (with more details in the next section) can be used in conjunction with a private BC network and store data off-chain to increase privacy and security. The emissions monitoring scenario was chosen as a starting use-case even though the vehicle would only need to communicate at a maximum rate of once a month. Therefore, the Transactions Per Second (TPS) required to implement such a use-case successfully is relatively low compared to a use-case like traffic monitoring, which would necessitate sub-second communication intervals, requiring magnitudes of order higher TPS. The fuel consumption use-case was also relevant from a regulatory perspective. It directly links to a policy priority and would allow a series of applications related to the abatement of greenhouse gas emissions from road vehicles. The use-case builds on the communication of onboard fuel consumption monitoring (OBFCM) data reporting requirements described later in subsection 3.2.1.

Pilot 3 intends to demonstrate how adding complexity may affect the BC systems and showcase the plausibility of their interaction. In research and software development projects starting with simple scenarios and then adding complexity is the best practice. Connecting the BC system (second use-case) developed at the JRC on Hyperledger Fabric to another heterogeneous BC system built on Hyperledger Indy that deals with the SSI management (first use-case) is challenging. Hyperledger has no native way to connect these BC systems. As such, a gateway was needed to translate the messages communicated between the two systems to understand each other. As the task of developing such a gateway could take more time than the duration of the BC4T project to develop, it was decided to seek outside collaboration with researchers who had already developed such a gateway. The development and deployment of this system was undertaken as the third pilot use-case in cooperation with the CERTH.

Finally, identifying likely policy-related candidate cases for a possible first roll-out of such a system, the topics of taxation, tolling and emissions trading in transport were reviewed with a high-level description of the application of BC technology, followed by an outline of a possible implementation path. The EC is working on policies and directives related to adopting interoperable electronic road toll systems and enabling cross-border information exchange. In addition, considerations of extending the European Emission Trading System (ETS) to include transport emissions by 2030 could influence national taxing schemes.

1.1 Structure of the report

— **Chapter 2:** The first chapter focuses on the benefits of BC technology for Transport applications, introducing the basic concepts of what a BC is, how it functions on a high level, what types of BC networks there are, and what key technological features and components needed for the use-cases explored in this research. The chapter also lists the main BCs of interest in a technology landscape overview, touching upon the importance of interoperability from a technology-neutral and homogeneous perspective, considering six heterogeneous BCs which can intercommunicate. Finally, chapter 1 provides details on various platforms that provisions for SSI frameworks, such as, MOBI, Polygon ID and the European BC Service Infrastructure, whose aim it is to create frameworks and standards that are compliant with EU regulation and values, and how to help adoption thereby accelerating the development of BC technology and applications with the EU.

— **Chapter 3:** The second chapter gives an overview of the Relevant Regulatory Frameworks for BC4T and goes on to list the relevant parts of regulations that either the use-cases explored need to adhere to or can help enable due to the attributes of the BC technology and components used in the explored solutions.

— **Chapter 4:** The third chapter provides a summary description of the three pilot implementations undertaken in the scope of this research work

— **Chapter 5:** The fourth chapter summarises the findings of a desktop research review that focused on a possible high-level application of BC for tolling/taxation. It initially describes the current tolling technologies providing an overview of the directives and regulations associated with tolling. The current transport taxation landscape is presented along with emission trading with the EU, giving an overview of the European Electronic Toll Service (EETS); the BC-based systems for tolling, taxation, and the ETS are then described at a higher level, followed by a suggested path for implementing a future pilot to explore the feasibility of such systems. Subsequently a detailed outline of a BC-based supply chain auditing system to track how green the fuel is and provide sustainability certification for that fuel, both considering upstream and downstream interactions.

— **Chapter 6:** The final chapter summarises the main conclusions & follow-up chapter: Provides a summary of the main findings of the study and some suggestions on possible follow up research for policy activities of interest.

2 Technological Background of BC for Transport

This section outlines the benefits of BC for transport applications, followed by a description of the technical components used in the research. Initially, the basics of a BC and its functions are explained at a higher level, followed by a more technical deep-dive considering other key features and technological components required for the explored use-cases. The various types of BC networks are listed, and differences compared. A BC technology landscape overview then lists the main BCs relevant to transport applications. The summary concludes with a section detailing the importance of interoperability and a technologically neutral approach and how communication between heterogeneous BCs can be achieved, the importance of EU partnerships and services, namely the European BC Partnership (EBP) in the form of the EBSI.

2.1 Why BC for Transport

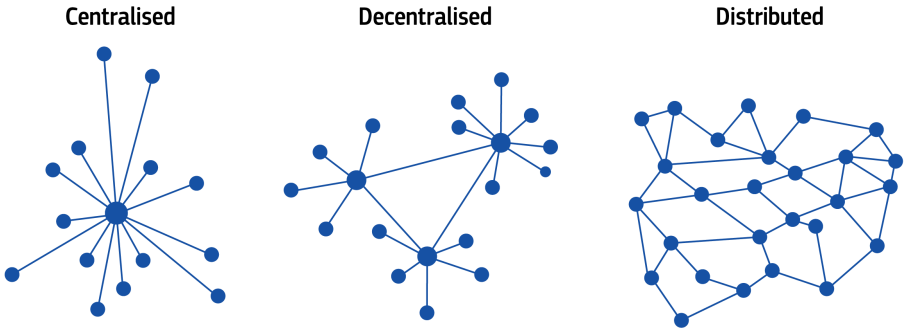
There are many benefits that BC as an emerging technology can bring to Transport applications; some of these benefits are listed as follows:

- **Immutability:** Very hard to change the history of hashes stored within a BC.
- **Decentralised Timestamping**: Clear record of when data have been transmitted, which contains the lifetime data of a vehicle, without need to trust a single entity.
- **Non-Repudiation:** Due to the immutability and decentralised timestamping of the hashed data records. It is tough for an entity to dispute their validity or which vehicle recorded said data.
- **Security:** With a decentralised network, there is increased security, due to no longer having a single point of failure.
- **Privacy:** With Zero-Knowledge Proofs (ZKPs) (described in a later section) an entity can have increased privacy while still providing a proof that a statement is true, or a data value falls within a range without providing any additional information to the verifier or leaking any information about the claim itself.
- **Auditability:** Authorities that require a global view of all the transaction and associated data can be given access with ease, with the data in a format that is easily audited digitally.
- **Identity Management:** Identities can either be managed via a Member State authority or a decentralised identity solution could also be used, allowing for increased privacy and security.
- **Automation:** Smart Contracts can be written and often reused between different entities and a set of agreements that can automatically take effect after a period or condition is met.

2.2 What is a BC?

BC records information such as messages, transactions or calls on executable code (smart contracts) batched together into blocks and added to a chain of blocks in sequential order once validated by the network. A transaction can be thought of as each transfer of an asset, where the BC is used to record those transactions such that all participants can trust that the records are valid without the need for an intermediary. A BC is decentralised, unlike a traditional database which is centralised with an administrator. Different types of BCs can vary in the degree of how decentralised they are.

Figure 1: Distributed Networks



Source: JRC, 2022.

When a transaction is initiated on a BC, a record of the transaction is stored inside a block and accompanied by a timestamp of the event. Once mined, the new block is linked to the previous block through a cryptographic algorithm called a hash. All the blocks since genesis are linked together and form the chain, thus named BC. Every node participating in the network holds a copy of the distributed ledger, with the data being replicated and synchronised continuously across all nodes.

Each peer using the BC network has a public key (an address) and a private key (can be thought of as a unique ID and a password in the form of a long alphanumeric string for each) which allows the peer to interact with the BC network (send/receive transactions, sign messages, etc.) according to a set of rules predefined in a BC protocol. A transaction initiated by a user from a public address to another public address will be digitally signed using the private key, which ensures that the transaction was sent by a user that has access to that private key.

The public address can be assigned to an IoT device, Vehicle, automated bot, piece of equipment, physical location or a container, properties can also be assigned to each address (for example, a container could have the status: "In transit between point A and B").

The key value proposition of BC is that the addresses on the BC network do not need to necessarily trust one another to be able to trust that transactions in a block are valid. This means that multiple entities can transact on the network without the risk that a party could manipulate the data without the other participants knowing about it.

Since the ledger is shared across all nodes, the data are protected from attacks aiming to alternate the data. A successful attack will require the attacker to hack the majority of nodes in the network and overwrite each node's data simultaneously. Even if this was achieved, users would be able to see that the data had been altered.

This high level of security and anti-censorship is one of the attractive features of BC, this is the reason why it is increasingly being used where it is important to transmit data securely or where it is beneficial to have a clear audit trail of exactly which transactions have occurred for a set of assets and when.

BC is changing the way that individuals, businesses and governments are able to exchange and trust data. The network effect of BC is more apparent as more of the world begins using it, as the network gradually becomes more secure, and the transfer of assets becomes more fluid.

As people begin embedding rules and logic directly into BCs using smart contracts, certain aspects of our day-to-day transactions will become autonomous, allowing for increased efficiency and control.

In Summary:

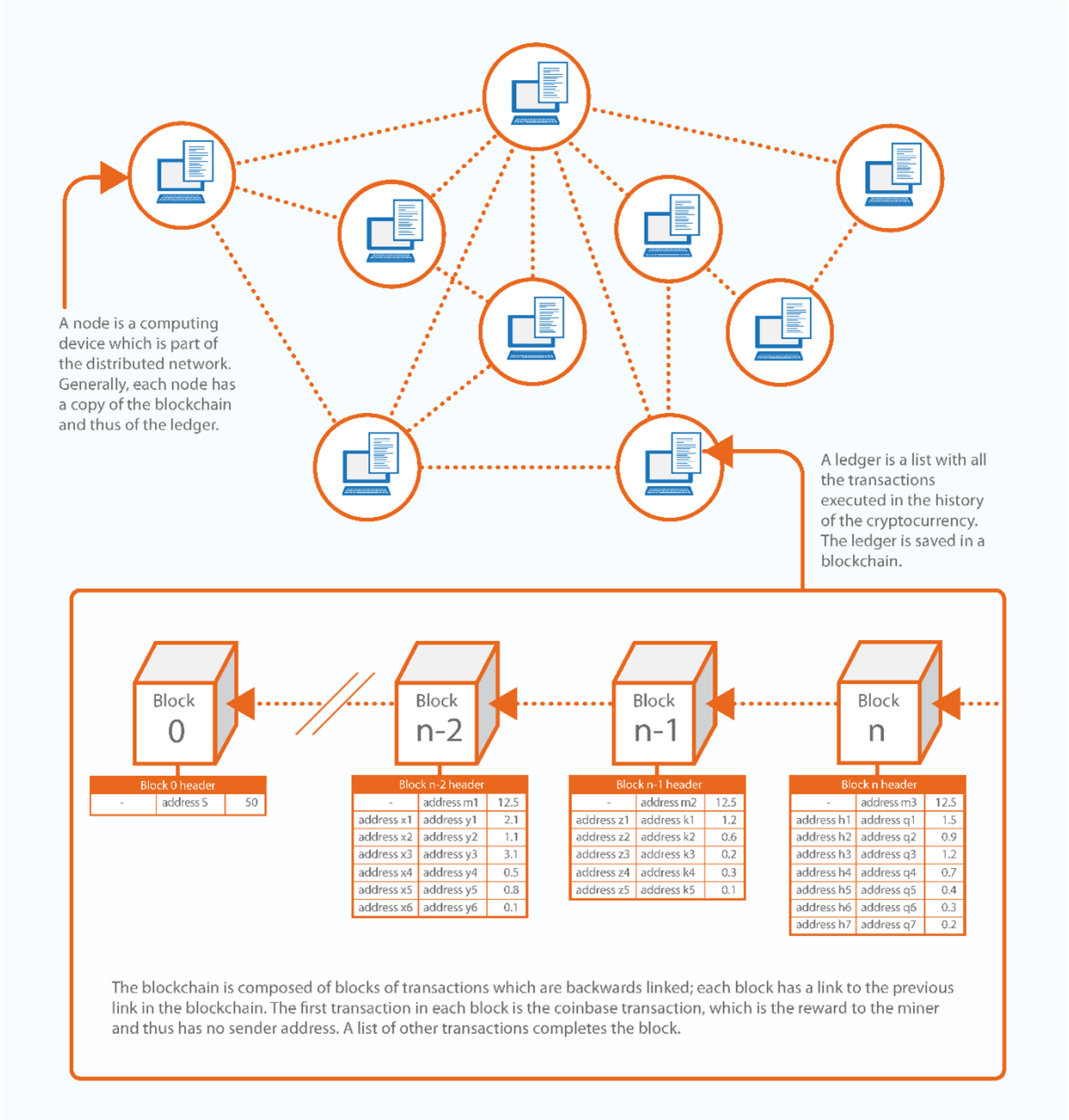
The technological components that make up a BC are not new and have been around for decades, consisting of cryptographic methods such as PoW (a form of cryptographic proof first invented by Moni Naor in 1993), networks, databases and public/private key pairs. What makes BC protocols so revolutionary is the sum of these traditional components. This combination enables transacting and recording data very securely on an immutable shared ledger. This shared ledger of all historical records among participants makes it extremely difficult to alter the data stored on the BC without detection; therefore, executions of a transaction can be done securely without an intermediary since there is a reliable truth agreed between all participants.

2.2.1 More Technical Dive, Key BC Architecture Components

The protocol is native to each BC and governs the operation of the network. For example, the protocol prevents validating invalid or duplicate transactions. In some cases, the protocol may be open source and network participants can agree on proposed modifications.

Nodes are connected and create the **distributed ledger network**, which enables the secure recording, storage and sharing of data in an immutable way using cryptographic methods and consensus algorithms. A node can be run on a laptop or even on less sophisticated hardware, and it only needs to communicate with or query the BC, generally done via the internet but could also be done via other communication channels.

Figure 2: BC network and block production depiction



Source: JRC, 2019.

The following example elaborates on how cryptography and consensus allow for trust on a BC without a trusted intermediary. Let's imagine that Alice wants to send tokens to Bob:

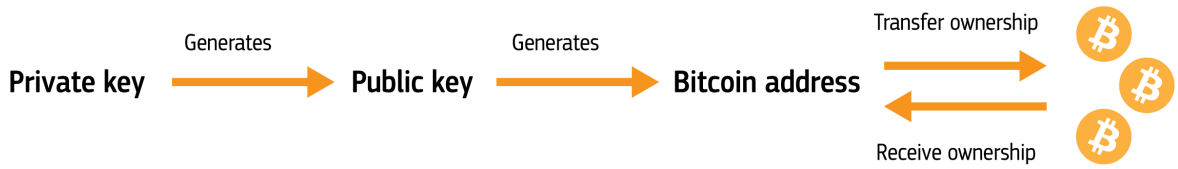
- Alice initiates a transaction request broadcasted to all nodes in the network. Nodes will then validate whether this transaction is valid. Whether Alice has enough tokens to send, if it is signed, etc.
- If Alice's transaction is valid, the nodes will bundle the transaction into a block with other transactions (the node will choose transactions paying the highest transaction fee).
- When the block is confirmed by a node using the consensus mechanism, the block is added to the chain that records the confirmed transaction of tokens to Bob's address on the BC.

Cryptography is how the security and immutability of the distributed ledgers are achieved. To participate on a BC, a user needs to generate a private key (long alphanumeric string analogous to a password) that can digitally sign and authorise transactions. This private key generates a public key (a public address that can be shared to receive funds, or for additional security and privacy is linked to another address that is shared with the public). The private key unlocks the cryptocurrency from the associated public address and the digital signature generated by the private key allows the tokens to be sent to another public address. Where the public address

is also a long alphanumeric string, analogous to a bank account number where all transactions can be seen by all participants and the amount of funds associated with each public address can also be viewed (in the case of a public permissionless BC (more later)).

The public addresses, which are derived from the private keys using cryptographic methods, are used to validate the authenticity of signatures to the associated private key. This allows for the secure validation of whether the transactions are authentic or not.

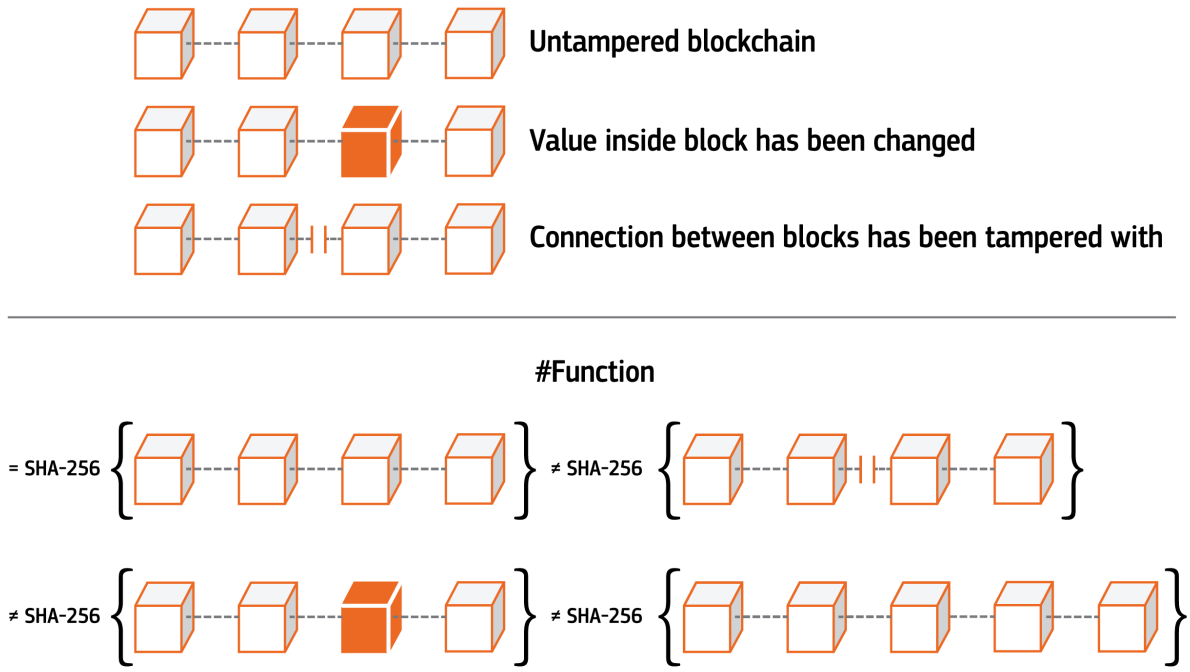
Figure 3: Bitcoin BC example.



Source: JRC, 2022.

Hashing is the cryptographic method that allows for the detection of any change in the original content in a block. A valid hash needs to be created for each new block to be considered for addition to the BC ledger. A hash is a fixed-length alphanumeric string, which is a unique cryptographic derivation of a set of digital data, in this case a block.

Figure 4: SHA-256 Hash Function



Source: JRC, 2022.

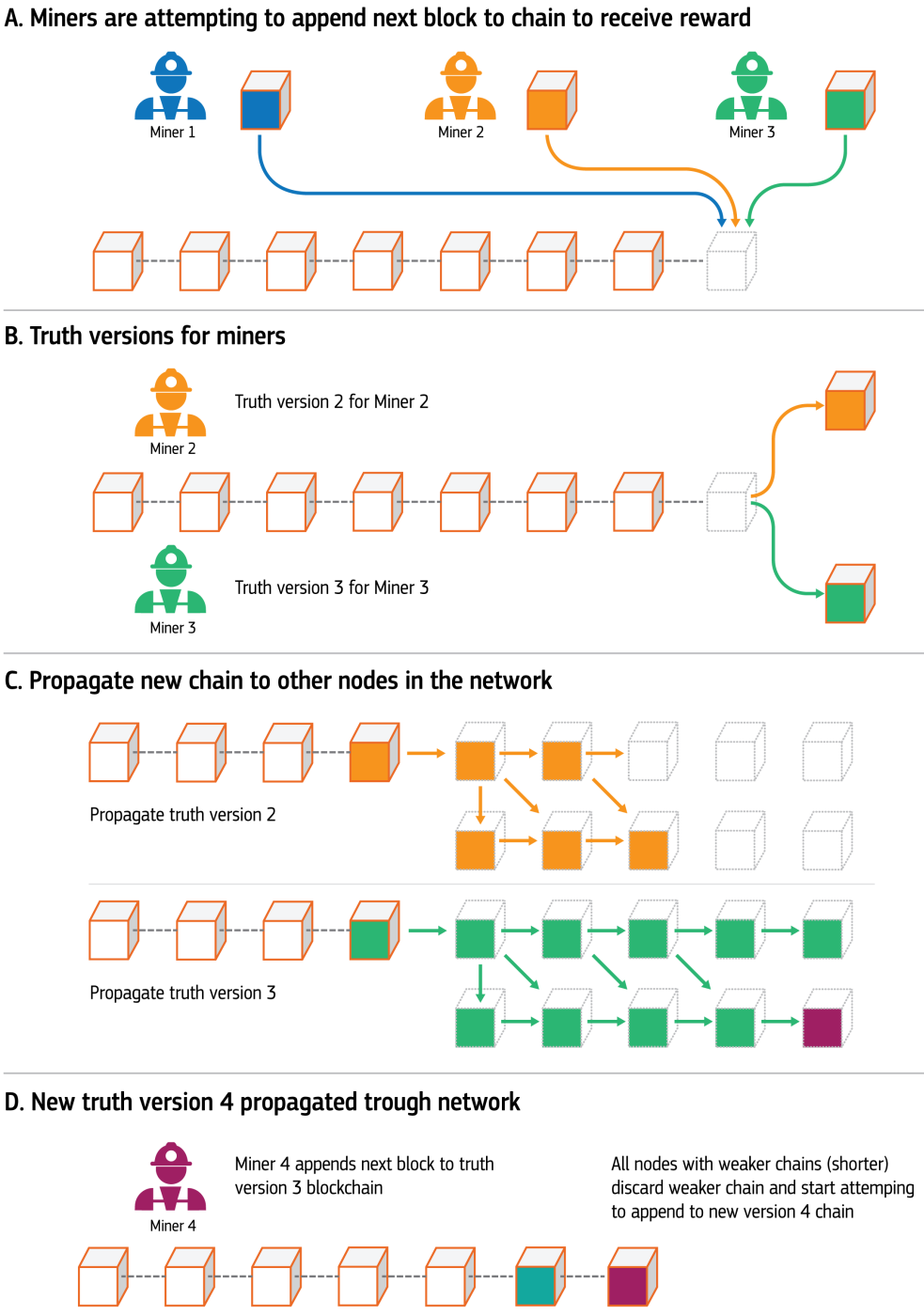
The original data cannot be generated by reverse-engineering the hash alone; this can be likened to how it is not possible to use a fingerprint to create a human finger. This analogy can be used to understand how the hash function is used as a digital fingerprint of the underlying hashed data. The data contained in each block is the input to the hash function, any slight change in this input data will lead to an output of an entirely different hash.

Even an insignificant change such as capitalising a letter contained within the data will lead to a hash that looks completely different. This component of the BC protocol allows network participants to detect any

changes in the copy of a ledger that a particular node transmits; that version of the ledger will then be rejected by the consensus mechanism on the other nodes.

A BC network can use many different **consensus mechanisms**, with many more being developed and adopted. The most common used for cryptocurrencies and public BCs mechanism is Proof of Work (PoW) which validates a newly assembled block consisting of transactions taken from a pool of pending transactions. This is done by incentivising miners to compete for a reward for mining the next block consisting of transaction fees paid on top of a block reward. Each miner contains a full copy of the ledger, which forms one of the nodes within the distributed ledger network. The miners repeatedly attempt to add a new block to their copy of the ledger by producing a valid hash of the block along with a randomly generated number (nonce). The goal is to create a valid hash with a low enough value chosen by the network's mining difficulty; this is adjusted by the protocol every two weeks so that one block is mined every ten minutes on average.

Figure 5: Miners on bitcoin network competing to miner the next block.



Source: JRC, 2022.

The mining node will then transmit the new version of the ledger to peer nodes in the network. Once the peer nodes have confirmed the hash output is a valid update and does not break any of the rules set out by the consensus rules, they adopt the new block and synchronise the newly updated ledger with the network. The other miners will then stop attempting to append a new block to the shorter version of the BC and start attempting to mine the next block using the latest copy of the ledger.

As the contributor of the new block constantly changes, it enhances the reliability and security of the network, along with the enormous amount of energy needed to outcompete the rest of the network's hash power. The consensus mechanism enables the network participants who do not trust one another to have an identical copy of the shared ledger without needing a trusted intermediary.

Another common consensus mechanism used is Proof of Stake (PoS). Some BC networks like Ethereum plan to migrate from using Proof of Work (PoW) to PoS to help with energy resource efficiency and transaction costs. To potentially act as a validator a node needs to put tokens at stake, essentially held in escrow by the network and subject to forfeiture should the node act maliciously. The more a node is trusted, the more likely it will be chosen in the block creation and validation process. Depending on the PoS consensus mechanisms in question, participants can delegate their stake to nodes that they trust or to ones which have been honest for a long period of time.

2.3 Types of BC Networks

There are three main types of BC networks: public permissionless, private permissioned and public permissioned.

Table 1: Types of BC Networks.

Type	Read	Write	Commit Block	Example BC
Public Permissionless	Open to anyone.	Open to anyone.	Open to anyone.	Bitcoin, Ethereum.
Public Permissioned	Open to anyone.	Authorised participants only.	All or subset of authorised participants.	Sovrin, Ripple, EOS, Hyperledger Indy.
Private Permissioned	Fully private or restricted to a limited number of authorised nodes.	Network operator only.	Network operator only.	Hyperledger Fabric, Quorum, Enterprise Ethereum Alliance.
Consortium	Restricted to a set of authorised participants.	Authorised participants only.	All or subset of authorised participants.	Hyperledger Fabric, Quorum, Enterprise Ethereum Alliance.

Source: Hileman & Rauchs (2017) (Hileman and Rauchs, 2017)

Public Permissionless BCs:

Everyone can view the contents stored on the BC, and anyone can participate on the network without invitation or permission and be free to leave the network. This is the main value proposition for BC, enabling peer to peer transactions without requiring a central authority to validate the transactions. The first BC, Bitcoin, is a public permissionless network, and since the inception of the BC, the public-permissionless version has garnered the majority of interest and activity from BC application developers.

There are challenges with public BCs, some of which are being solved:

— For widespread adoption of public BCs, they need to be scalable such that they can process many transactions per second (TPS). Traditional payment infrastructure providers like Visa have achieved TPS in thousands of transactions, whereas for example Bitcoin can process between 4 to 7 TPS and is limited by the number of transactions that can fit in each block (size of block) and the 10 minute interval between each block. Many different solutions are successfully worked on and implemented to scale up transactions while keeping the solutions as decentralised as possible (e.g., Bitcoin lightning network currently applied in El Salvador).

— Many entities do not want transactional data to be of public record. The hesitation towards the public networks stems from the data privacy and confidentially concerns leading research into private BCs.

Although there are many promising solutions to this issue now, using ZKPs for one to achieve data privacy while using public BCs.

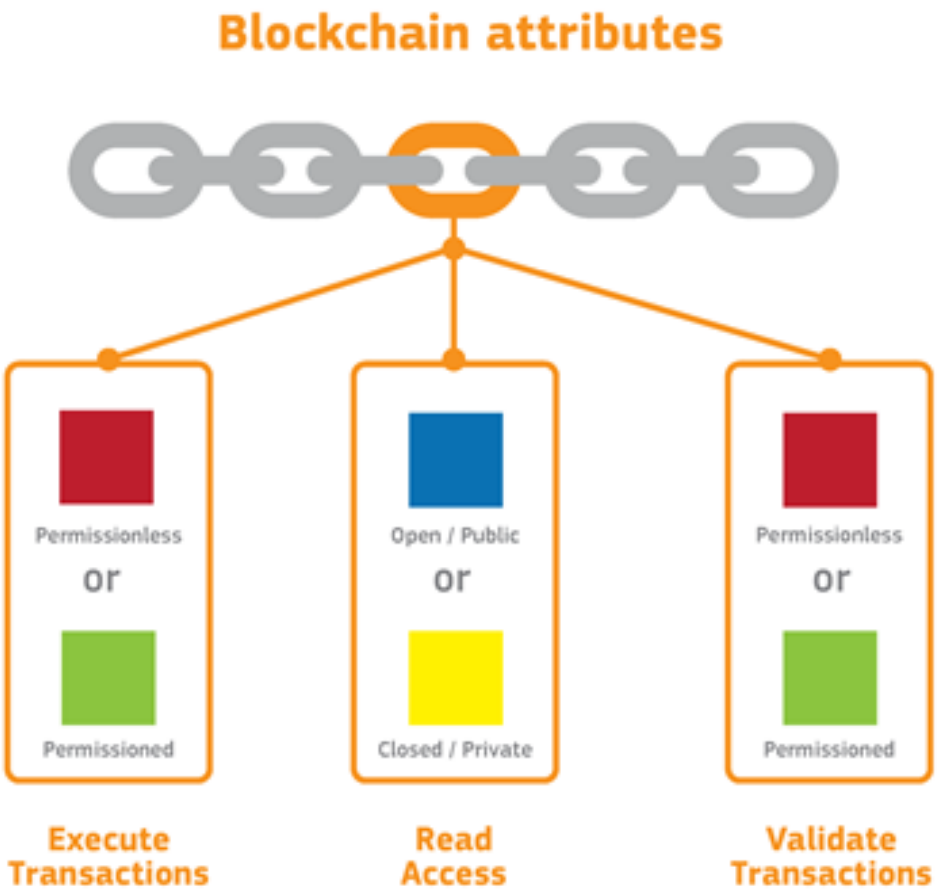
Private Permissioned BCs:

Nodes that are allowed to join this BC network are usually restricted to only those that are authorised. In addition, it can be that the Certificate Authority (CA) must authorise accounts that can submit transactions before being able to participate on the network. Due to the centralised nature of this type of BC network, scalability is facilitated.

Public Permissioned BCs:

Implementations of this flavour of BC network can permit any node to join the network yet limit which nodes are enabled to receive submitted transactions on. This means that these types of BC networks are more easily to scale due to being less decentralised but not completely centralised, like with private permissioned BCs.

Figure 6: Access Rights or Different BC Networks



Source: JRC, 2019.

Consortium BCs

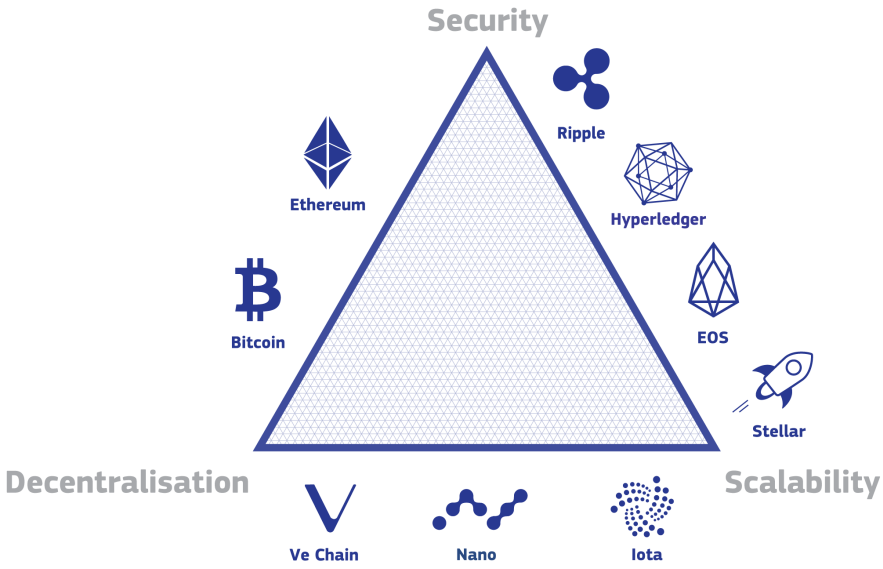
These BC networks combine aspects of public and private BC networks, although they are a bit more restrictive in nature than public permissioned BCs due to only authorised participants being able to read the BC and submit transactions to nodes.

2.3.1 Scalability Trilemma

There is a trade-off between scalability, decentralisation, and security (Hafid et al., 2020). You can choose any two of the three and implement design a BC network that can achieve those attributes to an extreme. There has yet to be an example of a BC network that can accomplish all three properties to an extreme.

With the scalability trilemma initially depicted by Vitalik (Sha, , Amiri et al., 2019), stating the trade-off of these three attributes as being “inevitable”.

Figure 7: Scalability Trilemma



Source: JRC 2022 adapted from sources (Hafid et al., 2020) and (Amiri et al., 2019).

When developing a BC, in practice, one or more of these three attributes needs to be compromised on, either being a more centralised network (like Binance Smart Chain), not being able to scale easily (like Ethereum or Bitcoin) or are less secure in general (like with Solana (CNBC, 2022), and Axie Infinity’s Ronin (Coindesk, 2022)).

2.4 Key Technological Features and Components Required

BC is considered a critical technological component of CO_2 emissions monitoring due to the increased security it can provide (removing the single point of failure from centralised solutions), enables data privacy without a third-party having access to an individual’s data, gives the end-user control over their data, and enables transparency when considering an emission trading system, while also opening the possibility to enable technical access to Decentralised Finance (DeFi) protocols if so desired for other transport applications not explored in this report. A key factor in the current BC projects choice for testing was scalability concerns, although this is becoming less of an issue with developments in public BC architecture.

2.4.1 Privacy

There are many privacy concerns associated with BCs, like the one with public networks, where the transactions and balance of wallets are openly visible with a query using the wallets’ public address. Although this public address is only a string and does not directly link an entity’s name, there are ways to associate the public address to an entity’s name by analysing all the transactions performed by the said entity and with whom and when. Especially if at some point they interacted with this wallet address from a platform which they did Know-Your-Customer (KYC) with or if they did not use a Virtual Private Network (VPN) and can associate certain traffic with times of transactions.

One public network BC that focuses on both signature privacy and metadata privacy is the NYM project, which will be described in detail in a later section. Another example is Hyperledger, a private network attempting to deal with the entire ledger being visible by opting to make it a private network where only the entities belonging to a channel can only access the transactions made by that channel’s members. Despite the use of channels, they do not provide levels of privacy wanted or needed by the user or use-case.

For private and public BCs, encryption or other privacy enabling techniques like ZKPs can be implemented as a component of the BC system, allowing for data minimisation, and increasing privacy regarding other network participants.

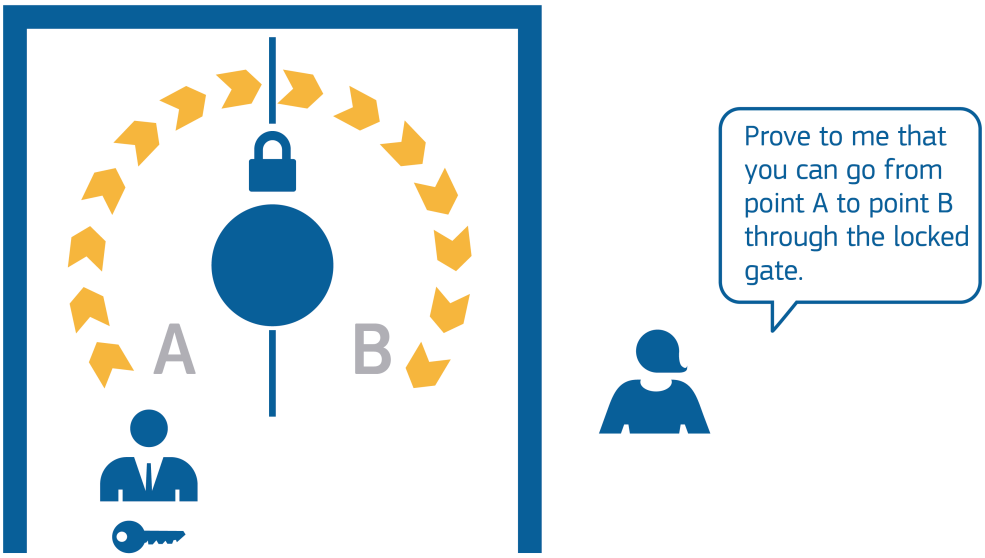
2.4.1.1 Zero-Knowledge Proofs

ZKPs is a cryptographic method in which the prover can show the verifier that a claim is true without providing any additional information to the verifier or leaking any information about the actual claim itself. This allows for claims to be verified by adopting ZKPs, enabling privacy by providing the minimal information required to verify a claim. This prevents the disclosure of sensitive personal data to the verifiers while providing proof that certain parameters are met of that a claim is true or false.

Types of ZKPs include algorithms such as Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs) (Guan et al., 2020, Ben Sasson et al., 2014, Pinto, 2020, Panait and Olimid, 2021), Zero-knowledge Scalable Transparent Argument of Knowledge (zk-STARKs) (Panait and Olimid, 2021, Ashur and Dhooghe, 2018), non-interactive Zero-Knowledge Range Proof (ZKRP) (Li et al., 2020), among others.

In recent years there has been a significant increase in research papers utilising ZKPs for solving the issues relating to data integrity and data privacy in mobility applications such as; Traffic Management using Hyperledger Fabric and Hyperledger Ursa cryptographic library (Li et al., 2020) combined with Zero-Knowledge Range Proofs (ZKRPs) which allows the BC network to validate that a secret number (Li et al., 2020) is within a known range without disclosing the secret number . Additional research has included ZKPs for other applications of Location in IoT (Wu et al., 2020), which is key for applications such as automating the charging process of electronic vehicles (Gabay et al., 2020).

Figure 8: Over Simplified Depiction of ZKPs.



Source: JRC, 2022.

2.4.2 Identity

While the emission monitoring requires the vehicle identity (IoT device identity or VIN) as a key component, the emission tolling and trading mandates the driver identity (user or could include passengers). With access management of identities controlled by a centralised authority, there are issues ranging from security with a single point of failure, performance should there be a technical issue, or a Denial of Service (DoS) attack and privacy concerns should the centralised database information be leaked (Haddouti and Kettani, 2019, Cao and Yang, 2010, Dabrowski and Pacyna, 2008).

2.4.2.1 X.509 Certificates

A particular format of Public Key Certificates (PKCs) that links public keys to an entity's name is the X.509 certificate, defined by the X.500 working group (Cooper et al., 2008). Although the X.509 certificate can be

self-signed, normally, there is a Certificate Authority (CA) who is trusted and signs the certificate. The certificate can then be used to enable secure communications with another entity or authorise a transaction or validate documents signed by the corresponding private key.

An entity that requires a certificate to be signed submits a request via a Certificate Signing Request (CSR). This request is initiated by first generating a public/private key pair and using the private key generated to sign the CSR, which contains the public key and information relating to the entity (can include credentials or a proof of identity) while keeping the private key hidden. The public key is used to verify the entity's signature, if validated and approved, the CA will issue an X.509 certificate that links the public key to the entity's identifying information along with the name of the entity (referred to as the distinguished name).

In the X.509 standards, there is also a method defined for certificate revocation, in which a list is distributed that contain certificates that are no longer valid according to the signing authority.

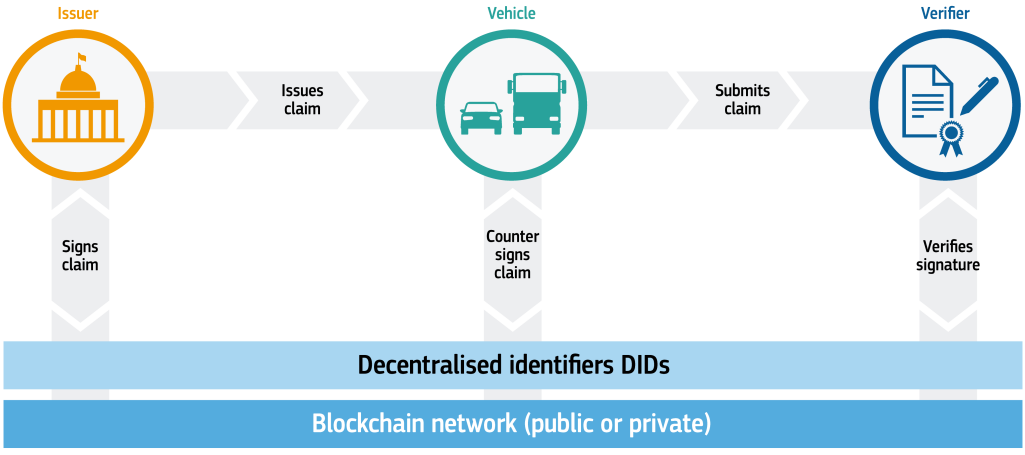
2.4.2.2 Self-Sovereign Identities

Research and development into the identification of entities (organisations, devices, and users) over the internet, named "Self-Sovereign Identity" (SSI), has been on the rise. The main idea behind SSI is that entities, especially users, should have oversight over their own identity and ownership of the associated data, instead of third parties storing and managing the information related to their identity. SSI allows for increased privacy, decentralisation, and oversight over one's own identity.

A significant analysis of the different approaches for online identity and authentication in the context of IoT environments has been explored by Fredrecheski et al (Fedrecheski et al., 2020) that includes the benefits and drawbacks of using standards such as X.509 (Terzi et al., 2020, Fedrecheski et al., 2020), PGP (Fedrecheski et al., 2020, Callas et al., 1998) and SSI (Terzi et al., 2020, Fedrecheski et al., 2020). This research advocates for the use of the two main standards used in SSI frameworks which are Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) (Reed et al., 2020, Consortium et al., 2019). DIDs incorporate cryptographic methods for identification while VCs enable authentication of a claim or credential with a focus on privacy often using ZKPs.

To enable an entity's full control over its own digital identity (Allen, 2016), SSI utilises data identifiers that are kept offline and carried by the owner within a physical wallet. Compared to digital certificates or account-based solutions held by a centralised database which is currently the norm, having privacy and security issues attributed. As society is giving more importance to privacy and security of information, research in SSI has developed a set of technical specifications to implement SSI. These standards include definitions for SSI (Allen, 2016, Ferdous et al., 2019) as a set (for example, name-value pairs) or all attributes and identifiers relating to an individual encompassing over one or many decentralised domains. The entity or individual remains in control of the attributes associated with their identity (Ferdous et al., 2019).

Figure 9: Vehicle with Self-Sovereign Identity



Source: JRC, 2022.

2.4.2.3 Decentralised Identifiers

A DID allows for digital identity without a centralised entity that can be used as a permanent identifier which is resolved to get some metadata. It is verified through cryptography and can be utilised to encrypt communication channels for secure messaging. An entity, depending on the purpose, can have many different DIDs. The standardisation of decentralised identities has been accelerated by the World Wide Web Consortium Credentials Community Group (W3C-CCG) (Reed et al., 2020).

The identification of the framework of a DID is possible with a prefix used within the syntax *did:<framework>:<did>*, for example, *did:sov:ADfadfQEKn234rafsAS34F* for Sovrin (sov,) that utilises Hyperledger Indy or another is *did:uport:CLkjkvk375Akdu83asdDF* for uPort (uPo,) that develop identity-centric applications on the Ethereum platform. The prefix facilitates the identification of the underlying framework of a specific DID.

An in-depth analysis of the different frameworks popular for SSI has been performed by Bartolomeu et al (Ferdous et al., 2019), discussing and concluding that no production-ready SSI framework is available, and all of the mentioned frameworks will face feature changes and modifications.

DID Documents (DDo) contain the public keys linked to the DID, the DID itself, and the service addresses it can interact with. The service information details which entities can be communicated with and the public key to encrypt and authenticate the messages sent to those entities. For increased privacy and security, the DDo can be stored locally with the user and the private key associated with the public key contained in the DDo, which grants control over the DID itself (Fedrecheski et al., 2020).

2.4.2.4 Verifiable Credentials and Claims

Verifiable credentials (VCs) allow for provable and portable claims about an entity and are one of the W3C (Consortium et al., 2019) recommendations. An example would be if an individual claims to have the name John or a device claim to be a vehicle. A VC is linked to a specific DID, for example, to the vehicle it relates to, in addition, it contains information about the DID that it was issued by and a cryptographic proof. A verifier can then use this information to check from a public ledger that contains issuers, read the information in the DDo of the issuer and verify the authenticity of the VC (Fedrecheski et al., 2020).

2.4.2.5 Required Properties of SSI Solutions in General

When considering general use-cases of SSI that are user-centric (can have different implementations focused more on law enforcement applications), it is important to consider what properties are required for SSI and how BC technology combined with ZKPs enables these properties.

C. Allen (Mühle et al., 2018) built upon the work of K. Cameron's seven properties (Cameron, 2005) of evaluation criteria for SSIs by dividing the stated properties into more defined characteristics, enabling more comprehensive analyses. The following characteristics that are quoted (Stokkink and Pouwelse, 2018) are from the research performed by Q. Stokkink and J. Pouwlse where they added the final characteristic that a claim needs to be verifiable (Stokkink and Pouwelse, 2018); otherwise, the claim a user is making is of-course meaningless.

1. **Existence:** "Users must have an independent existence. An SSI should be based on an identity in the real world and cannot exist exclusively in the digital world. At any time, a person should be able to independently create a digital identity, without the intervention of a third party".
2. **Control:** "Users must control their identities. Users have the full authority over their identity. "They should always be able to refer to it, update it, or even hide it"".
3. **Access:** "Users must have access to their own data. All personal claims and data should be easily retrievable for a user. No personal data is hidden for the user."
4. **Transparency:** "Systems and algorithms must be transparent. SSI solutions and their algorithms should be open in how they function, how they are managed and updated. "The algorithms should be free, open-source, well-known, and as independent as possible of any particular architecture"" (Mühle et al., 2018).
5. **Persistence:** "Identities must be long-lived. Identities can only be removed by the user. Claims can be updated and removed, but the identity that belongs to these claims should be long-lived".
6. **Portability:** "Information and services about identity must be transportable. An identity should not be held solely by a third party. It should be transportable, since third parties may disappear".

7. **Interoperability:** "Identities should be as widely usable as possible. A true SSI is globally usable and not limited to certain niches".
8. **Consent:** "Users must agree to the use of their identity. Claims and data cannot be shared without the user's consent. Users are in control of the sharing of their data".
9. **Minimisation:** "Disclosure of claims must be minimised. Only the necessary data must be shared, when sharing some part of an identity. For example, only sharing being older than 18, instead of your date of birth. This property fits well with zero-knowledge proofs".
10. **Protection:** "The rights of users must be protected. The rights and freedoms of individuals have priority over the needs of the network".
11. **Provable:** "Claims must be shown to hold true. It should be possible for claims to be verified, for example by trusted third parties".

These characteristics that should be incorporated into SSI solutions are enabled by BC, ZKPs, decentralised, encrypted storage (or local storage of user's data on IoT or mobile device) and interoperability solutions (described later). Allowing for providing EU citizens with the possibility of controlling their own data and digital identity without a few large companies based outside the EU in practise being the ones who hold and control the data and digital identities.

2.5 BC Technology Landscape and Overview

In this subsection an overview of the relevant BC networks is provided, with details of performance, scalability and energy uses; for the BCs of interest for transport applications.

The BC technologies used will vary depending on the use-case and the entities involved. As described in the following section, BC architects and developers are researching and implementing methods for cross-chain communication as the different systems created for specific use-cases will need to interoperate, allowing for a network of BC networks running in tandem and communicating when needed. This section presents a review of the current state of the art in BC frameworks.

2.5.1 Hyperledger

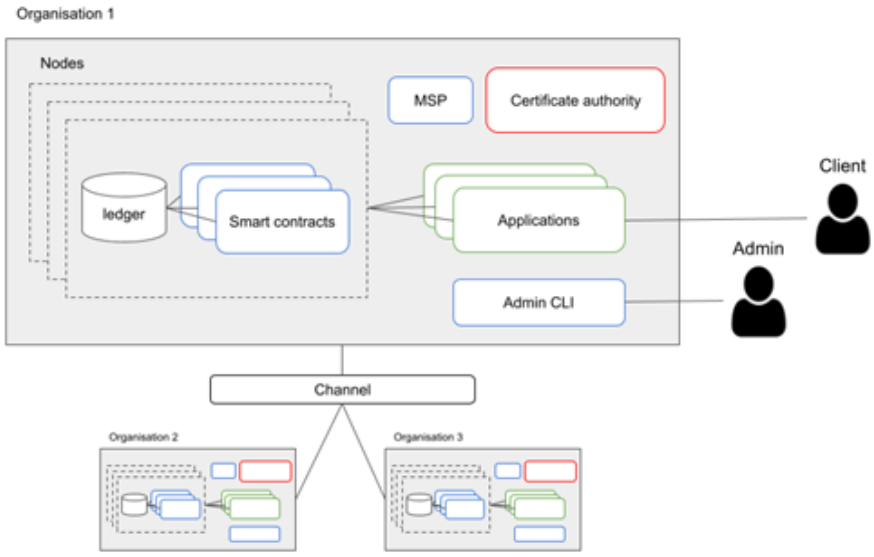
Hyperledger was started in 2015 as a series of open-source frameworks, focusing on different solutions and tailoring the BC frameworks for different tasks. The Linux Foundation initially developed the Hyperledger Foundation (rebranded in 2021), but later received contributions and membership from IBM, Intel and SAP. (**?**)

Hyperledger Fabric

Hyperledger Fabric (HLF) is a framework for developing a private-permissioned DL with a modular architecture design (HLF, a). Users and nodes who participate in the network need to have a unique identity managed by the Membership Service Provider (MSP) (Androulaki et al., 2018). These assigned unique identities also have an associated privilege which is set by the MSP. The MSP has the function of verifying the identities and roles of participants in the network.

Under the Hyperledger Fabric framework, networks form the technical infrastructure that provides ledgers and smart contract services to applications managed by different organisations, as would be the case for the proposed architecture. In most cases, *"multiple organisations come together to form a channel on which transactions are invoked on smart contracts"* (Hyperledger, 2022a), whilst permissions are determined by a set of policies agreed upon a channel's original configuration.

Figure 10: Hyperledger Fabric conceptual network structure



Source: JRC, 2022.

Organisations, such as regulators, service providers, fuel suppliers, and distributors, conceptually form entities with access to channels and can issue identities to participants so that every transaction's source is identifiable. The identities of BC nodes, the clients or the administrators must be created by a Certificate Authority (CA) associated with each organisation. CAs play a key role in the network because they dispense certificates used in identifying components that belong to an organisation. These certificates are stored in a set of folders called MSP.

Scalability:

- **Transactions per second (TPS):** Scaled to fit needs. An experiment performed by IBM shows for a node with 4 virtual Central Processing Units (vCPUs) and 16 Gigabytes (GB) memory with Solid State Drive (SSDs), and 2 endorsers reach 785 TPS, 4 endorsers reach 948 TPS, 8 endorsers reach 1265 TPS (Liu et al., 2020). A paper looking at scaling HLF via reducing bottlenecks and reducing the overhead of transaction ordering reaches 20k TPS (Gorenflo et al., 2019).
- **Energy consumption:** Depends on the network implementation in question.

Hyperledger Indy:

Hyperledger Indy (HLI) is a public-permissioned DL design with a focus on decentralised identity applications, hence allowing for SSI (HLI, a) Applications. HLI does not contain the functionality for smart contracts hence does not allow for many of the operations that are required for CO_2 monitoring, trading, and tolling (such as the transfer of tokens) without combining with the capabilities of HLF for example. HLI utilises the Plenum consensus protocol (HLI, a), which is a specific implementation of the Redundant Byzantine Fault Tolerance (RBFT) protocol (Abraham et al., 2018). Validation and ordering of identities and Verifiable Credentials (VCs) are performed by participating nodes interconnected to persist in the same ledger state with each communication signed utilising elliptic curve cryptography.

Hyperledger Quilt:

Hyperledger Quilt (HLQ) is an implementation based on Java for the Interledger protocol enhancing the inter-operability of payments across fiat and digital currencies (et al, 2022). HLQ uses atomic swaps (Foundation, 2022d) for the transactions to provide an implementation of core actions in a ledger-agnostic manner. As of August 2021, the Foundation announced (HLq,) that no new features and no active support are developed by the maintainers.

Table 2: Types of HyperLedger Frameworks and Descriptions.

Frameworks	Description	Type
HL Aries	"Hyperledger Aries is infrastructure for BC-rooted, peer-to-peer interactions" (HLA, a).	Library
HL Avalon	"Avalon is a ledger independent implementation of the Trusted Compute Specifications published by the Enterprise Ethereum Alliance. Avalon extends computational trust to off-chain execution enabling improved BC throughput and scalability and Improved transaction privacy with attested Oracles, trusted reporters of data generated outside of the BC" (HLA, b).	Tool
HL Besu	"Hyperledger Besu is an open source Ethereum client developed under the Apache 2.0 license and written in Java. It can be run on the Ethereum public network or on private permissioned networks, as well as test networks such as Rinkeby, Ropsten, and Görli. Hyperledger Besu includes several consensus algorithms including PoW,PoA Istanbul Byzantine-Fault Tolerant (IBFT), (Etherhash and Clique), and has comprehensive permissioning schemes designed specifically for uses ina consortium environment" (HLB, a).	DL-software
HL Burrow	Modular BC client that supports EVM and WASM type smart contracts. Utilises Byzantine-Fault Tolerant (BFT) consensus through Tendermint algorithm. Aimed to be used for public permissioned PoS applications but can also be utilised for private/consortium network applications (HLB, b).	DL-software
HL Cactus	"Hyperledger Cactus is a BC integration tool designed to allow users to securely integrate different BCs" (HLC, a).	Tool
HL Caliper	Hyperledger Caliper is a tool to benchmark and measure the performance of a BC for a certain use-case implementation. Currently functions with HL Besu, Burrow, Fabric, Iroha, Sawtooth and Ethereum (HLC, b).	Tool
HL Cello	Hyperledger Cello provides an operational dashboard for managing BCs efficiently that can run on top of various infrastructures from VMs to container platforms. Helps creating BaaS and serves as the operational dashboard for BC (HLC, c).	Tool
HL Explorer	Hyperledger Explorer is a tool for viewing and querying blocks, associated data (transactions, etc.) and other information stored on the ledger (HLE,).	Tool
HL Fabric	Platform for distributed ledger solutions modular architecture, allows for privacy, flexibility, resilience and scalability (HLF, b).	DL-software
HL Grid	Designed for Supply Chain solution implementation and business logic type smart contracts (HLG,).	Domain-specific
HL Indy	DL providing tools, libraries and reusable components purpose-built for decentralised identity applications, built to be interoperable with other BCs (HLI, a).	DL-software
HL Iroha	DL software aimed for simplistic use with infrastructure and IoT use-cases that require DL technology. Modular in design that utilises crash fault tolerant consensus algorithm, called YAC (HLI, b).	DL-software
HL Quilt	"Hyperledger Quilt is an implementation of the Interledger Protocol enabling payments across both crypto and fiat networks" (HLq,).	Library
HL Sawtooth	Modular platform used for building, deploying and running DLs Sawtooth various consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT) and Proof of Elapsed Time (PoET) (HLS,).	DL-software
HL Transact	"Hyperledger Transact is a library that aims to reduce the effort when writing DL software by providing a standard interface for executing smart contracts" (HLt,).	Library
HL Ursa	"Hyperledger Ursa is a cryptographic library which enables implementations to avoid duplicating other cryptographic work and increase security" (HLU,).	Library

Source: HyperLedger Website and Documentation

Hyperledger Cactus:

Hyperledger Cactus (HLC) is a tool to enable cross-BC communication and integration to enable BC interoperability (HLC, a). It aims to solve interoperability between the different BCs in a secure manner. The framework can accelerate the development cycle by including libraries, data models, and more. Some of the framework's features (petermetz et al, 2022) include connectors, atomic transfers, decoupled identity, and metrics.

Hyperledger Aries:

Hyperledger Aries is a toolbox for developing, transferring, storing, and using verifiable digital credentials. Protocols that enable connectivity between agents using secure messaging to exchange information are at the heart of the system. Peer-to-peer interactions between agents controlled by various entities—people, organisations, and things—are central to Aries. Verifiable credentials can be exchanged based on DIDs rooted in different ledgers (based on Indy or other technologies) utilising a variety of verifiable credentials implementations using its standardised messaging layer (HLA, a).

The Aries RFC repository is composed of a verbose list of documents, each of which addresses different technical aspects. Over time, changes to the specifications will result in different versions of the documents, with status (Proposed, Demonstrated, etc.) and protocol version numbers shifting. This is a positive signal towards gradual improvements regarding technical details stemming from the community's increased cumulative experiences. To facilitate true interoperability, the Aries community needed a means for implementers to target the same versions of the protocols. In addition, when the community stabilises, it needs a method to modify that target to adopt new and updated protocols. The Aries Interoperability Profile (AIP) is the technique that the Aries community has selected towards this goal. The solution discussed in a later section 4.3 builds on top of AIP 1.0.

2.5.2 Corda

Corda's development has been with applications specific to the financial services industry, unlike HPF and Ethereum which is in many ways industry agnostic.

Consensus is reached at the transaction level on Corda by only involving permissioned entities involved in that transaction. As the applications of Corda are not geared towards the topics of emission monitoring and no research papers have been found using Corda for IoT device use-cases, a review for this DL technology has not been performed.

2.5.3 Quorum

Similar to HLF, Quorum is an Ethereum based DLT implementation which is permissioned with a network and peer permissions management system and allows for increased privacy for transactions and smart contacts. The smart contract language is Solidity based (Quo,), and network implementations can still have an associate Ether token. A Quorum network can be deployed utilising the Istanbul BFT or Raft consensus algorithms and has increased performance when compared to the Ethereum mainnet due to increased centralisation. In the review of the online literature relating to mobility applications, only one study was found that considers Quorum (Brousmiche et al., 2018), and a limited number of papers relating to IoT devices (Nayak et al., 2018, Reyna et al., 2018, Chr, 2017).

2.5.4 Ethereum 1.0

Ethereum currently runs on a PoW consensus mechanism which requires a lot of energy to reach consensus among participating nodes in the network. Due to the network's popularity, currently exceeding even bitcoin in terms of the number of transactions, the cost of performing a transaction is becoming too expensive for most use-cases. When performing a trade on a Decentralised Exchange like Uniswap (more complicated than a simple transfer from one wallet to another where the cost can exceed 100$ just to cover the gas fees.

The resultant high gas cost to perform a transaction on the network leads to the use of layer two solutions until smart contracts are enabled on the beacon chain of Ethereum 2.0, which will run using a PoS consensus mechanism to reach scalability via a sharded network, enabling cheap transactions.

Scalability:

- **Block time:** Current average is at **13 seconds** (ycharts, 2022).
- **TPS:** On the 8^{th} of April 2021, the network was performing **16 TPS** TPS. Since 2017 the speed has ranged between 6 and 16 TPS depending on the number of miners and the hash rate of the network (blockchair, 2022).
- **Energy consumption:** Estimated Annual Energy Consumption is **26 TWh**'s compared to that of Bitcoin, estimated at 130 TWh.

Layer two solutions:

Layer two solutions are fast developing and have started to be implemented by a range of the BC Decentralised Applications (Dapps). They include the following networks.

- **Polygon (previously MATIC):** is a PoS, layer two solution that can reach cheap and fast transaction speeds by using sidechains for processing transactions submitted on the Polygon mainnet. Assets can then be bridged back to the Ethereum mainchain using the robust Plasma bridging framework (Pol, d), which is compatible with the Ethereum Virtual Machine (EVM).
- **Skale Network (SKL):** is another layer two solution that achieves high-throughput demand with efficient gas cost and is compatible with the EVM (Ska, 2022).

2.5.5 Ethereum 2.0

Ethereum 2.0 is a PoS public permissionless BC protocol, where scalability is reached by processing transactions on diverse shards and interoperating between these shards via a communication protocol.

Ethereum 2.0 has a hybrid consensus, in which block production and finality utilise different protocols. For finality, Casper FFG is used, which is a GHOST-based protocol that finalises batches of blocks in one cycle. It is planned to have 32 blocks in each batch being finalised during an epoch (period of time). With the estimated block time being 12 seconds, it is predicted that finality will be reached between 6-12 minutes (djrtwo, 2022).

For block production, Ethereum 2.0 uses the Random Decentralised Autonomous Organisation (RandDAO) protocol which is a slot-based protocol that chooses validators randomly to a slot and administers a fork choice rule for un-finalised blocks. For each validator instance, exactly 32 ETH is required as a stake. Validators, when selected randomly and grouped with a set of validators, are called a committee, which validates shards in the network. A large number of validators are required to guarantee the validity. For the network, 111 validators are required per shard and to reach finality a further 256 validators per shard are needed during an epoch. For 64 shards that would be 16,384 validators that are needed.

Scalability:

- **Block time:** Currently estimated at **12 seconds** with finality reached after 6-12 minutes (djrtwo, 2022).
- **TPS:** Estimated to be able to handle 100k TPS, although no empirical data yet.
- **Energy consumption:** PoS uses a minor amount of energy and could have nodes running on Raspberry Pi's, although no empirical data of network size, usage, energy consumption yet.

2.5.6 Polkadot

Polkadot (Pol, c, Pol, b, Pol, a) is a Nominated Proof of Stake (NPoS) multi-BC network, where most of the BCs in the network are built using Substrate (a modular framework typically using the GRANDPA consensus algorithm), with the aim to allow inter-communication between heterogeneous BCs. Polkadots multi-BC network consists of the following components.

Relay Chain:

is the mainchain of Polkadot, which consists of a narrow number of transaction types that are allowed, which validators can validate by holding a number of the native token called DOT. The minimal functionality allowed on the Relay chain is intentional (e.g. no smart contract functionality) as the main purpose of the Relay Chain is to coordinate the entire multi-BC system, with specific processing being delegated to and performed by the Parachains and Parathreads.

Parachains:

receive and process transactions and are dedicated to a chain that is running processes constantly (Parathreads can be shared between a group and are for processes that need to be run less frequently and are woken up when required). Parachains are where the majority of the processing occurs on the Polkadot network, where various-use-cases are performed on a particular Parachain (or Parathread) implementation. There is a constraint for Parachains to adhere to, which involves the generation of a verifiable by the validators proof assigned to the Parachain in question verifying the state.

A Parachain might focus on particular use-cases such as privacy or scalability, while others might not even have a BC architecture at their core. Due to this parallel architecture of the transactions processed on Parachains, the network achieves scalability, with security being shared and provided by the Relay chain validators. For some heterogeneous BCs, the Parachain would be responsible for its own security (an example being the state transition function is a ZKP or the BC is running its own consensus algorithm); there would need to be a Byzantine agreement between the stakers before a Parachain block is logged as valid. This agreement is needed, and the data associated with the alternative consensus would be unknown to the Relay Chain validators. The communication with other Parachains occurs using Cross-Chain Message Passing (XCMP) which is a mechanism based around Merkle trees to ensure fidelity.

Bridges:

are the technological components that enable BC interoperability in which transactions can be communicated between heterogeneous BCs running their native diverse consensus algorithms. These Bridges can have various designs, from more centralised and trusted to decentralised and trustless. One might use a Bridge Pallet for Substrate native chains, like Kusama and Polkadot. *"If the chain is not on Substrate, there would be smart contracts on the non-Substrate chain to bridge (Ethereum mainnet will have bridge smart contracts that initiates ETH transactions based on incoming XCMP messages)"* (Robinson et al., 2022). In the case of BCs with no smart contract support like Bitcoin, protocols like XClaim (Zamyatin et al., 2019) and similar ones could be used. Another option is the use of a Tendermint bridge (cho,).

The key roles played by participants on the Polkadot network are:

- **Validators:** When elected, they will produce blocks on the Relay Chain by sealing the Parachain block headers to the Relay Chain through accepting proofs of valid state transitions from collators, receiving a staking reward as an incentive.
- **Collators:** Run full nodes on both the Relay Chain and *"Parachains, collecting transactions from the Parachains, propose blocks and provide zero-knowledge non-interactive proofs proving the transactions result is a valid transition state to the validators"* (Robinson et al., 2022) on the Relay chain. In addition, they can receive/ send messages from/to other Parachains using XCMP.
- **Nominators:** Nominate their stake to a validator which increases the validator's likelihood of being elected to produce the next block and are rewarded with a portion of the staking rewards.

Interoperability:

Polkadot can reasonably be expected to be bridgeable to any systems programmable enough to recognise its GRANDPA-based finality technology and its associated pieces (one of which is designed to make it easy for Ethereum based DLs) and which themselves have a viable efficient light-client. The interoperability extends to all Ethereum based flavours of Hyperledger like Fabric or Quorum. The simplicity and flexibility of the Polkadot Parachain model do make private/permissioned networks fairly easy to fit; much more so than the smart contract model where you've little choice but to bridge.

Scalability:

- **Block time:** Blocks are currently produced once every **6 seconds** (Salman, 2022) with expected time to finality likely between 12-60 seconds.
- **TPS:** Estimated to allow the network to process transactions at **1K TPS** once fully up and running after Parachain auctions (Byrne, 2022).
- **Energy consumption:** Estimates will be known once Polkadot is fully up and running with Parachains and normal network usage levels are known.

Notable PolkaDot native projects relevant to project focus:

- **Kylin network** (Kyl,) providing valid on/off-chain data via Oracle and Data Marketplace.
- **Litentry** (lit, a) is a cross-chain identity aggregator enabling decentralised identity storage, identity authentication, identity ownership and identity data allocation (lit, b).

2.5.7 Cardano

Cardano (ADA) (Car,) is a third-generation, scalable, PoS permissionless public BC network that utilises the Ouroboros BFT consensus mechanism. The Cardano network has been slow in the architecture development process due to the fact that it has followed a more academic approach to its development, following a peer review methodology allowing for academic discussion and debate before choosing and implementing a certain architecture.

When considering mission critical software applications (for example traffic management) where bugs in the smart contract code could lead to human harm, there is merit to choosing Cardano over other BCs. This is due to the fact that Cardano is based on Haskell a functional programming language where you can build pure functions (function in the mathematical sense) in a modular way and test them in isolations, which allows code to be more easily verified that the code will behave as designed too.

Another interesting aspect of Cardano is the availability of tools and utilities incorporated into its design, such as use-cases specific ones, enabling the off-chain functionality auditing while maintaining privacy preservation on-chain and still be regulatory compliant and have data that can be provided to the relevant national authorities when an audit is required.

Scalability:

- **Block time:** Block time: Blocks are currently produced once every **20 seconds**, with **finality** reaching after approximately **2 minutes**.
- **TPS:** Needs more empirical data as smart contracts are recently enabled, and users and developers have started building on and adopting the network.
- **Energy consumption:** As the network uses a PoS algorithm, energy consumption will be small. Need more empirical data as smart contracts are recently enabled, and users and developers start building on and adopting the network.

2.5.8 Cosmos Network

Cosmos (Cos, b, Cos, a) enables multiple BCs to inter-communicate through the main BC called the Hub. The BCs that are communicating with each other through the Hub are referred to as Zones. Currently, the Hub and Zones normally use a particular Practical Byzantine Fault Tolerance consensus algorithm (Castro et al., 1999, Castro and Liskov, 2002) called Tendermint (ten,). Both the Hub BC and the Zone BCs require their own validators, with there being an element of trust between the validators of the Hub and the Zone interacting. One of the aims of Cosmos is to enable multiple heterogeneous BCs to inter-communicate, allowing for a variety of flavours of BC architecture to inter-operate from the type of consensus algorithms used to being permissioned or permissionless.

Scalability:

- **Block time:** Tendermint BFT typically has block times of between 1 and 8 seconds, with the Cosmos Hub having about 7.25 seconds per block and "instant" finality (i.e.) after each block produced (Cos, b, Cos, a).
- **TPS:** Can handle up to a few 1000 TPS (Cos, b, Cos, a).
- **Energy consumption:** Estimates will be known once the Cosmos network is more adopted and running at standard working conditions.

Table 3: Types of Hyperledger Frameworks and Descriptions.

BC Network	Type of Network	Consensus Strategy	Consensus Algorithm	Block Time	Time to Finality	TPS	Energy Consumption
Hyperledger Fabric	Private Permiss -ioned	Proof of Authority	Consensus module is chosen, set as RAFT - Crash Fault Tolerance (CBFT)	Chosen	Depends on system setup	1k to 20k	Depending on Infrastructure used. Normally low energy consumption.
Ethereum	Public Permiss -ionless	PoW	ETHASH (Dagger-Hashimoto)	13s	36x13s	16	High energy usage
Ethereum 2.0	Public Permiss -ionless	PoS	Hybrid of Casper FFG Practical Byzantine Fault Tolerance (PBFT) to achieve finality and RandDOA for block production	12s	6-12 mins	up to 100k	Very low energy usage
PolkaDot	Public Permiss -ionless	Nominated PoS	GRANDPA (PBFT) for finality and BABE for block production	6s	12-60s	up to 1k	Small due to PoS Consensus Strategy, need more empirical data for actual usage.
Cosmos	Public Permiss -ionless	Bonded PoS	Tendermint (PBFT)	1-8s	Instant finality after each block	up to a few k	Estimates known once Cosmos is more adopted and running in standard conditions.
Cardano	Public Permiss -ionless	PoS	Ouroboros (BFT)	20s	2mins	1k	Low energy consumption
Iota	Public Permiss -ionless	CCurl PoW	HoneyBadger (BFT)	7s	Node dependant	10k	Low energy consumption

Source: JRC constructed table 2022, from the following sources; (Foundation, 2022c, Foundation, 2022a, Foundation, 2022b, Polkadot, 2022, Cosmos, 2022, Cardano, 2022, Services, 2022, Iota, 2022)

2.6 Platforms with ZKP and SSI Framework Integration

As the interest and development in SSI frameworks rapidly increase and evolve to different subjects, some platforms are closer to being production-ready (currently still no production-ready platform for SSI). Once platforms that have implemented SSI frameworks are production-ready, there will be a plethora of new use-cases and applications throughout all sectors, not only transport.

2.6.1 The EBSI

In 2018, a collaboration started between all the EU Member States, Lichtenstein, Norway, and the European Commission called the European BC Partnership (EBP) to harness the benefits that BC could bring to the EU economy and citizens. This collaboration manifested in the creation of the *"EBSI with the mandate to leverage BC to the creation of cross-border services for public administrations and their ecosystems to verify the information and make services trustworthy"* (EBSI, 2017).

The EBSI is an EU-wide BC infrastructure with nodes deployed across Europe, guided by the public sector with EU regulations and values at the centre of the development process, aimed towards specific use-cases.

2.6.1.1 Platform Architecture

The EBSI Architecture enables verification of the authenticity of data cost-efficiently while increasing security and trust, helping public administrators protect against fraud. They allow businesses to connect with governmental bodies with ease and reduce administrative costs for regulatory compliance. In addition, it enables EU citizens to control one's data securely while facilitating credential and data portability cross-border over the EU. The EBSI has been built using pluggable BC protocols, for the moment, with a choice between Hyperledger Fabric and Hyperledger Besu, with Cross Ledger Integration on the roadmap for future releases. The EBSI infrastructure *"uses smart contracts to ensure that data sent through Application Programming Interfaces (APIs) are correctly recorded in a trustworthy way"* (EBSI, 2021a) and enables three types of off-chain storage: distributed, private, and external storage.

The European SSI Framework (ESSIF) enables *"citizens to create, control and utilise their own digital identity"* (EBSI, 2021a) while not being required to rely on a single, centralised authority. It will facilitate and enable many use-cases that rely on the ease of identification, authentication, and other identity-related data. ESSIF is being implemented as a generic and interoperable SSI framework which is *"part of a broader ecosystem and will interact with other platforms and systems of public and private organisations"* (EBSI, 2021a). Enabling many different types of entities to digitally interact with ease, not only public and private entities but also will allow for efficient and easy interactions between citizens and public administrations (or private entities) across all the EU Member States.

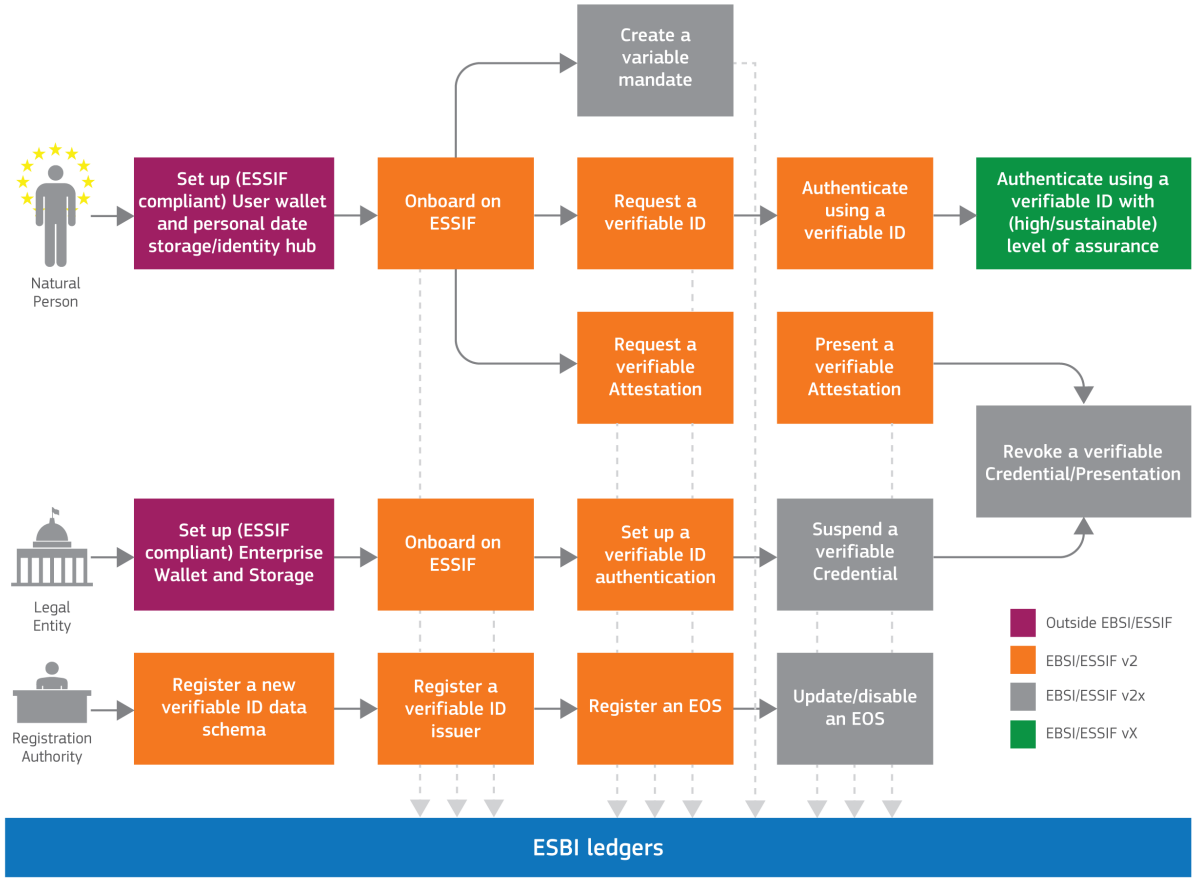
EBSI and ESSIF are being implemented to be compliant with regulations like GDPR and aligned with eIDAS, *"to improve its effectiveness, extend its benefits to the private sector, and promote trusted digital identities for all Europeans, and create a secure and interoperable European Digital Identity which gives citizens control"* (EBSI, 2021b).

The key objective is to create and define standards for a ESSIF and implement the required functionalities situated on the EBSI infrastructure. The identities of legal entities or natural persons need not only include identification and authentication information but could be associated with other data, for instance, commercial or social relationships, permissions (like driving licences, etc.), diplomas, rights to access a service, and so on.

Definitions of the standards for ESSIF need also include:

- an ESSIF Governance Framework.
- *"Specifications and guidelines for the technological components of ESSIF, such as the EBSI wallet"* (EBSI, 2021a), APIs to access diverse services, and other such technological components required.
- Reference implementations for various use-cases along with creating the core services to enable those applications.
- Enabling the interaction with other SSI ecosystems and platforms for interoperability.

Figure 11: European SSI Framework



Source: JRC 2022 adapted from EBSI website (EBSI, 2022b).

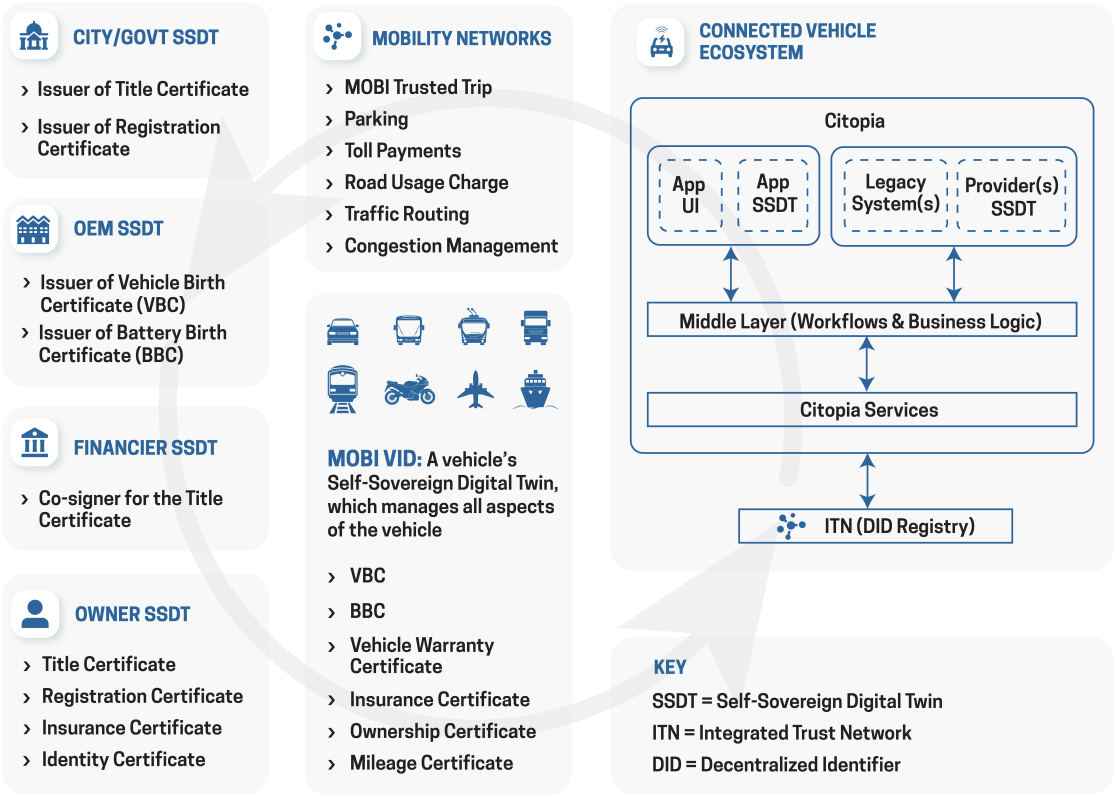
2.6.2 MOBI

"Mobility Open BC Initiative (MOBI) is a global nonprofit smart mobility consortium. MOBI and its members are creating BC-based standards to identify vehicles, people, businesses, and MOBI Trusted Trip" (MOBI, 2022a) to make transportation more efficient, equitable, decentralised, and sustainable. MOBI officially launched in May 2018 and released its first standard, Vehicle Identity (MOBI VID), which leverages the internationally accepted vehicle identification number (VIN) standard and the W3C Decentralised Identifier (DID) standard to define a vehicle's Self-Sovereign Digital Twin (SSDT), the following year. Since its launch, MOBI has formed ten working groups, released 14 standards, and launched several initiatives surrounding the MOBI Web3 Technology Stack (MTS). As detailed in MOBI's Whitepaper, there are numerous avenues in which BC can support mobility providers and consumers, such as:

- Verified Vehicle Digital Identification and data provenance
- Transparency and increased efficiency of Supply Chain through real-time tracking and planning.
- Automatic payments for vehicles and autonomous machines.
- Platforms for mobility commerce that are secure.
- Aid in advancing the sharing economy, namely with car and ride hailing.
- Mobility data markets for both human and autonomous driving.
- Usage based pricing of mobility, such as for insurance, vehicle payments, pollution, energy use, congestion, and infrastructure tolling.

Organisations wishing to participate in MOBI can inquire about joining the community on the MOBI website, or if an organisation wishes to participate in any of the MOBI pilots (MOBI, 2022b).

Figure 12: MOBI VID: A vehicle's Self-Sovereign Digital Twin, managing all aspects and lifetime events of the vehicle

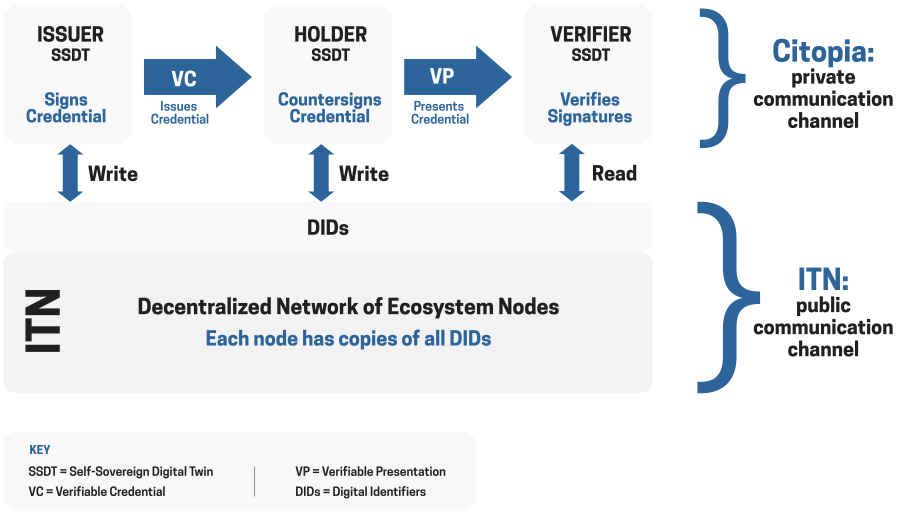


Source: MOBI 2022

2.6.2.1 Platform Architecture

MOBI launched two Web3 infrastructure initiatives to test and scale MOBI standards: the Integrated Trust Network (ITN) and Citopia. Together with the MOBI consortium, the digital infrastructures form the MTS.

Figure 13: MOBI Web3 Digital Infrastructure leveraging Zero-Knowledge Proofs and W3C Verifiable Credential Standard



Source: MOBI 2022

Made up of three layers, the MTS comprises the foundational technologies needed to verify decentralised transactions between connected entities.

1. *"The Foundational Layer, the MOBI consortium, creates standards to identify connected entities and shared business processes."* (MOBI, 2022c) The MOBI consortium is composed of the world's largest vehicle manufacturers, along with startups, NGOs, transit agencies, insurers, toll road providers, smart city leaders, and technology companies.

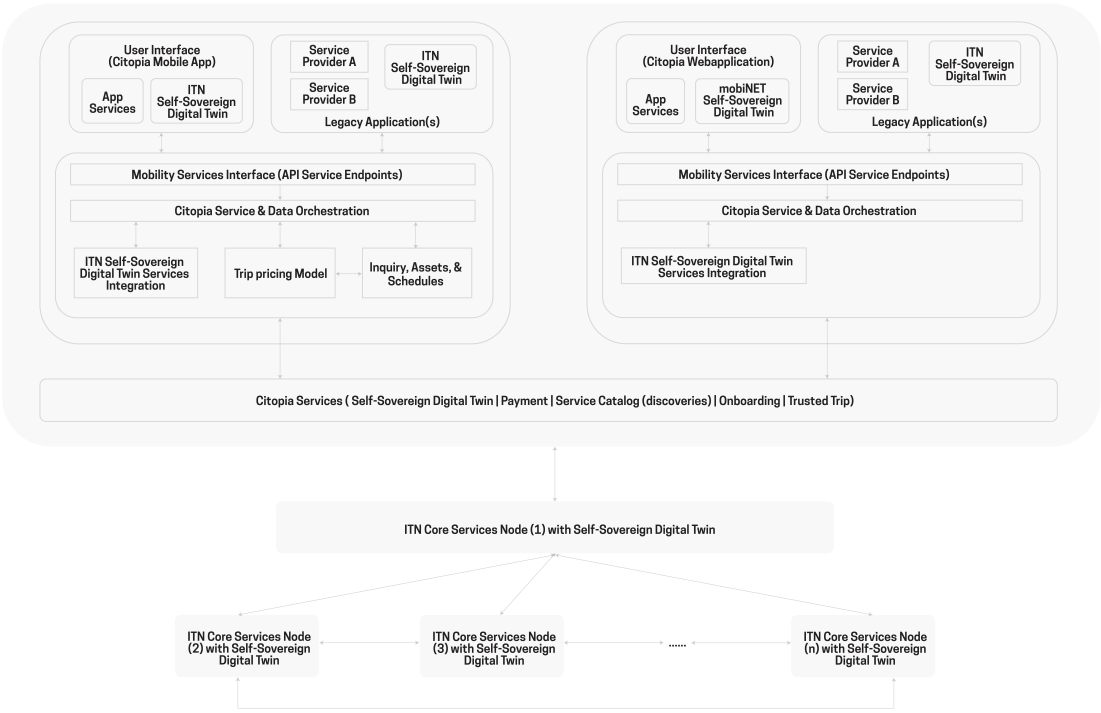
2. *"The Middle Layer, the ITN (formerly mobiNET), is a protocol-agnostic digital infrastructure to provide trusted identity services. The goal is to unlock monetisation opportunities across countless mobility services by allowing application interoperability and multiparty data sharing, enabling participants to execute trusted decentralised transactions at the edge."* (MOBI, 2022c)

3. *"The Top Layer, Citopia, is a trust-less decentralised marketplace to onboard SSDTs and enable VC issuance for business automation using Zero-Knowledge (ZK) Proofs; monetising assets such as infrastructure, services, and data. Citopia enables countless track and trace use-cases in the supply chain and unlocks marginal cost pricing for numerous mobility-as-a-service transactions, including urban road tolling, meter-free parking, congestion management, usage-based insurance, and many more."* (MOBI, 2022c)

Each layer provides a different architecture and function (separation for decentralization), together forming a holistic approach to Web3 applications for the connected ecosystem.

In early 2021, *"MOBI launched the Distributed Registry for Intelligent Vehicle Ecosystem Sustainability (DRIVES)*

Figure 14: High-Level Pilot Solution Architecture Overview



Source: MOBI (MOBI, 2022c)

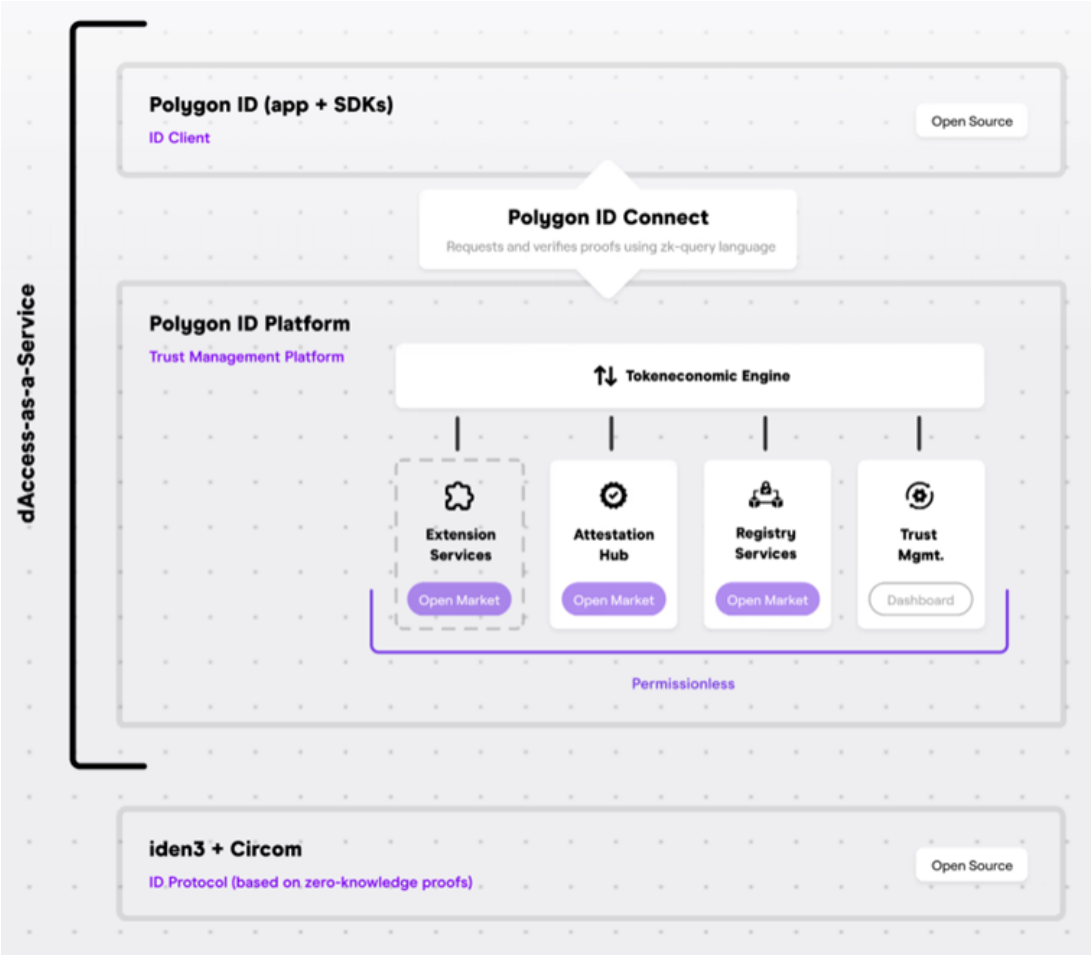
Program to demonstrate" (MOBI, 2021) MOBI standards implementation on Citopia Marketplace connecting to the ITN, and how DIDs enable automate transactions in the connected decentralised ecosystem. Members of the DRIVES Program produced the MOBI Trusted Trip (MTT) standard and published it in October 2021. MTT leverages MOBI VID and other existing standards together with Citopia and the ITN to link the decentralised identifier, or DID, of any entity with its timestamped locations into a verifiable trip to enable *"marginal cost pricing for many new classes of mobility transactions"* (MOBI, 2021). Citopia is the decentralised marketplace that enables users and providers to manage their own MTTs and transactions while retaining data privacy under ZK. MOBI completed its first Trusted Trip demo in October 2021.

Ongoing and future demos and pilots will bring the MOBI Technology Stack to scale and unlock countless opportunities in the connected and decentralised mobility ecosystem. Pilots include Citopia vinTRAK (trusted vehicle track and trace), Citopia partsTRAK (supply chain track and trace for vehicle parts), and Citopia MaaS/Multimodal (seamless multimodal trips track and trace with integrated itinerary planning, ticketing, and payment). The latter was awarded a US Government Transit IDEA seed grant in early 2022.

2.6.3 Polygon ID

Polygon has committed substantial funding to ZKPs, over $1 billion, which is the focal point of their planned development. Polygon ID has one of the first platforms to emerge from the ZK product portfolio (Team, 2022c).

Figure 15: Polgygon ID Architecture



Source: Polygon ID Team, 2022 (Team, 2022c)

Polygon ID contains the proceeding characteristics:

- Decentralised SSI models for identity solutions powered by BC.
- To maximise user privacy, ZKPs are native to the Polygon BC and used by default.
- Decentralised Self-Sovereign Apps are scalable due to the low cost of the Polygon L2 network and are enabled by private on-chain verification.
- Based on current standards and keeping up to date with developments within the SSI and ZK ecosystem.

2.6.3.1 Platform Architecture

Polygon ID is still in the development process, where the end product will be a structured set of tools that form the platform's services and identity solution. Enabling developers to learn, test and integrate with ease, creating

Self-Sovereign dApps, utilising Polygon IDs on-chain identity and privacy functionality.

The product portfolio has been structured in the following way:

— Polygon ID Wallet is built on a set of open-source developer and user kits.

— Polygon ID Platform that can be used to define and manage the trust lifecycle of dApps and the tools they depend upon, such as ZKPs, trust anchors, etc.

— Polygon ID Connect is a public service platform that enables users to integrate their access rights across wallets and applications.

Polygon ID is by default private and enables on-chain verification and permissionless attestation, by making use of the open-source protocol Iden3 (iden3 Team, 2022) and the Circom ZK toolkit (Team, 2022a).

The full release of the Polygon ID Platform and SDKs is expected in Q3 2022.

2.7 Interoperability and Technological Neutral Approach

A fundamental principle which quickly becomes an overarching theme is the aspect of interoperability. Many projects whose aim is to create a platform for particular use-cases opt for an interoperable approach. Instead of just creating solutions on a specific BC such as Ethereum, they do so on many BCs.

This section will closely follow the structure and content laid out by *"A Survey on BC Interoperability"* (Belchior et al., 2020), which reviewed 404 documents on the topic of interoperability and categorised the interoperability approaches into *Public Connectors*, *BC of BCs*.

2.7.1 Public Connectors

The public connectors category identifies and defines different chain interoperability strategies across public BCs, this includes notary schemes, hash time-lock contracts and sidechains/relays (Buterin, 2016).

2.7.1.1 Notary Schemes

When an entity or a group of parties agree to perform a transaction on a BC after an event occurs on another BC or a centralised platform.

The most common implementations of notary schemes are Centralised Exchanges (CEXs) and DEXs. An example of an on-chain transaction initiated by the notary in the case of a CEX would be when a user performing a trade between two tokens then initiates a withdrawal. The trade and withdrawal request happens on the CEXs platform, which holds the private keys associated with the users' CEX wallets; once it has verified the requests, it sequentially performs the on-chain transaction from the associated CEX wallet to the users' personal wallet in which they hold the private keys.

For DEXs, the most familiar example is the Uniswap platform, with frequent forks of it to occur. There is no trusted centralised party in a DEX, as the user can initiate trades using a protocol that provides the trade matching engine and remains in control of the funds associated with their private key by utilising smart contracts and price oracles to perform the trade between two tokens. The provided liquidity for a set of tokens is locked into liquidity pools, contrary to the contemporary method of an order book encountered in CEXs and other types of DEXs. Currently, Uniswap supports Ethereum Request for Comment-20 (ERC-20) to ERC-20 trades and has recently included other BC networks and layer two solutions that are supported by their platform; such as Polygon, Optimism and Arbitrum.

The Interledger project (Int,) initially used an advanced form of a notary scheme utilising a Byzantine-fault-tolerant consensus algorithm to achieve consensus among a set of notaries to validate that a certain event took place, with a multi-signature being used to perform the payments. Interledger's more recent protocol implementations, though, are now based on hash-locking.

2.7.1.2 Sidechains and Relays

A system linked to one BC that can read, validate or communicate events and states to another BC.

A sidechain is a common way used to scale BCs (e.g. projects like Polkadot (Pol, c), Cosmos [(Cos, b) and sharding with ETH 2.0 (Kokoris-Kogias et al., 2018) when it is deployed) and interoperate. The main BC is linked to a separate BC through a communication protocol (Garoffolo et al., 2020), although you could have two dominant BCs, which are sidechains or each other.

An example of a mechanism used to interact with a sidechain is the two-way-peg utilised to transfer digital assets between the sidechain and main BC. The transfer of tokens between BCs mandates that a user's first step is to lock the tokens on the mainchain for initiating a transfer to a contract. The same number of tokens are then minted and released on the sidechain and sent to the wallet specified by the user who initiated the transfer. After the users have performed the actions on the sidechain, they can send back the tokens to the mainchain, where, depending on the implementation, a smart contract will lock or destroy the tokens minted on the sidechain before releasing the locked tokens on the mainchain (Kiayias and Zindros, 2019,Singh et al., 2020).

Relays keep track of block-headers on the mainchain and input them into a smart contract on the sidechain, utilising the consensus algorithm from the mainchain it will then perform the verification procedure. PoW would require proof that a greater amount of work had been performed to create the given header than any other header. For BFT consensus algorithms, it would be checking that two-thirds of the validators' signatures have been used to sign the block header in question.

Once the relayer has verified that the block header has been finalised, the relay can verify any desired transaction or state separately by verifying a single branch of the Merckle tree against the block header.

2.7.1.3 Hash Time-locked Contracts:

Operations between two parties on different chains where on party commits to performing a transaction within a certain time period by providing a cryptographic proof before the timeout.

Hash Time-locked Contracts (HTLCs) normally follow a similar method and are used to perform atomic cross-chain operations, often between BCs that are dissimilar in nature. An example of digital asset exchange between two BCs is as follows:

1. Alice creates a secret S using a salt (random data input) and proceeds to hash the secret, $\mathcal{H}ash(S) = \mathcal{H}_S$. Alice then communicates $\mathcal{H}_S$ to Bob.
2. Alice first locks her digital assets into a smart contract, Bob afterwards locks his assets, once Alice's assets are confirmed as locked. The smart contract contains the following logic:
   (a) Relative to Alice, if the secret is transferred in the time interval of $2N$ seconds, the digital asset will be sent to Bob or else it is transferred back to Alice.
   (b) Relative to Bob, if the legitimate secret S that hashed is $\mathcal{H}ash(S) = \mathcal{H}_S$ is provided within N seconds, the asset will be sent to Alice, or else it is transferred back to Bob.
3. When Alice reveals the secret in the time interval of N seconds, she claims the digital asset from Bob. In doing so the secret S has been revealed to Bob, enabling him to claim the asset from the smart contract.

HTLCs are mostly useful for active operations like atomic swaps and cannot be used for passive operations like cross-chain oracles.

2.7.2 BC of BCs

Frameworks for creating application-specific BCs which have been customised to solve a particular use-case, these BCs can then communicate and interoperate with one another using a communication/messaging protocol, often using a main BC or sometimes called a relay chain that connects these secondary chains and prevents double-spending. These methods include a framework for creating the individual networks, how consensus is achieved, what the incentives are for participants and how the contract layers should be created to share re-usable data. The two networks with the largest market capitalisation are Cosmos and Polkadot, described in detail in the previous section.

While Polkadot is able to interoperate with instances of the same BC engine plus two or more heterogenous BCs, Cosmos can only interoperate with instances of the same BC engines and up to two heterogeneous BCs (Belchior et al., 2020) means that the most interesting BC of BCs (BoBs) network for interoperability purposes is currently PolkaDot. The Market Capitalisation reflects the fact as Polkadot and Cosmos hold the 11^{th} and 25^{th} rank among the Public Networks, respectively, at the time of publishing this report.

2.7.3 Hybrid Connectors

Another method for interoperability between different BCs is to abstract away the BC layer by providing a set of modular operations that enable a dApp to communicate with different BCs for specific use-cases without requiring many diverse APIs.

2.7.3.1 Trusted Relays

Trusted Third Parties (TTPs) can be used to divert transactions from one BC to another, enabling specific tasks to be performed for a certain application on a BC that is best suited for a specific task within a dApp. A registry of BCs aids in the detections of the intended BC, with the various APIs governed by the Trusted Relay with modular consensus performed cross-chain.

Hyperledger Cactus (HLC):

HLC's aim is to remove fragmentation of BC architectures and allow for a system of connected heterogeneous BCs. Cross-chain transactions are validated by a Cactus consortium that runs a group of validator nodes for each connected BC which acts as an interoperability validator network which performs the proofs of the state of the connected ledgers. These groups of interoperability validators agree on the state of the BC in question via a consensus algorithm, where each proof of the current BC state is performed and signed by multiple validator nodes (Hyp, 2022). These Cactus validator nodes (performing the proofs for interoperation's) are very similar to TTP intermediaries or the notary schemes which require intermediaries to retrieve the current state of a BC and send this information to another BC. In contrast the previously described relay method in which the state of one BC can be sent directly to another via read, write or event listening functions directly (like with Polkadots Relay Chain) rather than requiring any TTP intermediaries (Belchior et al., 2020).

At present, Hyperledger implementations (Fabric, Besu, etc.), Corda, and Quorum are supported by HPC, aiming to support public BCs and BC migration functionalities in the future (Belchior et al., 2020, Hyp, 2022).

2.7.3.2 BC-Agnostic Protocols

Cross-chain dApps that function over various heterogenous BCs can be implemented via a BC abstraction layer, where a system chooses the BC a transaction should belong to (can be on an individual node basis) such that consensus is reached on the BC that the functions of a dApp need to be performed on (depending on security, privacy, scalability requirements of that function). These solutions facilitate BoBs, although business logic is commonly more confined.

2.7.3.3 BC Migrators

The state of one BC can be migrated to another using BC migrators. Presently only data migrations have been performed, but it is expected that migrating smart contracts will also be achieved in the future (Hyp, 2022). *Fynn et al* (Fynn et al., 2020) demonstrate a BC migrator tested on Ethereum and Hyperledger Burrow.

2.7.4 Interoperability Use-cases

Portable assets:

The ability to move tokens from one ledger to another with trust minimised and 1-to-1 backing. For example, it could be a hypothetical Government issued coin that can be transferred to another chain to be used as collateral for trading, with the option to move back to the Governmental ledger if desired.

Atomic Swaps:

Enables the digital assets exchange (or a bundle of assets) from one user to another who are on different chains in a way which guarantees that either both transactions occur or neither do, in a secured way.

Cross-chain Oracles:

An action is performed on a BC when an oracle sends proof that an event occurred, a condition is fulfilled on (for example, an address is connected to a unique identity) another BC. In such a situation, the BC being read does not change state over the operation.

Asset Encumbrance:

Perform a conditional lock of digital assets on a BC which can only be unlocked when certain conditions on another BC are met. The applications could in principle be wide ranging: related to activities pertaining to financial services and products, court orders, among many others.

General Cross-chain Contract:

Is an agreement in the form of a smart contract between two BCs, or a smart contract that stands by until an event occurs on another BC before triggering a function. Applications are numerous and varied, one such example could be for dividend payments on one BC for entities that hold digital security on another BC that is more tailored towards securities and regulations.

3 Overview of the Relevant Regulatory Frameworks

In the previous section, knowledge of the key technological components required to understand the pilot studies performed in this Science for Policy Report were introduced.

This Section details the relevant parts of regulations and directives that either affect the implementation paths of the use-cases or where technical components of the solutions investigated can help enable the implementation of these regulations and directives.

3.1 ICT Regulatory Framework Relevant in General to BCs and Data Sharing.

A major concern of many EU citizens when it comes to applying BC-based identity systems is that their privacy, security, and control of one's data would be threatened. Data privacy and Identity of EU citizens are enshrined in the General Data Protection Regulation (GDPR), eIDAS and the ePrivacy Directive. Any vehicle and user identity solutions for transport applications need to account for these regulations and even enable them by providing increased data protection compared to centralised systems. There is a current proposal to amend eIDAS to include a European Digital Identity and mentions the use of SSI and tamper-proof solutions. The ePrivacy Directive, which was put into force in 2002, has been under review since 2017, with the most recent proposed draft from November 2021.

3.1.1 General Data Protection Regulation

The GDPR 2016/679 (EC, 2008) published on the 27th of April 2016 and enacted in May 2018 is a fundamental law for the data protection and privacy of EU citizens. It encompasses EU principles and rights, enabling the protection of personal data and the free flow of non-personal data. The key relevant components of GDPR for the application of BC for transport use-cases are described as follows:

- **Security of Processing of Personal Data:** The controller and processor of personal data in a system must have appropriate protective measures, both technical and organisational, against security threats to the system. That could put at risk, *"the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed"* (EC, 2008).
- **Data Protection by design and by default:** Data Protection practises are required to be considered by the controller in the design phase of the system in question, which contains or processes personal data and is implemented during the production phase of said system. These Data Protection principles include but are not limited to data minimisation and pseudonymisation. In addition, measures need to be in place by the data controller that only personal data are processed solely for the intended purpose, including both the quantity and the length of time that the data are stored.
- **Conditions for Consent:** The data controller must be able to provide evidence that a data subject has provided their consent to process their personal data. *"The data subject has the right to revoke the consent given at any time"* and with ease (EC, 2008).
- **Right to erasure ('right to be forgotten'):** The data subject has the right to instruct the data controller to erase their personal data from the system in question either because the person's data are no longer necessary or simply because the data subject has now decided to withdraw consent. The data controller must act to erase or modify the data without undue delay. Where the data subject may request their personal data be modified to reflect changes that may have occurred.
- **Rights of access by the data subject:** The data subject has the right to have confirmation as to whether a system processes their personal data, obtain their personal data that are processed by the said system, including information on what the purpose for processing is, types of personal data used, where the data have been processed and for how long they were held, and who else has had access to these data. This information shall be easily provided to the data subject, although the controller may charge a reasonable administrative fee.
- **Data portability:** The data subject has the right to request and receive their personal data that have been held and processed by a system in a structured and common machine-readable format. In addition, the data subject should be able to transfer said personal data to another data controller without any obstruction or hindrance.
- **Responsibility of the controller:** It is the data controller's obligation to implement sufficient organisational and technical structures *"to ensure that the processing of personal data is"* adherent to GDPR (EC,

2008), with the nature, scope, context, and purpose of the data processed into account in relation to the risks and their severity of a breach for the freedom and rights of the data subject.

— **Application:** The application of GDPR applies to open systems connected to the internet and closed systems, which are not linked to a local area network or the internet. There are certain activities that do not fall under the GDPR, such as:

  - For law enforcement authorities that function to prosecute criminals.
  - Activities based outside of the EU, that do not interact within the EU.
  - Personal actives of an individual, such as for household activities.

— **Data retention:** The GDPR states that the length of time for which personal data of a subject is held does not exceed its intended purpose, where depending on the said purpose and the context for which the data subject has given permission, it may vary in different contexts.

3.1.2 ePrivacy Directive

The ePrivacy Directive 2002/58/EC (EC, 2002) was first put into force in July 2002, with proposed draft amendments to the regulation starting from 2017, with the most recent draft version from November 2021. The ePrivacy Directive provides a clarification on the requirements for electronic communications, such as data exchange and user consent, enforcing privacy for communications and metadata, more effective enforcement of confidentiality rules and application of the rules to new players.

The key relevant components of ePrivacy Directive for the application of BC for transport use-cases are described as follows:

— **Security of processing:** The service provider must perform an appropriate level of organisational and technical measures to safeguard the security of its services, in relation to considerations of the severity of the risk presented and the cost of implementation in regard to the state of the art.

— **Limitation of processed data and consent:** Only in select situation may a service provider may process digital communication information and only for certain types of content. In addition, the data subject must have provided their permission to use this data. Once consent has been provided, it may be withdrawn by the data subject at any point in time.

— **Traffic data:** A subscriber or users' data and metadata processed and stored by a service provider need to be anonymised or erased once it is not required for the purpose of transmitting a communication and in addition to all requirements and restrictions stated in the GDPR must be adhered to.

— **Confidentiality of the communications:** Through national legislation, Member States are required to ensure the confidentiality of communications and their related metadata. This is to prohibit listening, tapping, storage or any kind of communication surveillance or interception by third parties of the user's communication and related metadata without the consent of the user unless when legally authorised to do so.

3.1.3 eIDAS

The eIDAS Regulation No 910/2014 (EC, 2014b) published on the 23^{rd} of July 2014 aims to increase "trust in electronic transactions" within the single market by creating a common framework for secure electronic interactions between public authorities, businesses, and citizens to increase the efficiency of private and public services online. The Regulation includes the requirements that an advanced electronic signature needs to satisfy.

The Commission communication 'A Digital Agenda for Europe' of the 26^{th} of August 2010 outline the issues with fragmentation in the EU digital market pointing out issues relating to interoperability and the rise of cybercrime creating major frictions to the success of the EU digital economy. In the report 'Dismantling the obstacles to EU citizens' rights' of 2010 the Commission noted the importance of solving the main issues obstructing EU citizens from benefiting from an EU digital single market with cross-border digital services (EC, 2014b).

The eIDAS Regulation was created to support:

— Accelerated advances in vital *"areas of the digital economy and push for a completely integrated digital single market"* (EC, 2014b) by enabling cross-border applications of digital services, with a special focus on expediting secure electronic identification and authentication.

— Strengthening the EU digital single market by generating suitable circumstances for bilateral acknowledgement of the essential facilitators of cross-border interactions, *"such as electronic identification, electronic documents. electronic signature and electronic delivery services, and for interoperable e-government services"* throughout the EU for all its citizens (EC, 2014b).

— Emphasising the priority of the security of electronic services, notably electronic signatures, and the requirement for the establishment of public key infrastructure at the pan-European level. The Commission is *"called on the set up a European validation authorities gateway to guarantee the cross-border interoperability of e-signatures and to boost the security of transactions"* (EC, 2014b) performed over the internet.

These aspects of the eIDAS regulation with help combat key issues, such as citizens are often unable to use their electronic identification to authenticate their identity in another Member State due to the fact that the national electronic identification method in their country of origin is not recognised and interoperable in other Member states (EC, 2014b). This creates an obstacle that prevents service providers from realising the benefits that the EU internal market could provide. Interoperable and *"mutually recognised electronic identification will enable cross-border services in the internal market"* (EC, 2014b), allowing for businesses to operate with ease cross-border without the expensive and sometimes too costly barrier of interacting with many public authorities with completely different standards and requirements.

eIDAS is a manifestation of the European Commission's focus on Europe's Digital Agenda (EC, 2021b) enacted to trigger digital growth within the EU by enabling interoperability. The Member States must adhere to a common framework and defined standards such that eIDs from the other Member States can be recognised without jeopardising security or the false validation of an eIDs authenticity.

The requirements that an advanced electronic signature need to adhere to are as follows:

1. it is unique to the signatory,
2. and can identify the signatory accurately,
3. the data that the subjects' electronic signature is linked to, when tampered with, is easily detectable.

All Member States must accept an electronic time stamp issued in a Member State following EU standards. In essence, where the time stamp meets the requirement that it links the data and time in a way in which the data is resistant to tampering without detection and is signed using an advanced electronic signature or equivalent method, such that the integrity and accuracy or the time of the stamp is not in question.

Regulation (EU) 910/2014 (eIDAS) is the only framework for trusted cross-border electronic identification (eID) of a natural person. Following its enactment in 2014, it was based on the nation eID systems that are conditional to diverse standards and only facilitate the electronic identification needs of a small segment of EU citizens and businesses.

3.1.4 European Digital Identity Proposal to amend Regulation (EU) 910/2014

The COVID-19 pandemic has had a dramatic effect on the rate of digitalisation, which has led to both the public and private sectors conforming to digital services. Nowadays, it becomes an expectation of EU citizens and businesses that activities such as enrolling at a foreign university, tax declarations, banking, car rental, loans and insurances, authentication over the internet for payments or services, and more should all be digital and with a high level of assurance of security, privacy and with convenience for the user.

The increased rate of digitalisation from the COVID-19 pandemic has created the demand for means to authenticate and identify online, including the need to exchange information relating to one's identity digitally: certificates, attributes and qualifications one holds (could include ID number, residence address, age, qualifications, driving licence and other permits or payment information). The need to authenticate and identify online has sparked off a new paradigm, with the adoption of *"advanced and convenient solutions that can integrate different verifiable data and certificates of the user"* (EC, 2021). *"Users expect a self-determined environment where various credentials and attributes can be carried and shared, such as your national eID, professional certificates, and public transport passes. These are so-called self-sovereign app-based wallets managed through the mobile device of the user allowing for secure and easy access to different services, both public and private, under their full control"* (EC, 2021).

The use of more advanced solutions such as SSI is supported by a proposal for a regulation seeking the amendment of Regulation (EU) 910/2014 on June 2021 as regards to establishing a framework for a European Digital Identity (EC, 2021). The proposal to amend eIDAS aims the provision for cross-border use of:

— *"access to highly secure and trustworthy electronic identity solutions,"*

— *"that public and private services can rely on trusted and secure digital identity solutions,"*

— *"that natural and legal persons are empowered to use digital identity solutions,"*

— *"that these solutions are linked to a variety of attributes and allow for the targeted sharing of identity data limited to the needs of the specific service requested"* (EC, 2021).

A new environment has emerged where attention is directed to the provisioning of trust attributes associated with an identity. Attempting to facilitate the authentication and identification of users with a high level of assurance while putting the users in control of their own data and identity in a user-friendly interface. In addition, the European Digital Identity Framework provides EU residents with control over who has access to their digital twin, to exactly which data may be shared and for how long. A high-level of security assurance is required w.r.t. the *"digital identity provisioning, including the issuance of a European Digital Identity Wallet and infrastructure for the collection storage and disclosure of digital identity data"* (EC, 2021).

In the conclusions of the European Council of October 2017, there was a call for an EU wide framework for secure public identification and interoperable digital signatures to enable EU residents to have control over their online identity and the data associated with it. This will also provide for *"access to public, private and cross-border digital services"* (EC, 2021). In addition, the EC communication "2030 Digital Compass: The European Was for the Digital Decade" of March 2021 appointed the aim by 2030 to have an EU framework for the *"deployment of a trusted, user-controlled identity, allowing each user to control their own online interactions and presence"* (EC, 2021). The European Digital Identity Proposal echoes the need for a more harmonized approach to digital identification to that of divergent national methods and the vitality this will give to the EU digital Market by enabling citizens, businesses, and public services to identify online conveniently and uniformly while facilitating data subjects control over what personal data is shared and when. All EU citizens should benefit from secure access to public and private services provisioned by an ecosystem at the EU level that enables trust between participants relying *"on verified proofs of identity and attestations of attributes"* (EC, 2021) and verifiable claims. The reliability of digital identity solutions will support competition within the EU, by benefiting *"from a harmonized European approach to trust, security and interoperability"* (EC, 2021).

It is, therefore, necessary to additionally lay out the conditions to be included in a harmonised framework for European Digital Identity Wallets:

— Enable users to access a large scope of cross-border private and public services through electronic identification and authentication, both online and offline.

— May aid the institutional needs of public bodies, administration, international organisations, and agencies.

— Benefit from the potential delivered by tamper-proof solutions to provide a high level of assurance.

— Grant users the ability to *"create and use qualified electronic signatures and seals, interoperable accepted across the EU"* (EC, 2021).

— When adopted or issued by the Member States, use a common standard to allow seamless interoperability and a high level of security.

— Permit the issuance and handling of trustworthy digital attributes and support the decline in administrative strain, enabling citizens to use the verifiable credentials and claims in their private and public interactions. For example, EU citizens should be capable of proofing digitally, ownership of a valid driving licence issued by a Member State Vehicle Registration Authority, *"which can be verified and relied upon by the authorities in the other Member States"* (EC, 2021).

— *"Qualified electronic ledgers record data in a manner that ensures the uniqueness, authenticity, and correct sequencing of data entries in a tamper-proof manner. An electronic ledger combines the effect of time stamping of data with certainty about the data originator similar to e-signing and has the additional benefit of enabling more decentralised governance models that are suitable for multi-party co-operations. For example, it creates a reliable audit trail for the provenance of commodities in cross border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative*

public services. To prevent fragmentation of the internal market, it is important to define a pan-European legal framework that allows for the cross-border recognition of trust services for the recording of data in electronic ledgers" (EC, 2021).

— *"The certification as qualified trust service providers should provide legal certainty for use-cases that are built on electronic ledgers"* (EC, 2021).

3.2 Regulatory Frameworks Specific to the Pilots Use-Cases Explored

3.2.1 Regulatory background, in use fuel consumption monitoring

Regulation (EU) 2018/1832 (EC, 2018) of November 2018 decreed, starting from January 2021, On-board Fuel and/or Energy Consumption Monitoring Devices (OBFCM devices) as compulsory devices in all newly produced commercial and light passenger vehicles sold in the EU. Where the Regulation defines an OBFCM device as *"any design element, either software and/or hardware, which senses and uses the vehicle, engine, fuel and/or electric energy parameters"* (EC, 2018).

The ensuing Regulation (EU) 2019/631 of April 2019 *"setting CO_2 emission performance standards for new passenger cars and for new light commercial vehicles"* (EC, 2019h), further detailed that the EC is required to store a record of the data reported by the Member States under Article 7. In addition, Article 12 details which parameters need to be shared from OBFCM devices with the EC, starting from the 1^{st} of January 2021; these include the Vehicle Identification Number (VIN) or any other parameters required to ensure the obligation of the EC to *"monitor and assess the real-world representativeness of CO_2 emissions and fuel or energy consumption values determined pursuant to Regulation (EC) No 715/2007"* (EC, 2019i). In practice the parameters required to monitor CO_2 emissions and fuel/energy consumption are as follows.

For a **conventional internal combustion engine** vehicle:

— Total Distance Travelled (Lifetime)

— Total Fuel Consumed (Lifetime)

And for a **hybrid vehicle** the additional data required by the regulation to be reported are as follows:

— Total Distance Travelled (Lifetime)

— Total Fuel Consumed (Lifetime)

— Total distance travelled in charge depleting operation with engine off (Lifetime)

— Total distance travelled in charge depleting operation with engine running (Lifetime)

— Total distance travelled in driver-selectable increasing operation (Lifetime)

— Total fuel consumed in charge depleting operation (Lifetime)

— Total fuel consumed in driver-selectable charge increasing operation (Lifetime)

— Total grid energy consumed in charge depleting operation with the engine off (Lifetime)

— Total grid energy consumed in charge depleting operation with the engine running (Lifetime)

The lifetime values are stored within light and heavy-duty vehicles. The need for regular monitoring of the fleet's real-world fuel consumption is introduced in Regulation (EU) 2019/631 (EC, 2019h) and Regulation (EU) 2019/1242 (EC, 2019g). These regulations also state that the EC has the obligation to process the collected data and create aggregated, anonymised datasets on an annual basis. The pseudonymised datasets collected on a per manufacturer or Member State basis shall be published annually to verify the representativeness of real-world CO_2 emissions. Regulation (EU) 2019/631 (EC, 2019h) stated the three modes of possible data collection, consisting of data derived from: manufacturers, national authorities or directly transferred from the vehicles themselves.

Regulation (EU) 2021/392 (EC, 2021a) put into legislation an obligation for the Member States and manufacturers to compile data from OBFCM devices and transmit it once a year to the EC via data exchange platforms provisioned by the European Environmental Agency (EEA). Currently although the Regulation (EU) 2019/631 (EC, 2019h) stated three modes in which the data can be collected, in practice only two are used, either from manufacturers when a vehicle owner has agreed to share their data or via national authorities who

gather vehicle data during the Periodic Technical Inspection (PTI), which is does not occur regular enough as the legislation requires this data each year, and could be used primarily for validation purposes rather than annual monitoring.

A JRC report (Commission et al., 2022) focuses on the direct transfer from vehicles to the EC, without any intermediating entities linked to the vehicles' lifecycle. Such an approach could increase the levels of privacy by decoupling the VIN of the data source to the data collected from that source. This is achieved by associating the data collected from the OBFCM device to an Over The Air (OTA) Device ID, such that vehicle data at the VIN level is held physically separate from vehicles identifiers such as the VIN. Where the OTA Device communicates with servers held by the EC. The present report extends on such a solution with the addition of further privacy preserving tools, such as use of SSI Frameworks where the vehicle generates its own DID, with the Verifiable Credentials issued by the Member State Vehicle Registration Authority that already holds all the relevant information of the vehicle, such as who it is registered to, what the VIN is, etc. and can associate the DID of a vehicle to its VIN and other vehicle registration information held at the Member State level. Once a Verifiable Credential is issued, the vehicle can then periodically transmit its emissions data from the OBFCM device OTA to the EC, increasing both the control of the vehicle owner's data and further increasing levels of privacy and security of the system. In addition, methods and tools are used to enable data provenance and integrity assurances, increasing the security and the trust in the validity of the data collected, including keeping an accurate timestamp of said trusted data.

This collection could constitute a typical example of vehicle-data that need to be communicated on a regular basis to the EU authorities, preserving the privacy, provenance, and integrity of the information. Hence it is considered a characteristic case where BC could offer benefits.

4 BC4T Pilot Studies

In the previous sections, basic technological knowledge was introduced about BC needed to comprehend the BC4T pilots' studies. Key concepts and regulations were also introduced relevant to the explored use-cases due to the sharing of data (GDPR), enforcing privacy principles for metadata and communications (ePrivacy), the use of identity, authentication, and trusted services (eIDAS), as well as the proposal to amend the eIDAS regulation to contain the European Digital Identity and compliant wallets. Tamper-proof solutions and the use of Self-Sovereign Identity and Apps were also indicated.

The project objectives were:

1. To gather know-how on BC technology for the automotive and road transport sectors.
2. To provide a policy-relevant overview of the status in the development and deployment of BC implementations regarding road vehicles.
3. To conceptualise prototypes linked to ongoing JRC policy support activities (i.e. digital identity, vehicle fuel consumption and emissions monitoring) serving as the basis for future research on these topics.
4. To develop computer simulation and analysis tools necessary to test BC systems' applicability and likely performance for the above mentioned and possibly other future implementations.

Given the broadness of the road vehicle sector and the significant number of BC applications appearing, the BC4T project focused on two primary case studies:

1. the application of BC technology for vehicle identity attribution and
2. real-world vehicle CO_2 emissions and energy consumption monitoring

These two indicative first implementations helped guide the realisation of actual pilot implementations and allowed a first stress test of the available BC technology. The three pilots explored within the BC4T project are:

Pilot 1 - SSI Management System: The pilot proposed a solution for a Digital Identity Management Systems (DIMS), forwarding data to either a centralised or decentralised database. Simulation of an EU-based vehicle identity management system based on SSI and MS Vehicle Registration Authorities interacting with the EC. The implementation was performed in collaboration with MOBI, a non-profit consortium focusing on BC for mobility.

The SSI Management System (SSIMS) was considered an ideal candidate for the use-case as it could enable an ecosystem of applications-oriented at the vehicle level. In addition, SSIMSs are important for many future transport applications that will require a digital twin of the: vehicle, user, or even digitalised components of the vehicle itself as the whole is the sum of the parts. For an entity to interact with the digital world, it will require a digital representation (a digital twin or Digital Identity). As stated in the regulation, the essential features of the technology used must have privacy, security, and users in control of their own data and identity at heart.

Pilot 2 - Provenance and integrity of vehicle data: The pilot developed a BC Network architecture built on the Hyperledger Fabric network. Subsequently, the study group simulated a data exchange BC-based monitoring mechanism (vehicle fuel consumption/CO_2 emissions monitoring used as an example), guaranteeing the provenance of emissions data and its integrity for monitoring and other possible purposes; the simulation assumed vehicles interacting with the EC and Member State (MS) Vehicle Registration Authorities. The pilot was deployed by the study team on the JRC Experimental Platform for Internet Contingencies (EPIC) infrastructure.

Additionally to the elevated interest from a regulatory perspective, this use-case was chosen as a typical example of regulated vehicle-to-authorities communication. The example builds on the basis of monitoring of fuel consumption, enabling the communication of onboard fuel consumption monitoring data (OBFCM) and data reporting requirements, but the same principles could be applied to any similar vehicle to public communication, such as confirmation of roadworthiness, emissions compliance, vehicle insurance coverage license plate validation and others. Such data exchanges become of particular interest in the EU where 27 different national authorities need to communicate regarding vehicles that could potentially be registered in one member state but circulate in anyone of the 26 others.

It was also relevant from a demonstrative point of view. As a standard practise, a PoC with a simple identity management system is first done, and then complexity and functionality are added. The BC4T project started

with deploying a simple identity management system that utilises the same certificates as most web services you normally access online, use X.509 certificates, previously described in subsection 2.4.2.1. These can be in conjunction with a private BC network and storing data off-chain to give increased levels of privacy and security. Although the main reason for starting with this use-case was that the vehicle only needs to communicate a maximum of once a month, the TPS needed to successfully implement such a use-case is relatively low when compared to a use-case like traffic monitoring which would require sub-second communication intervals, hence requiring magnitude of order higher TPS.

Pilot 3 - SSI Management System combined with Data provenance and Integrity: This pilot attempted the integration of two BC systems, such as pilots 1 and 2, to achieve interoperability. The integration used OpenID Connect standards for their SSI tool that communicates between Hyperledger Aries and Indy in order to add a more robust identity layer to the Hyperledger Fabric Network of the previous work to enable data provenance and integrity. This activity was performed in collaboration with Informatics and Telematics Institute (ITI), an emerging technology research group within the CERTH.

As with most research and software development, starting with simple scenarios and then adding complexity is a reasonable practice. In this sense, pilot 2 attempted a connection between the BC system developed at the JRC on Hyperledger Fabric in communication with another heterogeneous BC system built on Hyperledger Aries and Indy that deals with the SSI management similar to that of Pilot 1. The endeavour is challenging as Hyperledger has no native way to connect these systems. A gateway was needed to translate the messages communicated between the two systems to understand each other. As the task of developing this gateway could take more time than the duration of the BC4T, it was decided to seek outside collaboration with researchers who had already developed such a gateway, the most relevant found in the literature review was created by a team in ITI, within CERTH.

4.1 Pilot 1, SSI Vehicle Identity Management Pilot

The scope of the pilot was to test the performance of an AWS cluster simulating the performance of the required process flows of the Vehicle Identity Management System, hardware requirements and cost would be for 280 million vehicles. The pilot was purely exploring the performance of the identity management system and did not include the data integrity and provenance system as will be described in subsequent use-cases. A robust Identity Management System, using X.509 Certificates, was built with an SSI framework incorporated by MOBI. The SSI framework used was based on existing standards largely followed, or in the situation where there is yet no clear standard, MOBI implemented their MOBI VID Standard (Vehicle Self-Sovereign Digital Twin), with the ambition to become part of the industry norms. This pilot was developed in collaboration with MOBI.

More information about the infrastructure used to test this pilot can be found in subsection 2.6.2.1.

4.1.1 Hardware and Software Setup

4.1.1.1 Hardware Setup

For this pilot an AWS cloud computing infrastructure was used. The resources used comprised of:

- 75 instances of AWS c6i.xlarge which consists of 4 virtual Central Processing Units (vCPUs) and 8GB Random Access Memory (RAM) for each instance. The 1 million vehicles were split over these 75 instances.
- 1 instance for RDS of an AWS db.m6g.8xlarge consisting of 32 vCPU, 128 GB RAM. This was used for the Issuer of each MS and the EC verifier.

4.1.1.2 Deployment Architecture

- The ITN Core Services and the Fabric DLT were deployed into two separate AWS 3-node EKS clusters with ingress controllers and load balancers
- The Self-Sovereign Digital Twins representing the cars, registration authorities and the EC were deployed again into separate AWS 3-node EKS clusters with ingress controllers and load balancers
- All AWS EKS clusters operated in the same AWS security zone

4.1.1.3 Software Deployment

1. Configuration, containerisation, and deployment of the multi-node (1 order + 3 peers) Fabric DLT version 2.3 into its designated AWS EKS cluster following well documented deployment scripts (see example below)
2. Configuration, containerisation, and deployment of the Core Services with Core Services Self-Sovereign Digital Twin into its designated AWS EKS cluster
3. Configuration, containerisation, and deployment of the three different Self-Sovereign Digital Twins (cars, registration authority, EC) into their designated three separate AWS EKS Clusters Note, that the discovery of the Self-Sovereign Digital Twins, and establishment of communication is based on the API endpoints specified in the DID documents created for each actor (cars, registration authorities, EC). The communication between the various Self-Sovereign Digital Twins as representatives of the cars, registration authorities, EC, and the ITN followed the DIDComm messaging standard.

Note, that the discovery of the Self-Sovereign Digital Twins, and establishment of communication is based on the API endpoints specified in the DID documents created for each actor (cars, registration authorities, EC). The communication between the various Self-Sovereign Digital Twins as representatives of the cars, registration authorities, EC, and the ITN followed the DIDComm messaging standard.

For deployment on Kubernetes the ITN Services Hosts are as follows: the details for which have been quoted from a private Github Repository (to ITN, 2022) (created by MOBI's ITN contributors), which the EC project team has access to.

Deploy Ingress controller

`kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.0.4/deploy/static/provider/aws/deploy.yaml`

Change `deploy/ingres-controller/ingress.deployment.yml` accourding to your cluster settings and run:

`kubectl apply -f ./deploy/ingress-controller`

Create namespace

`kubectl apply -f ./deploy/core-services/itn.namespace.yml`

Deploy Ingress API

You shoud edit `./deploy/core-services/ingress/api.ingress.yaml` before deployment.

If you have a SSL certificate for your domain, you should create a secret for this certificate:

`kubectl create secret tls itn-https -n itn –key ${YOUR_KEY_FILE} –cert ${YOUR_CERT_FILE}`

If you don't have SSL Certificate, remove the `tls` section.

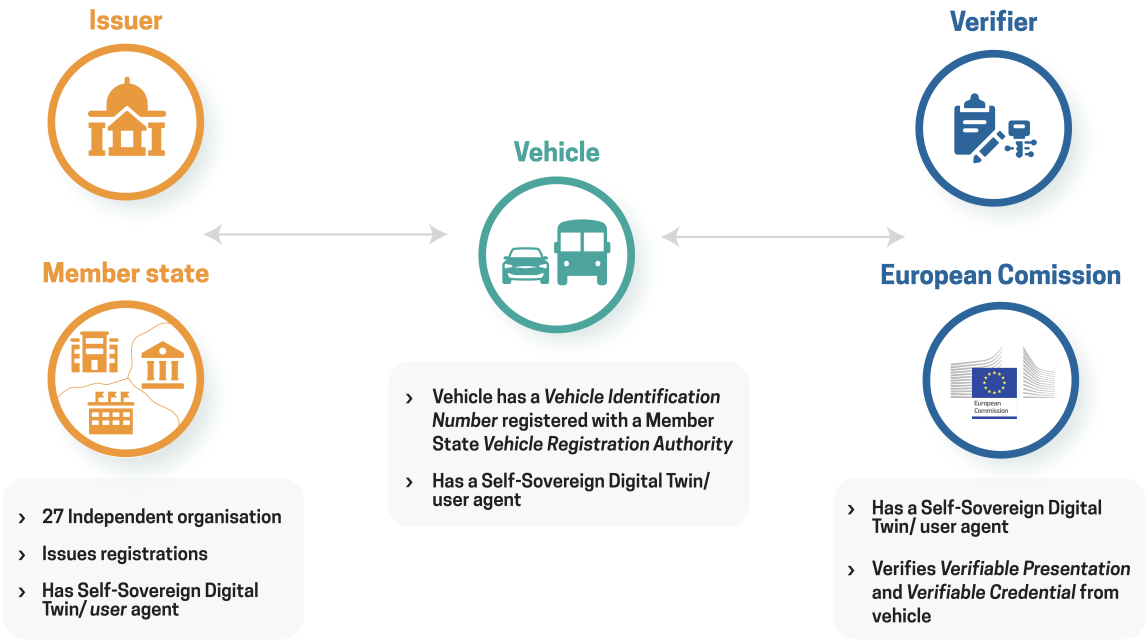
Then you should change the domains inside the `rules` section to your own domains.

NOTE: Two new consortia (MEF Forum and AAIS) have joined MOBI's effort for a trusted IoT identity registry for eCommerce. mobiNET, with new consortia members, has evolved into the Integrated Trust Network (ITN). Organisations and consortia interested in joining the effort can inquire about the ITN on the MOBI website (MOBI, 2022b). The ITN is member-owned and operated.

4.1.2 Experimental Setup

In this pilot, MOBI and the EU Commission tested the performance and scalability of Citopia for transactions (exchange of value, goods, or data) between the EU Commission, 27 Member States' Registration Authorities, and Connected Vehicles using MOBI decentralised identity solutions (ITN DID method). The three process flows required for the Vehicle Identity Management System were tested for performance.

Figure 16: Assumptions



Source: JRC and MOBI, 2022.

The simulation aims to test the use case of vehicle emission self-reporting with SSI infrastructure. Self-Sovereign Digital Twins and Verifiable Credentials are created on Citopia to simulate the interaction of EU Commission, Member State Vehicle Registration Authorities (RAs) and Vehicles. The experiment tests the scalability performance of the EU's 27 states and 280 million vehicles.

The simulation includes three flows:

1. issue vehicle registration credential flow,
2. self-issue vehicle data (such as for example emissions) credential flow,
3. verify data credential flow.

The example use-case of vehicle CO_2 communicating and registering its emissions data was chosen due to the fact that this data need only be transmitted once a year according to regulation, and hence would be a use-case that does not require a very fast network.

The Issue Vehicle registration credential flow simulates vehicles registering themselves with Member State Vehicle Registration Authority and receiving their Verifiable Credentials. Self-issue data flow, for example, in the use CO_2 emissions or fuel consumption, simulates vehicle reporting emission data to EC in Verifiable Credentials. Verify CO_2-emission Credential flow simulates EC verifying the Vehicle Credential and the Reporting Data Credential from the individual Vehicle.

Issue Vehicle Registration Credential flow: A vehicle asks the Member State Vehicle Registration Authority to issue a credential. This flow consists of the following operations:

1. Establishing a secure connection between two entities (Vehicle and RA) on Citopia.
2. Vehicle sends an issue credential request to the RA on Citopia.
3. RA receives issue credential request and asks Vehicle to prove by reading DID information from the ITN.
4. Vehicle receives a "request proof" message from the RA and presents the proof back to the RA on Citopia.
5. The RA receives the proof, verifies it, issues a "Vehicle Credential" credential, and sends it to the Vehicle on Citopia.
6. Vehicle receives the issued credential and stores it in its Self-Sovereign Digital Twin.

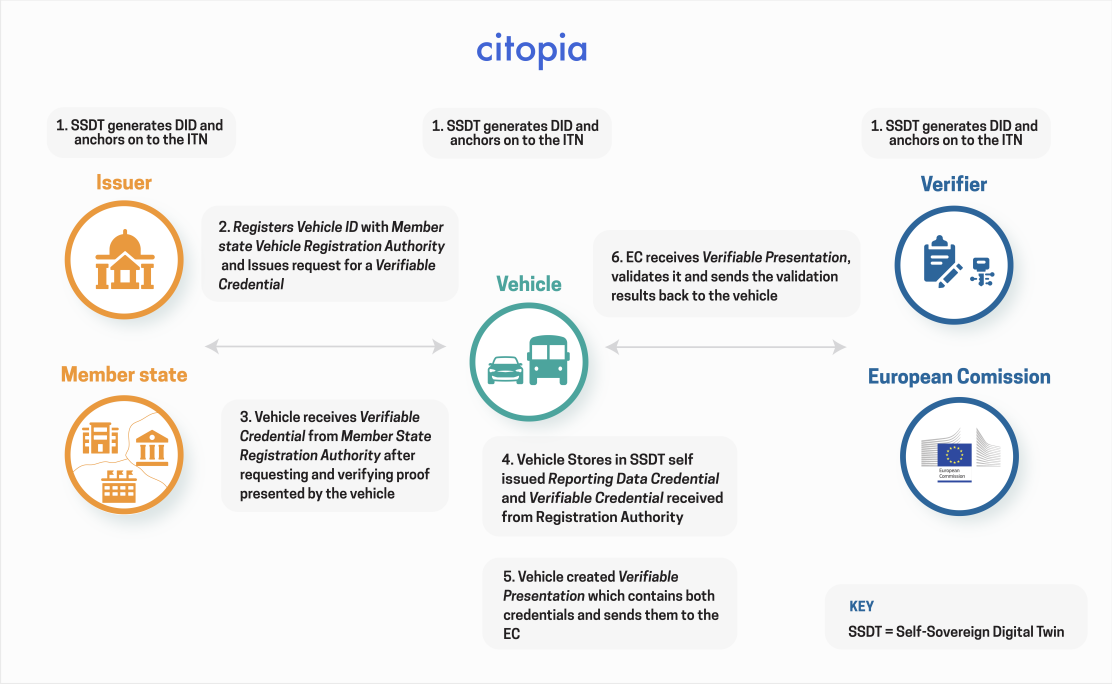
Self-Issue CO_2-emission Credential flow: A vehicle self-issues a CO_2-emission credential. This flow consist of following operations:

— Vehicle self-issues "ReportingDataCredential" and stores it in its Self-Sovereign Digital Twin.

Verify CO_2-emission Credential flow: A vehicle sends two credentials from its Self-Sovereign Digital Twin (SSDT) and sends as a Verifiable Presentation to EC for validation. This flow consists of the following operations:

1. Establishing a secure connection between two parties (Vehicle and EC) on Citopia.
2. Vehicle takes two credentials from its SSDT:
3. "VehicleCredential" issued by the RA.
4. "ReportingDataCredential" self-issued by Vehicle.
5. Vehicle creates a Verifiable Presentation (VP) including both credentials and sends it to the EC on Citopia.
6. EC receives the VP, validates it (validate proofs, diddocs, contexts) and sends the validation result back to Vehicle on Citopia.
7. Vehicle receives validation results from the EC and stores them in its SSDT.

Figure 17: Entity Interaction for Identity Management System Using ITN for Identity Management and Citopia for Verifiable Credentials and Presentations



Source: JRC and MOBI, 2022.

4.1.3 Results

It was demonstrated that for the three process flows required for SSI solutions, with 1 million tested vehicles, the number of flow executions per second, on resources that include 75 c6i.xlarge AWS instances (4 vCPU, 8GB RAM each) and 1 db.m6g.8xlarge AWS instance for RDS (32 vCPU, 128 GB RAM). As seen in Table 4, the resultant number of flow executions per second is a magnitude of order larger than what is required for the use case. Even if scaling from 1 million to 280 million might not be 100% linear, it will not be far off linearity, and so any small reduction in the flow executions per second will be negligible compared to the overall speed achieved.

Table 4: Performance results of Pilot 1, in terms of Number of flow executions per second.

Flow name	Time to complete 1 million flow executions	Number of flow executions per second
Issue credential (IC)	9 minutes (average**)	1851
Self-Issue (SI)	1 minute 40 seconds (average)	10000
Verify credential (VC)	7 minutes (average)	2380

([1]) 1 million of IC, 1 million SI, and 1 million VC.

([2]) Tested 5 executions with different results: 9:10, 9:30, 8:30, 8:40, 8.50. For simplicity the average was used.

([3]) **Note:** Readers should not use proportionality to estimate costs but can for storage and compute resources, Number of execs per second from 1 million vehicles to 280 million vehicles

Source: MOBI, 2022

4.1.4 Conclusion

The EU mandates 280 million vehicles to communicate their reporting data once a year. The number of Flow Executions per Second (FEPS) per Year required is 280M FEPS. Considering the fact that out of the three flow processes for the SSI management system, the slowest is the Issue Credential Flow, this is 207 times faster than the system requires for transmission of emission monitoring data on an annual basis. This statement can be made because the storage and compute resources scale linearly. However, the cost will scale differently depending on the deployment model – federated approaches with multiple processing centres require less expensive compute and storage resources than a single centre requiring expensive high-performance computing.

If emissions reporting occurred more frequently than the regulation requires, say on a monthly basis, then the SSI management system would be 17.25 times faster than required.

4.2 Pilot 2, Integrity and Provenance of Emissions Data from Vehicles

This pilot investigated the possibility of using BC technology for storing in-use vehicle data. As a straightforward and realistic example, the monitoring of fuel consumption, and indirectly through it CO2 emissions, data was used. In the previous Pilot 1, DIDs, VCs and Verifiable Presentations were used to exchange verifiable data which is stored off-line and communicated using a private messaging protocol. In some situations, the data stored by the vehicle might be used for mission critical applications, like in situations where emissions data may be linked to tolling or rules prohibiting the circulation of a specific vehicle inside a regulated area. In this scenario the data used needs to be tamper-proof and trusted. Other use-cases could be envisaged, either on a vehicle-to-authorities communication level or a vehicle-to-user, or vehicle-to-stakeholder in general, fostering the development of an eco-system, either from a regulatory perspective such as taxation and tolling to foot printing services and shared mobility pricing solutions. The study provides some additional insight on taxation and tolling later in the report.

With the transportation industry producing 29% of global greenhouse gas (GHG) emissions in 2019 alone, it is essential to apply the right tools policymakers, vehicle manufacturers, and service providers need to incentivise vehicle decarbonisation. The BC implementation deployed in Pilot 2, can help to achieve this due to the benefits of the functionality provided to:

— Maintain the privacy of the data,

— Utilisation of the flexible access control features, and

— Data can be irrevocably deleted, making it GDPR friendly.

However, the lack of a standardised solution means these efforts are fragmented across jurisdictional lines and are ultimately not scalable.

4.2.1 Hardware and Software Setup

In this section, the hardware and software implementation that the JRC deployed for the needs of BC4T project are described. The following sections explain the technical setup, the process that was went through for preparing and deploying the proposed solution, the different testing parameters, and finally the results of Pilot 2.

4.2.1.1 Hardware layer - Experimental Platform for Internet Contingencies (EPIC)

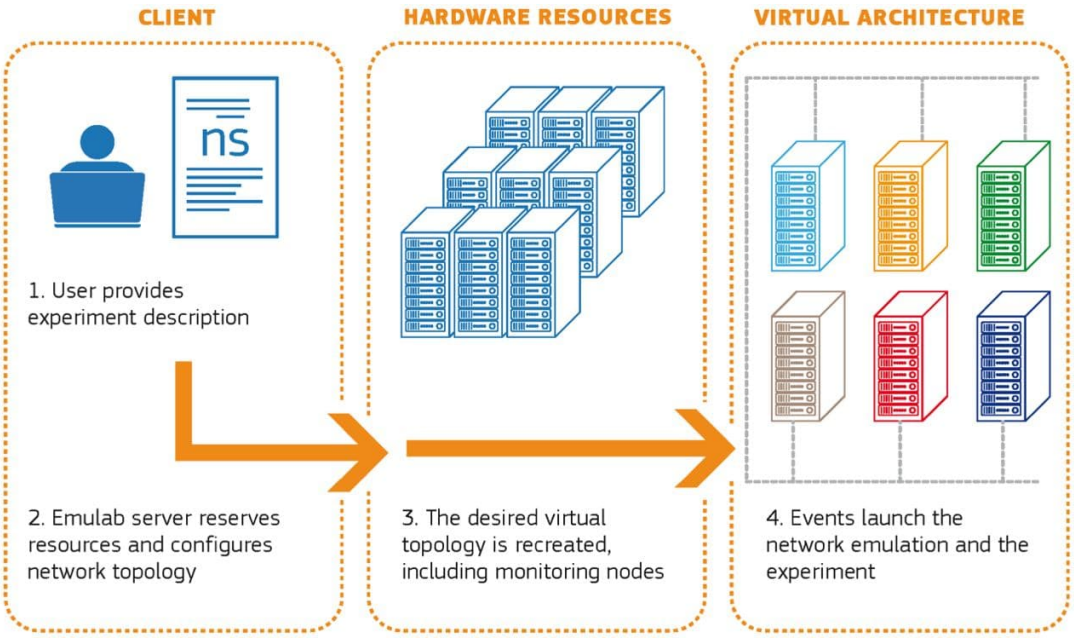
To deploy the initial implementation, it was required to have infrastructure large enough to simulate a real BC network that would theoretically be spread across all Member States (MS). This was in mind originally at the conception of the project and led to identifying the JRC's EPIC cluster as the ideal resource for the purposes of the BC4T project. Use of EPIC not only enabled the simulations of the chosen BC network to simulate on, but in addition allowed for the emulation of the actual network characteristics to closer approximate reality by mapping certain network topologies.

The EPIC (Siaterlis et al., 2013) is a hybrid facility for studying the security and stability of distributed systems. The architecture of EPIC relies on DETER software (Kline et al., 2018, Benzel, 2011) and provides an emulation-based environment to enable testing repeatability and results reproducibility. EPIC allows the emulation of real-world network topologies by assigning physical and virtual equipment in order to recreate the emulated network. The system enables the setting up of the network topology of every experiment including the characteristics of every network link (bandwidth, delay, packet loss rate, etc.). Over this network, standard applications and services can be deployed.

In terms of resources, EPIC consists of 512 nodes each with at least two 1Gbps network interfaces dedicated to the experimental network topology and one 1Gbps network interface connected to the control network. Eight switches are dedicated to the experimentation infrastructure; the nodes can be interconnected with different network topologies.

In order to setup an experiment, the user first needs to provide an experiment description using a specific programming language. The description, among others, defines the name and number of the nodes that are going to be used at the experiment, the kind of hardware they will have, the operating system they will use, what kind of network topology is going to be setup for the nodes, their IPs, etc. Once the description is defined, the Emulab server of EPIC reserves the necessary resources and configures the appropriate network topology. Then, at a hardware level, the desired topology is created. Finally, the experiment nodes are launched with the desired OS, and the experiment is ready to be used by the user. A high-level overview of this process can be seen in Figure 18.

Figure 18: Executing an experiment on EPIC



Source: JRC, 2019.

4.2.1.2 Software Stack

Having set up the hardware on EPIC, the next step is to define and deploy the necessary software. At the end of the experiment setup on EPIC, the user is basically given nodes with a clean operating system running on top of them. Thus, the user must install the necessary end-user applications needed for the use-cases he wants to test.

4.2.1.2.1 Choice of BC Implementation

As a BC implementation Hyperledger Fabric version 2.2 was chosen (subsection 2.5.1) as a private system that is also modular (Hyperledger, 2020) was wanted. Moreover, the smart contract was considered an important aspect of the implementation, and the fact that Hyperledger Fabric supports Java, Go and JavaScript as a programming language gives the flexibility needed to develop the use-cases with all the necessary features. Finally, Hyperledger Fabric provides support for simplified SDKs (Software Development Kit) and also has a large online community, which is very useful for troubleshooting. In the performed experimental setups, HLF is deployed on top of Ubuntu 18.04.

As in the text that follows, many terms that directly relate to the Fabric implementation are used, here the definitions of these terms are listed, as found in the Hyperledger official page (Hyperledger, 2020):

- **Channel:** *"A channel is a private BC overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be authenticated to a channel in order to interact with it"* (HLF, 2020b).
- **Membership services:** *"Membership Services authenticates, authorises, and manages identities on a permissioned BC network. The membership services code that runs in peers and orderers both authenticates and authorises BC operations. It is a PKI-based implementation of the Membership Services Provider (MSP) abstraction"* (HLF, 2020a).
- **Organisation:** *"Also known as "members", organisations are invited to join the BC network by a BC network provider"* (HLF, 2020a).
- **Private data collection:** *"Used to manage confidential data that two or more organisations on a channel want to keep private from other organisations on that channel. The collection definition describes a subset of organisations on a channel entitled to store a set of private data, which by extension implies that only these organisations can transact with the private data"* (HLF, 2021).
- **Endorsement policy:** *"Defines the peer nodes on a channel that must execute transactions attached to a specific chaincode application, and the required combination of responses (endorsements). A transaction that is submitted must satisfy the endorsement policy before being marked as valid by committing peers"* (HLF, 2021).
- **Orderer:** *"A node that performs transaction ordering. Along with other orderer nodes it forms an ordering service"* (HLF, 2020a).

4.2.1.2.2 Use of Private Collection Instead of Separate Channels

When the design of the experiments was initially started, maintaining the data privacy in the solution was focused on. HLF offers two well studied routes out of the box to this case. The first is on-chain via multiple channels, and the other is off-chain via private data collections.

On-chain Data Storage

A new channel is created consisting just of the organisations that will be sharing that private data. Each channel has its own ledger accessible only by its members. In this case, for the 27 Member States that need to be sharing the data with the European Commission, 27 distinct channels need to be created. This solution maintains the privacy of the data as data will only be shared between the EC and each member state but adds to the administration (having to maintain 27 policies, chaincode versions, etc). Moreover, this architecture does not offer any easy solution for sharing data amongst the Member States or moving assets between organisations (in case of trans-border movement or exporting vehicles between countries). If two or more Member States need to exchange data in a private way, a new channel between them will have to be created, adding even more complexity to the system. Having many channels also leads to a lack of information among the participants, as they are not aware of the transactions that take place in a channel they do not belong to.

Apart from the previous, in the case of multiple channels, data gets stored on the ledger where it becomes immutable, potentially making the solution non GDPR compliant. Even though there are ways to mitigate this by data encryption coupled with key destruction (Forum, 2018), it is still a grey area and beyond the scope of this report.

Off-chain Data Storage

Private data collection (PDC) is a way of maintaining privacy by storing off-chain data inside the Fabric ecosystem, making them accessible by chaincode on peers of an allowed subset of organisations. In a PDC, only a defined set of peers belonging to authorised organisations stores the data locally; the rest of the members of the channel only receive a *"hash of the data as evidence of the transaction"* (HLF, 2021).

Private data collection has a set of functionalities that make it ideal for the use-case explored:

1. Maintains the privacy of data,
2. Has flexible access control, and
3. Data can be irrevocably deleted making it GDPR friendly.

Although the data are maintained locally on the permitted peers of the authorised organisation, access control can be easily changed when some of that data need to be communicated to other organisations on the same channel without compromising privacy. Through the use of the gossip dissemination protocol, data be easily transferred across organisations. Moreover, by using the transaction information on the channel ledger, the receiving organisation can verify the validity of the received data. Since the actual data is not maintained on the channel state but on a private database, the actual data can be irrevocably deleted.

The above mechanism and the fact that the data can be controlled by chaincode enables the secure transfer of asset ownership where data are copied and verified on destination. Equally, on the source, the data can be deleted, and a third trusted organisation can endorse the deletion. Additionally, the automatic deletion of data is baked in HLF with the capability to define a set number of blocks before they get deleted from the private database.

For the aforementioned reasons, it was decided to follow the off-chain private data collection route.

4.2.1.2.3 EC Hosting Orderers

In the design, it was decided to maintain the ordering service inside EC premises and not spread it amongst the Member States. There are three main reasons for this decision. Firstly, such an option would simplify the architecture of the system and reduce the technology burden on the Member States. Moreover, the EC is considered as a trusted partner and can act as a facilitator of the network.

Finally, the third reason concerns the performance of the system when its components are geographically split. Orderers on HLF v2 are using an implementation of the raft protocol (Ongaro and Ousterhout, 2013) in order to achieve consensus. This algorithm has a follow-the-leader model where the members of the quorum vote to elect a leader who then is the only one responsible for log replication. All read/write operations go through this leader. It has been shown (Ng, 2020) that this model in geographically distributed networks can cause high network latency both for read and write operations when a remote or otherwise high latency leader is elected.

For the above reasons, it was decided to maintain the ordering service in the EC. Although this does make the system more centralised, it allows for high performance and low latency.

4.2.1.2.4 Orchestration Layer

Since the EPIC experiment only provisions full Linux nodes and modern software practices dictate the use of containers for ease of use and portability, it was decided to use Kubernetes on top of EPIC in order to facilitate deployment, scalability and reproducibility of the system the project team developed.

Kubernetes has become the de facto container management platform for large and complex workloads. Kubernetes is a portable, extensible, open-source platform for managing containerised workloads and services that facilitates both declarative configuration and automation. It takes care of setting up the networking layer for the

containers, the storage provisioning and scaling according to the needs of the experiment (Kubernetes, 2022). Kubernetes can be extended with multiple services such as Prometheus (Prometheus, 2022) for monitoring, service meshes such as Istio (Istio, 2022) or package managers like Helm (Helm, 2022). On EPIC, the Kubernetes cluster was deployed on top of the Linux nodes provisioned by each experiment using the Kubespray deployer (Kubespray, 2022).

4.2.2 Experiments for Emission Data Monitoring

The aim of the experiment is to verify the feasibility of storing emission data from the whole EU vehicle fleet using BC technology in a secure and privacy-preserving way. The intention was to show by emulating a representative setup that the overall BC performance, including transaction throughput and latency, meets the minimum requirements for such a system.

The project teams goal was to achieve the aforementioned minimum throughput for 280M vehicles in EU, i.e. 107 transactions per second and a latency that would not cause operational interruptions. The business logic of the experiment is as follows.

When a new vehicle is registered with the Registration authority of a Member State, a new X.509 certificate is created by the MS CA using a random Universally Unique IDentifier (UUID). Then the car enrols with the Member State providing the VIN and any other relevant private data. The private data are stored only on the MS servers, and proof of the transaction is stored on the global state database of every MS organisation. Once the registration is complete, the vehicle will send the emission data to the relevant MS organisation as well as the EC organisation. These data are stored only on the MS and EC servers, and proof of the transaction is once again stored on the global stated database on every MS organisation.

In the performed experiments, following entities were used:

1. Vehicles,
2. National Authorities from Member States (Regulators, Compliance Institutional bodies, and Registration Authorities) here collectively referred to as RA, and
3. European Commission.

The reason for choosing the specific design where the private data is represented by a UUID is the requirement for a privacy friendly solution for what concerns sensitive data. Fabric being a permissioned ledger requires an identity mechanism and provides an abstraction for that called Membership Service Provider. The default implementation is using RFC5280 (Cooper, 2008), which is the specification for the X.509 certificate. These certificates, when designed, were never intended with privacy in mind, so the certificate usually contains attributes that do contain Personal Identifiable Information (PII).

The Vehicle identification number (VIN) (vehicles, 2009) and any Personally Identifiable Information (PII) will be kept with the member state registration authorities and will be replaced by a UUID. That UUID will be provided as user id when generating a new X.509 certificate for a new vehicle thus leaving the responsibility of managing PII to each Member State and decoupling the vehicle certificate from its VIN.

Data generated by the vehicles will be stored in a private collection on the peers of each individual member state as well as the European Commission's peers. The rest of the members of the channel will only be getting a hash of that data. *"The hash serves as evidence of the transaction and is used for state validation and can be used for audit purposes"* (HLF, 2020b).

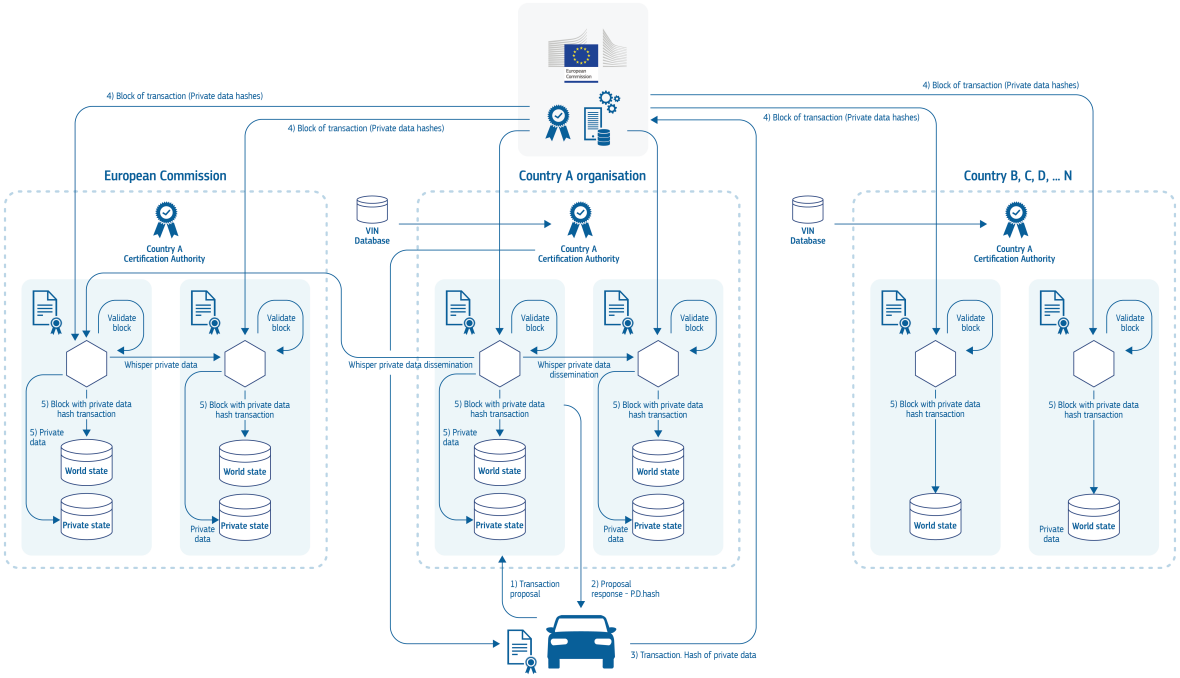
As shown in Figure 3 19 to store the emissions data produced by each vehicle a BC with a single channel and 28 organisations is proposed (27 member states + EC). Each member state will have its own MSP (CA) and will be generating certificates for vehicles registered in its jurisdiction. It will also maintain a number of fabric peers that will be storing the transactions as well as the emissions data or any data deemed private generated by each vehicle. A high-level transaction flow is as follows:

1. A new vehicle is registered with Fabric. The member state registration authority (RA) generates a UUID that acts as a primary key in their database.
2. Member State CA registers a vehicle using that unique identifier.
3. Vehicle enrols to organisation receiving an X.509 certificate from member state CA.

4. Vehicle makes a transaction proposal containing private data (distance travelled, CO_2, etc).
5. At least one endorsing peer from the vehicle's member state organisation and at least another from the European Commission simulate the transaction, store the private data temporarily and return to the vehicle a proposal response containing the hash of the above data.
6. The vehicle sends the proposal response to European Commission's orderer.
7. The orderer puts the transaction in block and when the block is filled sends it over to all the registered peers of all member states.
    — Notice that the transaction in the block only contains the hash of the private data.
8. Peers of member states that have access to the private data verify that the hash in the public block matches the data.
9. Peers with access that don't have the data use the gossip data dissemination protocol to pull private data and verify the hash.
    — In case the EC is considered a trusted organisation, the data will be transferred to the EC peers using the gossip protocol.
10. Peers with private data store them in a private state database and add the block containing the transaction hash to their ledger.
11. The rest of the peers validate the transaction as normal and add the block to the ledger.

It is important to note that the TLS provides encryption for data in transit and for *"data at rest can be done via file system encryption on the peer"* (HLF, 2020a) but it's not native to the HLF framework.

Figure 19: Network Design of Simplified Scenario with Full Transaction Flow



Source: JRC, 2022.

4.2.2.1 Experiments Overview

In order to understand in depth, the use-case considered, two setups were chosen that were executed multiple times with a varying number of organisations and clients. The major difference between each experiment was the endorsement policy and the way clients were setup.

In the initial setup, the endorsement policy required an endorsement from the majority of the endorsers on the network. This was found to cause unneeded network traffic and a big storage footprint. In the later setup this was changed to require an endorsement only from the endorser of the vehicle's registration member state and an EC endorser.

Regarding the clients, initially, it was setup so that a small number of clients maintain the connections and are constantly sending transactions. Although this showed a high number of TPS, it did not represent the reality where vehicles connect, send the transaction, and disconnect. Over the later iterations of the experiment, moved to a model where clients connected, authenticated, sent a transaction with the required data, and closed the connection.

For all the experiments, it was taken into consideration the following simulation parameters:

- The number of nodes for the Member States and the EC.
- The number of transactions per time period required for emission monitoring (1 per month).
- Size of data requiring transmitting (from OBFCM regulation)
- Standard fuel vehicle: total distance travelled (lifetime), total fuel consumed (lifetime), UUID.

4.2.2.2 Experiments Configurations

Using the above-mentioned hardware and software (subsection 4.2.1), the experimental setup was performed. In the sections below the experiments components have been listed.

4.2.2.2.1 Network emulation and node configuration

The experiment was deployed with 80 EPIC nodes. On the test network each node was connected to a central switch using a 1GBPS line without any traffic shaping. The nodes assigned were of EPIC type x3550vm2 each with 6GB ram, 40GB HDD & 2 vCPU of Intel Xeon E5-2609 v4 @1.7 GHz.

4.2.2.2.2 Kubernetes configuration

On top of the aforementioned nodes, a kubernetes cluster was deployed with 3 nodes on the control plane and the rest on the data plane. One of the control plane nodes doubles as an NFS server for sharing configuration amongst HLF components. More specifically, Kubespray v2.15.1 was used to deploy Kubernetes v1.21.1. The version of docker used is 20.10.

4.2.2.2.3 Hyperledger Fabric

At the time this research started, the latest version of Hyperledger Fabric was 2.2. Since then, versions 2.3 and 2.4 have been released without major improvements in performance or changes in the basic components of the system. Therefore, the same version of HLF was used in order to get comparable results throughout the experimentation.

To the best of the project teams knowledge, at the time of development, there was no documented way of installing Hyperledger Fabric version 2.x on top of Kubernetes. The project team, therefore, had to create a custom solution. In order to deploy the HLF on Kubernetes, a custom operator was produced consisting of multiple jinja2 templates and python scripts. For building and launching the chaincode, a custom image that communicates directly to the Kubernetes API was utilised (djboris9 et al, 2022).

To simplify things, a single endorsing peer is used for each organisation and a common TLS-CA service is employed for all HLF organisations. The HLF network is run using a single Raft orderer. Each container is deployed on its own node apart from the peer and chaincode containers that are deployed on the same node in order to use the fastest loopback interface. The cli containers are used only during the deployment of the system and are shut down once finished. The load clients sit outside the Kubernetes cluster on top of normal EPIC nodes.

Overall, there was the following structure per member state organisation:

- a peer pod,
- a chaincode pod,

— a CA pod, and

— a temporary cli pod.

Moreover, the orderer consisted of:

— a CA pod,

— a single orderer pod, as well as

— a temporary cli pod.

4.2.2.2.4 Measuring Results

In order to measure the results and have a common ground for comparing the different experiments, as list of defined metric that were used in all cases have been referenced below (Hyperledger, 2018):

$$Read\_Latency = Time\_of\_Received\_Response(t) - Submit\_Time(t) \tag{1}$$

$$Read\_Throughput = \frac{Total\_Read\_Operations}{Total\_Time\_in\_Seconds(t)} \tag{2}$$

$$Transaction\_Latency = [Confirmation\_Time(t)@Network\_Threshold] - Submit\_Time(t) \tag{3}$$

$$Transaction\_Throughput = \frac{Total\_Committed\_Transactions}{[Total\_Time\_in\_Seconds(t)@Number\_of\_committed\_nodes]} \tag{4}$$

Following the above pattern, the following metrics are defined:

$$Write\_Latency = Time\_when\_Commit\_Confirmation\_Received(t) - Submit\_Time(t) \tag{5}$$

$$Write\_Throughput = \frac{Total\_Write\_Operations}{Total\_Time\_in\_Seconds(t)} \tag{6}$$

The measurement of write latency is done at the client level whereas metrics on transaction latency and transaction throughput are measured at the HLF network level.

To find the transaction throughput of the network the broadcast_processed_count metric was monitored on the ordering service, that measures the number of processed transactions over a certain time. The primary interest was in the write performance of the system, so the latency presented here is the write latency measurements from all clients, averaged out.

On the client, the time to execute each transaction is measured. The metric only considers the transaction roundtrip and does not include the time taken to setup the connection to the peers required.

During each experiment run, since the broadcast_processed_count contains both valid and failed transactions, the number of failed transactions was monitored on each peer to validate the system's health. For that the ratio of endorser_successful_proposals vs endorser_proposals_received was close to 1 was verified. Similarly, the number of failed transactions on the clients was kept track of.

Monitoring of the system was done in two ways: Using a Prometheus (Prometheus, 2022) log server to gather information from the orderer and all endorsing peers, and on the same time the performance on the client side was measured by code instrumentation. For visualisation of the data gathered by Prometheus, Grafana (torkelo et al, 2022) was used.

The main performance metrics of interest is the throughput and latency as these are the most objective metrics to verify the system has the potential to fulfil the requirements of the use-case. Specifically with 281 million motor vehicles in Europe (ACEA, 2022) reporting once a month would require a minimum of 107 transactions per second in order to achieve this, assuming all requests were evenly distributed across this time period, without including any retransmissions, or peaks of data at certain time periods.

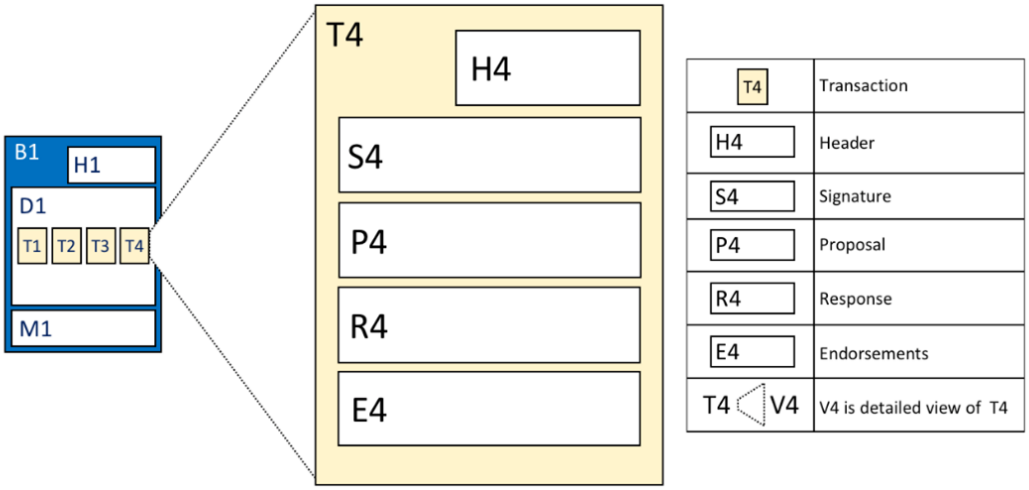
Latency becomes important when real time data is required or when operating an interactive application. Although this is not the case for this experiment, low latency means less timeouts and less retransmissions of data.

4.2.2.3 Experimental setup 1

This is the initial implementation of the design described previously. As an endorsement policy, the default *"MAJORITY Endorsement"* was used. This means that each transaction must be executed and validated by a majority of endorsing peers belonging to each member state. As seen in Figure 20 depicts, HLF stores all endorsements in the transaction. Consequently, the size of each transaction increases linearly with the number of endorsing peers. In the case of a "MAJORITY Endorsement" policy for 28 organisations, each transaction stored at least 15 endorsements. Each endorsement is the signed output of the chaincode execution (Androulaki et al., 2019). For the network developed by the project team, HLF is using the ECDSA with SHA256 signature algorithm that generates a signature of 64 bytes. The endorsement is accompanied by the X.509 certificate of the endorser, which adds an overhead of 800 bytes to it (Barger et al., 2020). This increased the footprint of each transaction by at least 12.6KB. As each peer had a ledger storage limit of 10GB, it was noticed that after around 100.000 transactions, all storage space was occupied.

Moreover the client configuration of this setup was not representative of a real world scenario. Each simulated vehicle connects once using a specific user identity and an X.509 certificate and constantly sends requests to the network. This means that the connect-discover-authenticate-disconnect workload was not taken into account, that occurs when a vehicle connects.

Figure 20: Transaction details. Transaction T4 in blockdata D1 of block B1 consists of transaction header, H4, a transaction signature, S4, a transaction proposal P4, a transaction response, R4, and a list of endorsements, E4. Source: (Hyperledger, 2020)



Source: JRC, 2022.

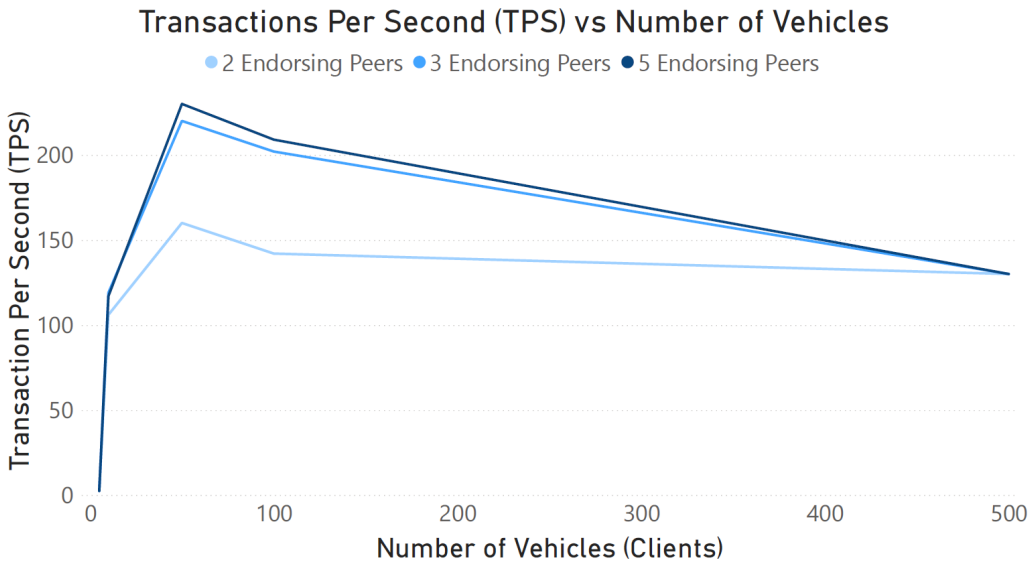
4.2.2.3.1 Results

In this section results are presented with the aforementioned setup. A total of 500 clients and 5 Member States (total 6 endorsing peers including the EC peer) were simulated. Beyond that, a break down in the network's ability to accept new transactions was noticed. With the addition of 100 more clients the system became unstable and the majority of transactions were timing out.

As seen in Figure 21, with all variations of the experiment as to how many endorsing peers are used, the maximum throughput is reached when 50 vehicles are connected. After this peak the throughput decreases, but still maintains a high number of TPS. As the goal was to have at least 107 TPS, this throughput is achieved in the current setup.

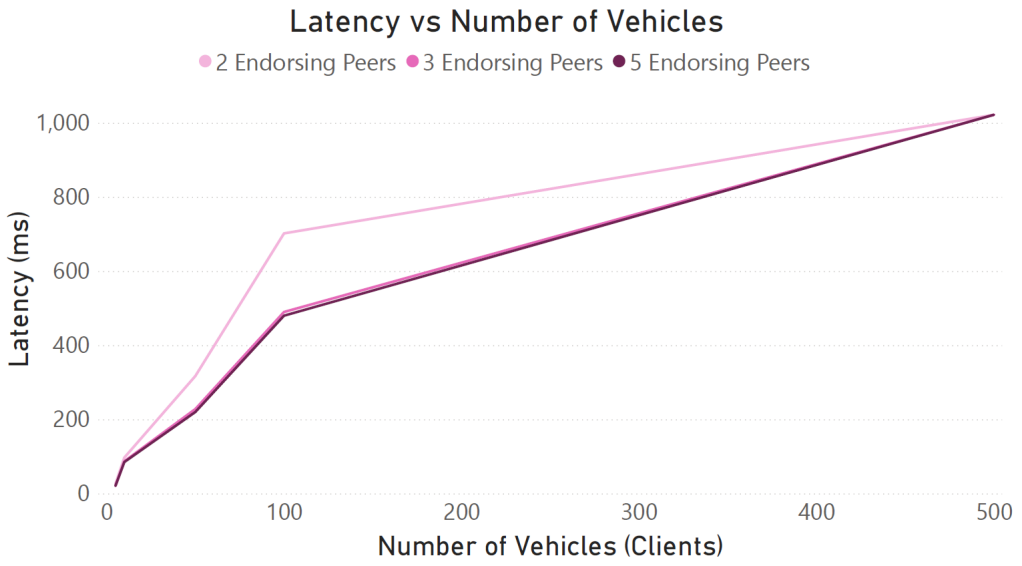
In the same tests, it was noticed that latency increases linearly with the number of vehicles in Figure 22. Once again, there are no variations between the different setups, and all three follow the same pattern. The above results show that the maximum performance is achieved at 50 clients with the system getting saturated with more clients as is evident from the average latency increase. The network reaches latencies of almost one second at the maximum number of clients which is significant but not at all prohibiting for such applications. The reason for the performance degradation is probably due to the very wide endorsement policy that requires a large number of signatures. According to Thakkar et al., the number of crypto signatures verification has a significant impact on performance and resource utilisation.

Figure 21: Transactions per second for 2,3,5 member states plus EC for a different number of simulated vehicles.



Source: JRC, 2022.

Figure 22: Latency for 2, 3, 5 member states and EC for a different number of simulated vehicles.



Source: JRC, 2022.

For the application of emissions monitoring, due to the data only requiring transmission once a month, the relatively large latency when compared to 5G (24ms) interacting with a centralised database is not an issue. Although, it could be a limiting factor on certain BC for transport use-cases.

4.2.2.3.2 Limitations

During this first round of experiments, two significant limitations were found, concerning disk usage and network connectivity. In particular:

1. Disk Usage: Incremental increase of storage due to consensus strategy. As discussed above with the tested endorsement policy HLF stores signatures of the majority endorsing peer for each transaction.

2. Network Connectivity: Maintaining open connections from a few clients to each peer does not represent real world usage; this testing strategy is only stressing parts of the system. When sending transactions using a limited number of vehicles can potentially lead to inaccurate results due to caches and database optimisations. Moreover, requiring signatures from each endorsing peer increases network usage and limits the number of organisations in the network.

4.2.2.4 Experimental setup 2

For this second set of experiments, the consensus strategy was modified to only require signatures by the endorsing peer of the member state where the vehicle is registered AND the EC endorsing peer, with the hashes of the data still added to the shared ledger. These changes were made for the following reasons:

1. EC is an inherently safe environment with the hashes used to maintain the integrity and auditability of the data.
2. A significant amount of storage is saved since each transaction only needs to be signed by endorsers from two organisations.
3. This change will also lead to less network traffic, as endorsement is required from endorsers of only two organisations.

The clients were also modified in order to replicate a real-world scenario. 100,000 VINs were generated for each member state and registered them with its CA. Each ID represents a vehicle. The simulated client randomly chooses an ID and uses it to connect to the peer of its member state. Through that peer, it discovers the rest of the network configuration as well as the endorsement policies. It then authenticates to the required peers, acts on the transaction, and disconnects. This process exercises the whole system rather than a specific subsystem and is more representative of the actual use-case.

In the performed tests 100,000 transactions per member state were sent, with a varying number of clients. As with the previous experimental setup the block size was set to 50 transactions. It has been shown that bigger block-sizes correspond to higher TPS and lower latencies when the transaction arrival rate is high (Thakkar et al., 2018). 50 was chosen as it's been shown to provide high TPS when using the leveldb database (Manevich et al., 2021), and during the experiments it provided a good compromise between low latency in small loads vs high TPS.

To generate enough transactions an async node.js script was used, utilising the Hyperledger Fabric SDK for node.js version 2.2 (Hyperledger, 2022b). The script initiates 5 connections, each representing a vehicle sending data. As soon as all 5 simulated vehicles have finished their interactions with the system, the connections are severed, and 5 new ones are initiated for different simulated vehicles. In order to achieve a large number of connections GNU parallel was used to run a copy of the script multiple times simultaneously.

4.2.2.4.1 Results

As shown in Figure 23 and Figure 24 it was possible to simulate the full-blown network with 27 member state organisation plus the EC. It is notable that it was able to accommodate 200 clients per MS (a total of 5400 simultaneously connected clients) that sent a total of 2.7M transactions, without any stability issues and with reasonable performance. It was noticed that for any number of organisations a saturation point was reached at around 250 TPS which appears to be the maximum throughput the system can reach with its current configuration.

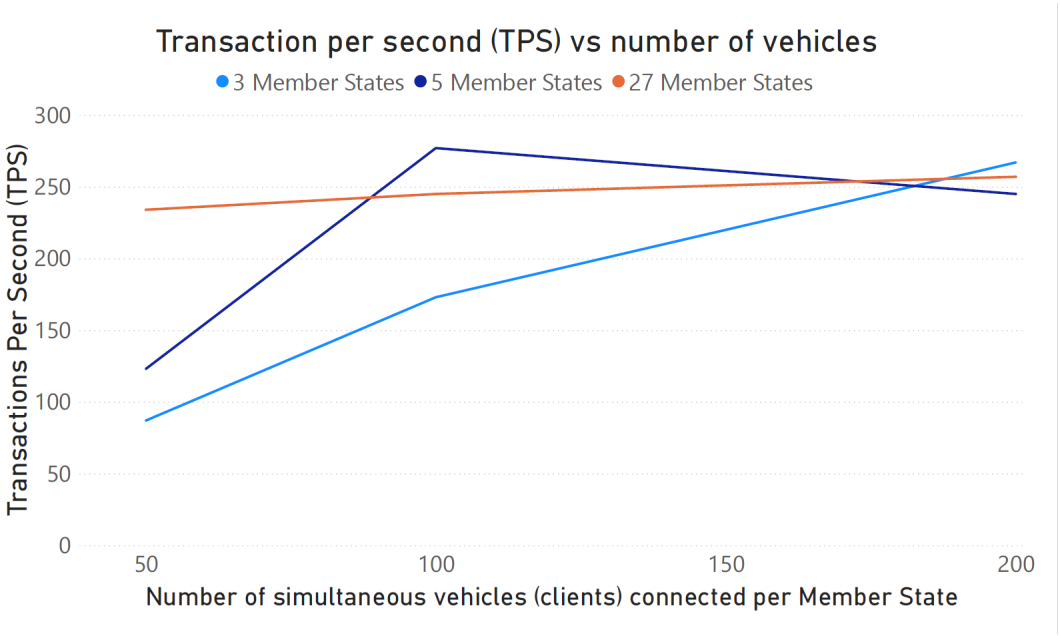
As seen in Figure 23, for a small number of member organisations with a few clients, there isn't enough load generated in order to saturate the system. With 3 MS the saturation point is reached at 200 clients per MS and the same applies for 5 MS. This is obvious from Figure 23 and Figure 24. For 100 clients per MS the network hits maximum performance with 280TPS and around half a second latency. When increasing the number of clients to 200 per MS the TPS goes down to 245. Since the latency remains constant as per Figure 24 the project team hypothesize that the network remains close or below the saturation point but this reduction is happening due to the increase in CPU utilisation caused by the large number of clients.

Although the system performance did not degrade, it was noticed that 100% of both vCPUs were used in all endorsing peers. With 27 Member States, the system was saturated even with a small number of clients. The latency was significantly higher than the previous 3 and 5 MS configurations for 50 simultaneous clients and increased to almost 2 seconds when there was 200 clients. Still, it is important to point out that the system remained stable, and no failed transactions or timeouts were seen on the client side. Not shown in the above figures are the trials with 300 simultaneous clients. For all different MS configurations, there was increased system instability with many failed transactions mostly due to timeouts and inability to connect to peer.

4.2.2.4.2 Limitations

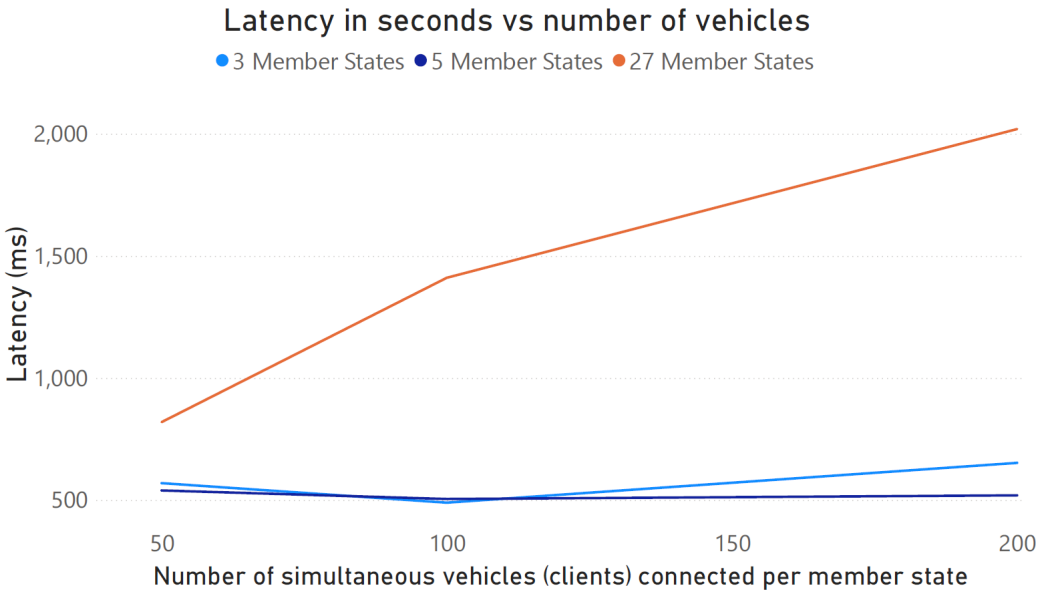
The main limitation noticed had to do with the number of clients. The system could not accommodate more than 200 simulated vehicles per member state organisation. When the vehicles in the simulation increased, the number of timed out transactions and the number of clients that could not connect increased dramatically.

Figure 23: Transactions per second for 3, 5, 27 member states + EC for a different number of simulated vehicles. Source: JRC, 2022



Source: JRC, 2022.

Figure 24: Latency in sec for 3, 5, 27 member states + EC for a varying number of simulated vehicles. Source: JRC, 2022



Source: JRC, 2022.

In addition, the load generating client strategy had to be changed from using a single async node.js script per endorsing peer to multiple short-lived ones due to a bug (Ryu-Shinzaki, 2021) that was leaving GPRC connections open causing memory leaks both on the client as well the peers. This means the NodeJS program is killed after every few thousand transactions in order to release the memory.

4.2.3 Conclusions

In this pilot the aim was to evaluate if sharing vehicle data to a BC-based system would be technically feasible with the current available technological solutions. The performed work was formulated towards this direction, using real-world fuel consumption monitoring as an example use-case. As a result, a vehicle fleet of 280 million vehicles were considered, having the legal obligation to transmit once per year their CO_2 emissions to the EC.

With the performed experiments, and in particular with the optimisations performed for the experimental setup 2 (section 4.2.2.4), a maximum of 5400 parallel connected clients was achieved, i.e., vehicles, spread in the 27 Member States, each one of them performing the full life cycle of connecting to the platform, discovering services, authenticating, sending the transaction, and disconnecting, which results in an approximate three second execution time. With these parameters, a maximum throughput of 257 TPS was reached, with the system being steady and responsive.

In an ideal situation, considering the 280M transactions needed as a minimum per year and dividing it by the highest reliable throughput that can be achieved under the current setup, a total execution time of approximately 12.6 days would be achieved for registering the transmissions of all the vehicles in the EU. This result is, of course, not realistic in a real-world situation, where the requests will arrive in a not-optimal timing, and moreover peaks and dead spots will also be observed. It nonetheless permits, the project team, to state that *"we are not only able to meet the legal requirement of recording one transaction per vehicle per year, but it is also promising to reach the given experimental goal of bringing down the requirement to 1 transaction per vehicle per month"*. The project team is indeed optimistic though, that with performance optimisations and with hardware improvements, the throughput of the system can be improved.

At the same time, with this work it was observed that there are some important limitations of Hyperledger Fabric, such as the large transaction overhead, in terms of disk usage, for every endorsement needed, as well as the ability to simultaneously handle many open client connections. The project team has improved the results in the experimental setup 2, working on the above limitations and already saw a significant performance improvement.

The EPIC has very recently deployed a new cluster which has upgraded RAM, CPUs and the addition of Solid State Hard-Drives (SSDs). Although the new cluster is still in the testing phase, the initial performance results of experiment 2 are five times faster in terms of TPS. It appears the bottleneck was arising from the previous storage disks only being 30GB in size and being very slow to read and write. As described previously, Hyperledger Fabric has intensive disk usage which was creating a large transaction overhead. So, it makes sense that with both massively increasing the speed and the size of the Hard-Drives, the resultant TPS has a fivefold improvement. Experiment 1 and 2 will be redone on the new EPIC cluster showing the vastly increased BC network speed and to provide the detailed results needed to show that the bottleneck was the storage disk on the old cluster. These results will be published in the form of journal publications and should be available after this Science for Policy Report is published.

Finally, with the experiment setups, the project team has gained valuable knowledge and practical know-how on deploying and using Hyperledger Fabric on top of Kubernetes. When the practical tests were started, this domain was still undiscovered, and the project team had to create custom solution. This process not only helped the project team to better understand the internal mechanisms of HLF, but also led us to completely automate the deployment procedure, thus facilitating the execution of many experiments with different parameters.

4.2.3.1 Next Steps

With the setup and results, the project team has achieved the original set of goals; however, room for improvement has been identified, which will be implemented as future work.

First of all, the project team would like to extend the experiments with other setups as well. The current setup of one peer per member state is not suitable for a production system as there isn't enough redundancy. It is planned to increase the number of endorsing peers per MS to test how the larger number affects the available throughput capacity of the network or allows for more vehicles to be simultaneously connected.

Moreover, using EPIC, a geographically distributed network will be emulated by introducing limitations between various HLF subsystems. It is the project teams aim to show that slow peers, or network performance on a member state organisation does not affect the performance of the whole network. Similarly, in order to reach more realistic test conditions, latency and packet losses will be introduced on the client connections to emulate a mobile network as would be the case with vehicles on the road where patchy network coverage could affect the the connectivity.

In order to amplify the results' collection, the project team will perform analyses on memory, CPU and disk storage usage of the developed BC system. It would also be beneficial to better understand the BC network requirements and operational costs for the lifetime of a hypothetical market-ready solution.

For what regards the actual use-case, the project team would like to enhance the services offered and implement SSI standards for vehicle digital identity management. By doing so, by using a more robust digital identity solution there are various benefits, including increased privacy when combining with Zero-Knowledge Proofs.

Finally, and very importantly, the project team would like to use a realistic model for what concerns everyday use of vehicles. It is understood that the transactions originating from the vehicles will not happen under ideal conditions, all arriving at a convenient time without creating long queues and delays; the results will therefore vary significantly in such a case. Studies have been identified (Paffumi et al., 2018) that indicate the distribution of vehicles across the week, indicating peaks and drops of mobility traffic. Matching the generated transactions with such models would help to better understand how the system would behave in real world conditions.

4.3 Pilot 3, SSI Vehicle Identity Management System and HLF Data Provenance Pilot

In BC4T, the property of data provenance and integrity was implemented using HLF, which is a framework for building general-purpose BCs. This was implemented using X.509 certificates to manage the identity associated with the different entities acting within the system. The other previously performed study described within this report was on the use of a more advanced identity management system, through an SSI framework, to allow for increased privacy and increased control of one data with functions such as choosing with ease which has what level of access and when. These two use-cases were then combined such that there is the data provenance and integrity guaranteed by the HLF network that communicates with a BC system that is dealing with the SSIs; built using Hyperledger Aries and Indy, which are purpose built for Verifiable Credentials, DIDs, and SSI management.

The JRC team members contacted the CERTH research centre after encountering a research paper in which they had connected an Identity Management System constructed on top of Hyperledger Aries and Indy, which utilise SSI standards such as VCs and DIDs, to Hyperledger Fabric that works with X.509 Certificates and has not the concept of VCs or DIDs. The communication between the heterogeneous BCs HLF and HLI was achieved through the creation of a gateway that can translate the SSI standards of VCs, DIDs and map them to X.509 certificates which can be understood and used by HLF. The JRC team decided to rather collaborate with CERTH instead of attempting to create such a gateway internally, as the development time and cost to do this would exceed the available time for the whole exploratory research project.

This technical implementation involved the collaboration between CERTH and the JRC team members of the BC4T project. The content of this section is organised as follows. A breakdown of the components that comprise the technical infrastructure is provided by a short description of their functionality. Next, in separate sub-sections, the two main flows of the system are introduced. The first is related to a setup process required to prepare the software components that are installed on a newly produced vehicle. The second is related to the solution's live operation, i.e., when a vehicle is in operation and submits emission reports on the BC.

4.3.1 Hardware and Software Setup

4.3.1.1 Hardware

In pilot 3 the hardware system used was identical to the infrastructure used in pilot 2, as in subsection 4.2.1.

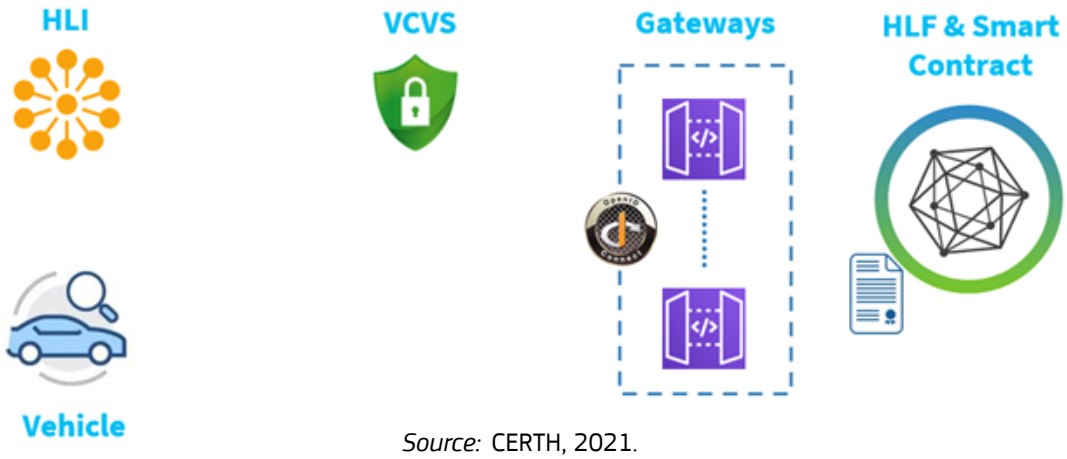
4.3.1.2 Software Stack

All previously mentioned software components for Pilot 2 relating to HLF have been mirrored in pilot 3, with the addition of the Vehicle Emissions Smart Contract Gateway that acts as an intermediate between the HLF and the SSI management system. An exhaustive list of the components for the whole system can be found in the Components Overview subsection 4.3.1.2.1 below and has been divided into two categories. The first category refers to the components which are related to the HLF BC network, and the second category consists of components relating to the SSI management part of the tool, namely those associated with Hyperledger Aries, Hyperledger Indy.

4.3.1.2.1 Components Overview

The components that comprise the technical implementation of BC4T, an overview of which is presented in the figure below, can be organised into three categories introduced in this section.

Figure 25: CERTH Technical Components Overview



Source: CERTH, 2021.

The first category is composed of components that are related to the Hyperledger Fabric part of the infrastructure, which are as follows:

- **Network:** Composed of two peer organisations that host and execute the smart contract (discussed below) and one orderer organisation that performs consensus, which provides for the ordering of events (blocks, transactions).
- **Vehicle Emissions Smart Contract:** This constitutes the main collection point for reports that are issued to it by vehicles. To provide for privacy, it internally employs private data collections and provides an interface that allows query functionality regarding registered vehicles, the reports that they submitted, and others based on the DID of each vehicle.
- **Vehicle Emissions Smart Contract Gateway:** An HyperText Transfer Protocol (HTTP) facade of the smart contract introduced above, which in short, exposes its functions as REpresentational State Transfer (REST) endpoints that can be invoked by vehicles to, mainly, post their emission reports on the ledger. This component also acts as an abstraction layer of the Hyperledger Fabric network and provides for increased modularity, among others.
- **Explorer:** A visualisation tool for Hyperledger Fabric that presents various statistics of the network, its structure, the chaincodes (smart contracts) that are instantiated on top of it, as well as the ability to inspect blocks and the transactions encompassed therein.

As described in the technological component overview section subsection 2.5.1:

Hyperledger Aries: is a toolbox for developing, transferring, storing, and using verifiable digital credentials. Protocols that enable connectivity between agents using secure messaging to exchange information are at the heart of the system. Peer-to-peer interactions between agents controlled by various entities—people, organisations, and things—are central to Aries. Verifiable credentials can be exchanged based on DIDs rooted in different ledgers (based on Indy or other technologies) utilising a variety of verifiable credentials implementations using its standardised messaging layer.

The second category is composed of components that are related to the Hyperledger Aries part of the infrastructure, which are as follows:

- **Hyperledger Indy Network:** A BFT BC that is purpose-built for identity that supports the SSI concepts. It is primarily focused on identity and does not provide built-in support for asset exchange or any kind of smart contract. HLI offers a decentralised source of trust for publicly available information that is needed for SSI systems. It is a public and permissioned BC. The public aspect means that everyone can read and use the ledger, while the permissioned aspect means that only authorised nodes can write on it.
- **Explorer:** A visualisation tool that provides similar functionality to that of the explorer of Hyperledger Fabric, albeit tailored for the Hyperledger Indy ledger.
- **Verifiable Credentials Verification Service (VCVS):** This component brings forth a new way of using and sharing VCs for authentication. It bridges the gap between the world of VCs with that of the traditional

OIDC standard. User authentication automatically inherits all the properties of SSI, such as data portability and minimisation. The VCVS can be integrated with any application and provide OIDC authentication. It can be deployed like an additional service for OIDC authentication towards legacy systems and provides for transparent integration with off-the-shelf Identity Management (IDM) framework, which reflects the benefits provided by building on top of standardised protocols.

- **Credential Issuer:** Provides for functionality that is relevant to entities that issue credentials in an SSI ecosystem, i.e., creating and publishing credential schemas and definitions on the Indy ledger, as well as, issuing credentials to other entities (vehicles in the case of BC4T), which can also be revoked if need be.
- **Vehicle SSI Agent:** This constitutes one half of the software components that are installed on each vehicle. It abstracts all the intricacies of the SSI-related protocols from the Vehicle Client application (discussed below) and provides functionality related to establishing peer-to-peer network connections with other entities of the SSI ecosystem (e.g., the credential issuer), receiving and validating arbitrary VCs and, subsequently, presenting them to verifiers (e.g., the VCVS in the case of BC4T).

Lastly, a set of miscellaneous components that do not strictly belong in any of the aforementioned categories but are relevant to the technical implementation as a whole:

- **Vehicle Client App:** The other half of the software components that are installed on each vehicle. This is essentially a daemon that, based on a configurable time period, attempts to publish emission reports on the Hyperledger Fabric network.
- **Setup Utility:** A collection of scripts that automate parts of the deployment process, such as initialising and setting up the Credential Issuer and, subsequently, issuing credentials to the SSI agent of each individual vehicle.
- **Reverse Proxies:** Standard SSL termination related functionality to provide for secure exposure of upstream services.
- **API Gateways:** An extra security layer between the actual upstream services and the requests that are routed to them that mainly serve as a point of verifying OAuth 2.0 and OpenID connect JSON Web Tokens (JWTs) prior to them being forwarded upstream.

4.3.2 Experimental Setup

For the initial deployment, it is best practise to keep the system's complexity to a minimum. To this endeavour, it was chosen to deploy the HLF part of the system to consist of only two organisations, initially, with the intention to scale up to 27 organisations after this initial test deployment was achieved successfully. The ordering service was identical to pilot 2, specifically running a single orderer under the administration of the EC.
As described in the hardware layer listing, the new component that acts as middleware between the Hyperledger Fabric and the Aries toolchain is the Vehicle Emissions Smart contract Gateway. Each gateway is connected to a Member State organisation and brokers the communication between the vehicle's SSI agent and the HLF smart contract. To provide load balancing and allow easy integration, the gateway was ported as a deployment in the Kubernetes cluster.

During this PoC and with the goal of simplifying the deployment, it was decided to maintain the SSI and client functionality independent from the data retention functionality provided by HLF. In this architecture, the components described in the second category related to Hyperledger Aries were kept outside the Kubernetes cluster and were deployed using docker compose on individual EPIC nodes. Specifically, the following deployment structure was used for all the components.

The HLF components were deployed inside the Kubernetes cluster. Specifically, with the following structure:

- a peer pod,
- a chaincode pod,
- a CA pod, and
- a temporary cli pod.

Moreover, the orderer consisted of:

- a CA pod,

— a single orderer pod, as well as

— a temporary cli pod

The SSI components were not deployed inside the Kubernetes cluster but were orchestrated with docker compose on individual EPIC nodes. Specifically, the structure is as follows:

— EPIC Identity Node 1:

- 4 Hyperledger Indy node containers
- Webserver container

— EPIC Identity Node 2:

- Verifiable Credentials Verification Service web server container
- Verifiable Credentials Verification Service database container
- Verifiable Credentials Verification Service Aries-cloudagent container

— EPIC client Demo node:

- 20 Aries-cloudagent containers
- 20 vehicle client containers.

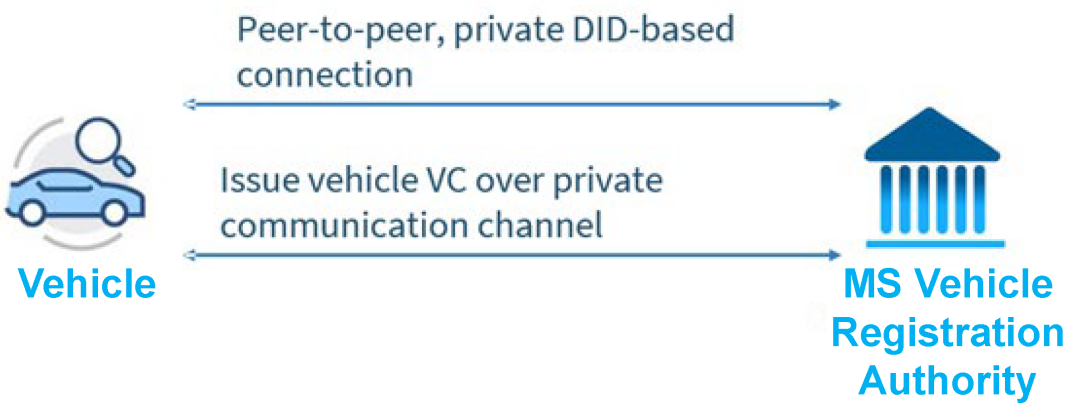
One important change to the existing smart contract used in Pilot 2 was the replacement of the UUID string used to uniquely identify the vehicle with its DID. In the current implementation, the DID identifies the vehicle. The gateway acting as the intermediate is using its own X.509 certificate to sign each transaction, making the DID string the primary vehicle data identifier for each payload added to the HFL ledger.

In this experiment, 20 virtual vehicles and their SSI agents were simulated. Since the simulated vehicles were deployed with docker compose, only a single virtual machine could be used to load all the required containers. In this case, the limiting factor was the memory size of the virtual machine.

4.3.2.1 Vehicle Setup

For a newly constructed vehicle to be able to issue emission reports, a setup process needs to take place which, in short, initialises its internal SSI agent by providing it with an appropriately formatted VC. In the scenario at hand, this flow takes place between the vehicle's manufacturer, which in SSI terminology plays the role of the credential issuer, and each produced vehicle, which in SSI terminology plays the role of the Credential Holder. A depiction of this flow is presented in the diagram below, along with a description of its involved steps.

Figure 26: CERTH Vehicle Verifiable Credential Issuance



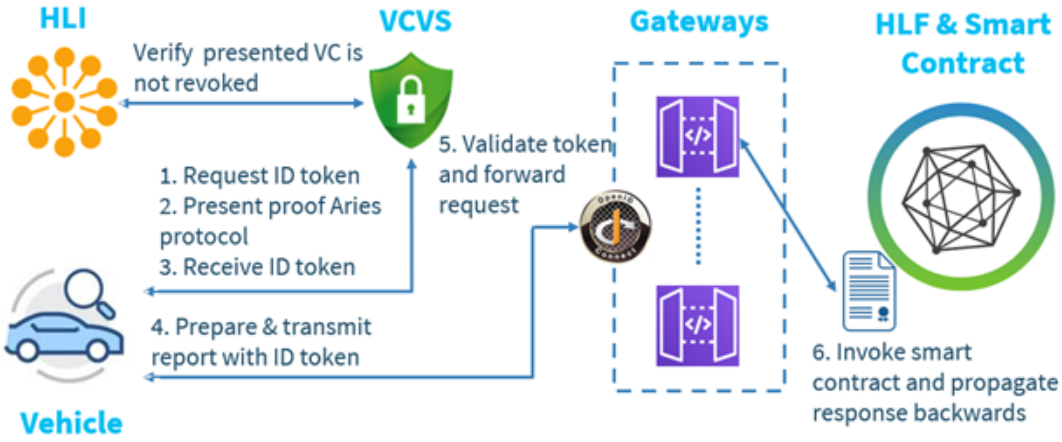
Source: CERTH, 2021.

The first step of this flow establishes a peer-to-peer, private DID-based connection between the vehicle's SSI agent and that of the manufacturer. Note that this process does not require the involvement of any other component, i.e., not even the Hyperledger Indy network, which is a testament to its pure peer-to-peer and scalable nature. The outcome of this step is the establishment of a secure and private communication channel between these two entities. The second step employs this secure communication channel to issue a VC to the vehicle that it can use, during its live operation (discussed in the following section), to prove the validity of its identity, as part of its emission report submission. The issued credential is composed of attributes that are relevant to vehicles, such as its VIN, model, fuel type, type rating, weight, a vehicle controlled DID, the identifier of the Original Equipment Manufacturer (OEM), and others.

4.3.2.2 Live Operation

Following the proper initialisation of a vehicle's software components, it can commence what is coined as its live operation, i.e., the process of periodically submitting emission reports on the Hyperledger Fabric network and, more specifically, on the respective smart contract. An overview of this flow is presented in the diagram below.

Figure 27: Live Operation Flow of Vehicle Interaction with Identity Management System on HLA and HLI communicating with HLF Data Provenance System



Source: CERTH, 2021.

As a starting point, each vehicle interacts with the VCVS by requesting the issuance of a valid OpenID token. In turn, the VCVS responds with a challenge, which is essentially a Hyperledger Aries proof request payload. The vehicle's client application inputs the proof request to its local SSI agent, who is responsible for completing all the involved steps of the protocol with the VCVS. If the proof request protocol terminates gracefully, the VCVS will issue an OpenID token to the vehicle. Currently, the lifetime, i.e., validity period of the issued JWTs is set to five minutes, which constitutes a standard value for this parameter. Consequently, this part of the vehicle emission report submission flow happens infrequently, which as a result provides for increased scalability.

Once in possession of a valid OpenID JWT, the vehicle's client application prepares the emission report, attaches the JWT on the appropriate HTTP header (Authorisation bearer) and issues an HTTP POST request on the appropriate REST endpoint. On receipt of the request, the JWT is processed by the API gateways and, if found to be valid, is forwarded upstream to the load balanced smart contract gateways. In turn, the smart contract gateway instance that receives the request invokes the appropriate function of the vehicle emissions smart contract that is deployed on top of the Hyperledger Fabric network. Assuming a happy path scenario, the contracts accept the emission report and respond with a success message, which is propagated, in a backwards fashion, to the vehicle's client application.

4.3.3 Results

With the experimental setup for pilot 3, 20 virtual vehicles were successfully simulated. Each vehicle is represented by its SSI agent and the simulated client program as described in Live Operation workflow subsection 4.3.2.2. For the whole duration of the experiment, each vehicle was sending a request with randomly generated emissions data every 50 milliseconds. With these parameters and having a steady throughput, it was observed that for both the Hyperledger Indy and the Hyperledger Fabric networks were stable without any sign of bottleneck.

With the development of this proof of concept, it was demonstrated that it is feasible to integrate the functionalities provided by Hyperledger Indy, Hyperledger Aries and Hyperledger Fabric. The integration was possible with the use of CERTH's custom toolchain that bridges the SSI functionalities of the above systems. To the best of the project team's knowledge, there was no other available solution with this capability at the time of development.

4.3.4 Conclusion

The final third pilot explored the integration of an SSI management system, using the data provenance and integrity attributes that were achieved in pilot 2. The deployed system enables vehicles, the EC and a Member

State to interact and communicate emissions reporting data between two heterogeneous BC systems working in tandem.

The deployment took place at the EPIC infrastructure of the JRC and it is currently running there. Integrating three heterogeneous systems with the development of a custom gateway that allows the different components to harmoniously interact in an efficient way, was challenging from a technical point of view, especially since there was no native communication offered by the Hyperledger ecosystem. However, the outcome was successful, and the project was fully operational; it was demonstrated the viability of an SSI Vehicle Identity Management System with HLF Data Provenance. It was showed that the existing BC ecosystem, combined with the necessary tools, is capable of creating a fully BC based emissions monitoring solution. As the main goal of the system setup was to demonstrate the project's feasibility, the setup has not yet been scaled up. The project team and their collaborators from CERTH are nonetheless confident that in the future *"we will be able to demonstrate that this solution can accommodate the whole EU vehicle fleet"*.

4.3.4.1 Next Steps

Having successfully deployed the PoC for pilot 3 for a single Member State organisation sets the tone for any future work.

Naturally, the initial work would be to expand the solution to 27 Member States. There is the need to explore how that will affect the performance of the system and understand the resource requirements for such a deployment. The project team and their collaborators from CERTH plan to not only increase the number of Member States in the network but also increase the number of simulated clients and verify stability under increased load.

Moreover, as in pilot 2 EPIC's capabilities to emulate multiple topologies will be exploited, in order to emulate a geographically distributed network where both the Hyperledger Fabric and Hyperledger Indy nodes are spread across multiple geographically distributed data centres. In addition, it will also be attempted to try and recreate real world situations such as where vehicle clients are connected to the system over a mobile network by introducing latency, bandwidth restrictions and packet loss. Moreover, multiple client configurations where the SSI agent will live on the edge in the vehicle will be tested, as well as tests where the SSI agent is cloud based.

Finally, as in pilot 2, it is the aim to use a realistic model for what concerns the everyday use of vehicles. It is planned to use the already identified studies (Paffumi et al., 2018) that indicate the distribution of vehicles across the week, indicating peaks and drops in mobility traffic.

5 Integration of BC in Tolling and Taxation – Possible Future Pilot Scenarios.

The three pilot studies undertaken were a first step in investigating different combinations of complex systems using BC4T and how they would fit into a regulatory and societal framework. Technological advances and the need to comply with legislation can lead to future innovation and stimulate new ideas about future research scenarios; however, there must be cohesion across the EU and adopted transportation systems, together with tolling and taxation, in the different countries. In fact, Pilot study 3 could spur a broad number of applications both of policy relevance, such as pollutant-based taxation and tolling, and user-oriented utilities based on self-sovereign identity solutions.

This section explores the use of taxation and tolling systems in relation to road usage, vehicle types, and congestion to spurring on possible future research scenarios. The chapter also provides some first insights on the possible relevance of a BC based emissions trading scheme for road vehicles. The latter concept could reflect a fuel tagging approach as foreseen in the recent EC proposal for the inclusion of the road transport sector in the EU emissions trading system (ETS) or a direct extension of the fuel consumption monitoring concept presented in Pilot 2.

The following paragraphs summarise the main findings of a fully detailed desktop review launched for the purpose. The detailed review focusing on Tolling and Taxation in Transport can be found in the Annex 6section giving all the details of tolling systems and methods, tolling technologies, and Tolling Directives and Regulations.

5.1 Tolling and Taxation in Transport

Tolling and taxation in transport are multifactorial, determined by fiscal policies, infrastructure maturity and even more complex ones when considering cross-border transport work. Moving forward, the proliferation of electric/connected vehicles, the mandates for climate action globally, and the availability of new key enabling technologies are expected to affect policy making, taxation harmonisation and interoperability. The European Union in particular, is already working on policies and directives to facilitate the interoperability of electronic road toll systems and facilitating cross-border exchange of information, whilst considering extending the European Emission Trading System (ETS) to cover transport emissions by 2030, in turn affecting national taxing schemes.

5.1.1 Diversity across Europe

Tolling schemes come in various flavours, with each country deciding how they are applied. They are primarily in place to support infrastructural maintenance and financing. Though most countries have tolling systems across their entire highway network, there are cases where they are only applied for certain parts of the infrastructure, like for tunnels in the Netherlands and Montenegro or bridges in Denmark. Another distinction is how tolling fees are applied based on the vehicle type, where pricing may affect all vehicles. Tolling can be increased in some countries based on tonnage (e.g., passenger vehicles vs trucks) or applied solely on heavier vehicles typically transporting goods.

5.1.2 Tolls v Taxation

Tolls are not taxes per se, or at least are not treated as such across the world. Tolls are typically user fees and thus applied for stretches of roads, tunnels, bridges, and other road infrastructures, whilst taxation of vehicles is determined state side. Taxation is commonly applied as Taxes on Acquisition, like registration tax and registration fees, and Taxes on Ownership, typically annual circulation taxes. Each country has its own taxation scheme, and they are based either on a vehicle's base price (ad-valorem based taxes), and/or vehicle type, reflecting engine size, fuel type and fuel consumption. The environmental burden of fuel consumption is also becoming an important factor in refactoring taxation regulations, with each country determining the timing and framework within which adaptations are taking place.

5.1.3 Tolling Systems and Collection Methods

Tolling systems have evolved over the years away from turnpikes and topical constraints to systemic approaches across entire countries. Over time they have proven to be a reliable source of financing for governments implementing such systems, providing the opportunity to extend the construction and support the maintenance of road infrastructures, bridges, tunnels, and roadside facilities. The predictive nature of annual income from tolling systems has not only led to easing the financial burden of governments, via allowing for long term public-private collaborations, has supportive for regional road network development subsidisation, but also in some cases is even considered as a leverage to decongest certain areas, such as city centres, or even reduce

emissions by raising toll fees.

There are three main types of tolling system currently implemented globally; the first two can be based on either manual or electronic fee payment, whereas the last toll system requires electronic payment.

1. **Open toll systems:** comprise mainline toll plazas. They are typically implemented for highway traffic, along predefined distances or geographically (e.g., prefecture based), whereby vehicles are obstructed by barriers, and tolling takes place in various forms, the most common of which is a flat fee per type of vehicle. They are based on manual and/or electronic collection of toll fees.
2. **Closed Toll Systems:** are based on entry and exit tolling. Under a closed toll system, charging is commonly based on distance travelled and/or type of vehicle. They are based on manual and/or electronic collection of toll fees.
3. **Open Road Toll Systems:** can be considered a hybrid between the previous main two systems in terms of tolling schemes. They do not require toll booths or plazas, as they rely on technology to identify vehicles and collect the appropriate fees.

The toll collection methods exercised can be unique in nature or a combination of several methods, depending on the toll system in place. Collection methods are added to the mix as technology is progressively integrated and when toll systems are transitioning to facilitate new externalities in favour of the public, adapt to environmental requirements, or even in compliance with new directives and regulations. The following are the main four modalities identifiable in global road networks:

1. **Manual toll collection:** comprise mainline toll plazas.
2. **Automatic Toll Collections:** is based on the use of Automated Coin Machine (ACM) in a typical plaza-based configuration.
3. **Electronic Toll Collection (ETC):** is based on enabling technologies to identify a vehicle equipped with a valid account accessible via an encoded data tag or transponder as it moves through a toll lane, to then post a debit or charge automatically to the account holder.
4. **Mixed Toll Collection:** is a mix of manual, automatic and/or electronic toll collection can be rolled out in certain transitionary phases of a toll system to ease the unobstructed operation and cashflow to the managing authority or partnership.

Regardless of whether tolling is applied in roadways, tunnels, bridges or other transport infrastructures, the aforementioned systems and methods of collection are applicable and are currently used around the world.

The following sub-section attempts to outline the kind of technologies currently in use per system to map the technological landscape in the field.

5.1.3.1 Tolling Technologies

Tolling is moving fast towards all electronic open road systems, whereby key enabling technologies are leveraged in the transition towards better control, scalability, and adaptability along the lines of a changing landscape, and new imperatives.

5.1.3.1.1 Legacy Toll Collection Technologies

In open and closed systems, manual and automatic toll collection methods are employed. The prerequisite is a decentralised infrastructure of toll plazas and booths, with local equipment and networked with a centralised data centre. The electronics of each booth are subsequently connected to the toll plaza control centre and subsequently all data are fed back to a centralised server, typically at the provider's Network Operations Centre (NOC).

5.1.3.1.2 Electronic Toll Collection Technologies

Electronic tolling technologies used for the charging and pricing schemes are proliferating across and especially promoted within the European Union, via specific Directives, in an effort to harmonise European road networks and systems and help policy making, support sustainable mobility, whilst ensuring road networks can be maintained and extended as per national planning. Some of the main contenders in the field are Dedicated Short-Range Communications (DSRC), Radio Frequency IDentification (RFID), Global Navigation Satellite Systems (GNSS), Automated Number Plate Recognition (ANPR), as well as smartphone embedded technologies.

5.1.4 EU Tolling Directives and Regulations

On the 29^{th} of April 2004, the European Parliament and the Council of the European Union issued Directive 2004/52/EC (EC, 2004) on the interoperability of electronic road toll systems in the Community. The directive had the scope of "laying down the conditions necessary to ensure the interoperability of electronic road toll systems in the Community. It was a complementary directive to the national electronic tolling services in order to ensure cross border interoperability of the then electronic tolling in force, hence did not require any electronic systems to adapt.

The directive, for the first time, officially mandated that all electronic toll systems brought into force on or after the 1^{st} of January 2007, should include the GNSS, GSM/GPRS and DSRC technology stacks, inclusive of the necessary On-Board Units (OBUs), and those tolling services should be interoperable and independent of decisions taken by member states. It went on to address the setup of a European Electronic Toll Service (EETS), the features of the service, the stirring committee (Electronic Toll Committee) and the implementation steps towards standardisation.

Following initial roll outs, the Directive was substantially amended and replace by Directive 2019/520 on the 19^{th} of March 2019 (EC, 2019f). This time it put forward the need for faster EETS deployment in Member states. It stipulated the relevance of the Directive in distanced-based tolling rather time-based tolling, distance, the need for open and public standards to achieve harmonisation across Europe, provided distance from national legal frameworks, put forth the necessary amendments required in support of national EETS providers within competing frameworks as well as to alleviate privacy issues, the use of On-Board Equipment (OBEs) in support of GNSS systems proliferation, whilst made provisions for DSRC and ANPR technologies within national contexts among others.

One of the most important considerations regarded the data exchange of EETS users between Member states, in compliance with applicable data protection regulations, for the first-time mandating data driven toll policy making across Europe. Member states were instructed to adopt and publish the laws, regulations, and administrative provisions in compliance with the Directive by the 19^{th} of October 2021.

This effort led to the adoption of Regulation (EU) 2020/204 on the 28^{th} of November 2019 (EC, 2019d) detailing the obligations of EETS providers in accordance with Directive 2019/520 (EC, 2019f). In general, it created a framework for conformity compliance across the board to ensure the implementation of interoperable standards and processes in tolling systems across Europe.

Meanwhile, Directive 1999/62/EC of the 17^{th} of June 1999 (EC, 1999) adopted a "polluter pays" principle for trucks, buses and vans, via several revisions up to July 2020. According to the action plan proposed all heavy-duty vehicles (trucks, long-haulers) would fall under distance-based road usage charging starting from 2023, whilst light-duty vehicles (vans, buses) will be included from the end of 2027, with passenger cars soon to follow, though not expressly addressed. This effort comes to encourage more environmentally friendly vehicles adoption, and a move away from time-based charging, driving lower CO_2 emissions from road transport.

The importance of a Europe wide interoperable EETS, apart from the strict framework of tolling schemes and cross-border collaboration among EETS providers and Member states, further aligns with the Green Deal goals of lowering emissions from road transport by 2030.

5.1.5 Congestion Charging

Congestion pricing addressed the demand side issues of road usage and was a strategy offered by economists to address traffic congestion, with implementations over the years found exclusively in urban areas, in and around city centres.

The concept of congestion charging addresses externalities, in that demand driven traffic can cause congestion but also increase noise, accident rates, and pollutants, an issue high in today's agenda of climate action. Congestion pricing can be fixed per type of vehicle, variable as in pre-set higher at times of increased congestion times, or dynamic by responding to in real time to traffic conditions. As congestion charging schemes have been increasing over the years, they are classified into four different types: cordon areas which are typically restricted areas within the city centre; area wide congestion pricing applied in wider urban settings; urban toll rings; and corridor or single facility congestion pricing (Cipriani et al., 2019, Vosough et al., 2022, Selmoune et al., 2020).

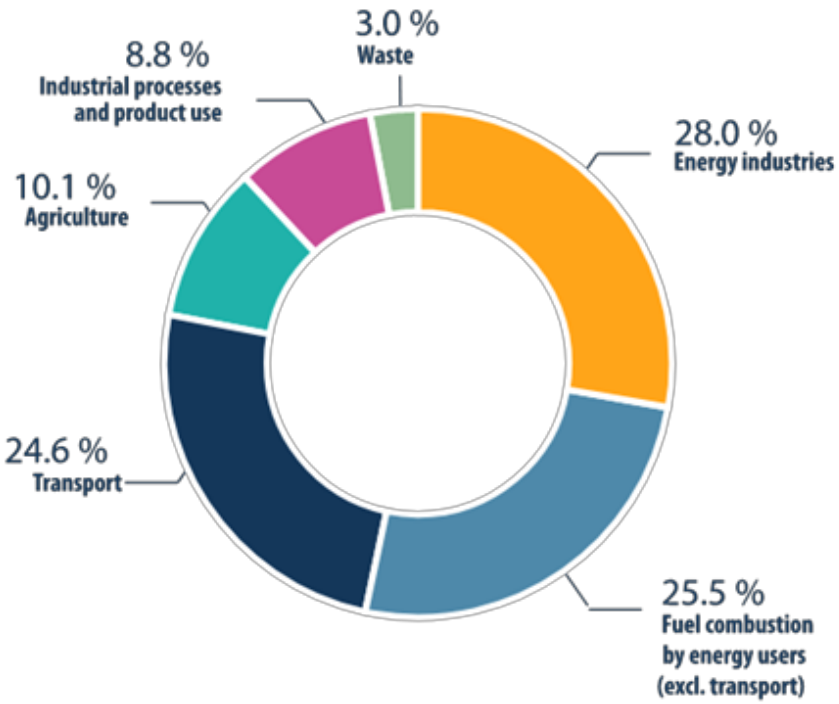
5.2 Emissions trading in the EU

In 1997, the Kyoto Protocol set legally binding emissions reduction targets, or caps, for 37 industrialised countries. Europe was among the first to react with policy instruments to meet the proposed targets, and in 2003 Directive 2003/87/EC (EC, 2021f) was adopted. This led to the setup of the European Emissions Trading System (ETS) in 2005, the world's first international emissions trading system built around a cap-and-trade scheme of CO emissions. After Phase I (2005 to 2007) and Phase II (2008 to 2012), the ETS expanded outside of the EU Member states, established a Union registry replacing national ones, the CO emissions cap was reduced, international trade was facilitated, and the aviation sector was added. Phase III, lasting from 2013 to 2020, more polluting sectors were added, and allowances were set aside for funding new renewable and climate action initiatives. Currently in Phase IV (2021 to 2030) the EU via the ETS is on its way to achieving climate neutrality by 2050 and a 55% reduction in greenhouse emissions by 2030. In addition the EU has set the priority to phase out combustion engine vehicles by 2035, whereby all new vehicles from this date must have zero emission power trains (Parliment, 2022).

5.2.1 Overview of ETS

The European Emissions Trading System (ETS) is the cornerstone system to tackle climate change and is based on a strict 'cap-and-trade' principle. This cap is gradually reduced aiming to reduce total greenhouse gases to 55% in 2030 with respect to 1990's emissions. Total EU greenhouse gas emissions were significantly, and the following infographic sourced by Eurostat outlines the contribution per source in 2018.

Figure 28: EU Greenhouse gas emissions data by source in 2018



Source: (EuroStat, 2018)

Figure 51 also illustrates that transport 2018 figures increased by 9.8% compared to 1990, although 2020 reports show that transport went into a steep decline mainly related to COVID-19 measures.

As the ETS is entering its fourth phase, it is setting more ambitious goals to reduce the emissions to 61% by 2030, almost doubling the targeted emissions reduction from 2.2% annually to 4.2%, whilst also gradually removing the current free allowances for aviation. This is planned to be extended to maritime transport however emissions from fuels used in road transport and buildings will be covered by a new emissions trading mechanism.

5.2.2 Renewable EV charging

Looking forward, one of the main challenges associated to zero-emission vehicles will be the real-time knowledge of the share of renewable energy used during the charging process. Electrification is the major solution

of global road transport decarbonisation efforts. However, currently there is no manner for public authorities and EV drivers to ensure that all the electricity used to charge their vehicles comes from renewable sources. As access to green energy solutions is democratised, the knowledge of this information is highly needed. To address this issue, Energy Web, Vodafone and Mastercard are developing a transparent process for fractionalizing renewable energy allowing anybody to acquire proof that the energy purchased for charging is certifiably from renewable sources. Using a single application with an integrated BC-based mobile wallet, users can also pick the best-priced electricity based on location and charging time, and pay for it automatically making use of e-roaming([3]) solutions. In this concrete case, when an electric vehicle is plugged in, the vehicle and charging station automatically identify themselves using Vodafone's network, while payments for the energy are made using Mastercard's payment gateways. Proof of green charging is sent to the user's smartphone by Energy Web, including the exact origin and energy type (Team, 2022b).

By giving drivers real-time information on the characteristics and compatibility of the nearest available charging point, and carrying out the transaction effortlessly, e-roaming will help to eliminate range anxiety - the fear experienced by EV drivers of running out of battery life. Moreover, it will also allow customers to consciously choose renewable electricity providers.

5.2.3 Trading Road Transport Emissions

The European Green Deal was set out in December 2019, reformulating Europe's commitment to tackle climate and environmental challenges. Within this set of proposals, a new emissions trading system for road transport and buildings (ETS-BRT) was suggested to be brought into force by 2025, along with a Social Climate Fund of €72.2 billion. As greenhouse gases are emitted by households and vehicle owners, the proposed regulated entities are fuel distributors. The timeline suggested is for distributors to report fuel distribution annually starting from 2024 to allow for a data driven cap on emissions to be placed by 2026. The Green Deal framework exercises a direct pressure to innovate, driving new technological advancements in the automotive industry, as well as new lower emission fuels in the market.

5.3 Vehicles as Identities

All vehicles have their unique Vehicle Identification Number (VIN). It is composed of 17 characters imprinted on the engine and other parts of a vehicle, which not only act as a "fingerprint" but also convey a vehicle's features and specifications. VIN can be used to track a vehicle's history, from manufacturing and registration to warranty and insurance. In essence, this asset has an enriched identity. Unfortunately, this identity is subject to fraud via removal, tampering, and cloning and liability can be attested to dealerships or even owners.

The issue of correctly identifying a vehicle is the cornerstone of tolling systems, whereby VIN is encoded to OBUs. Auto manufacturers are obliged to provide a VIN database for toll providers to access and subsequently correctly classify a vehicle for tolling pricing. This would mean that vehicles (and drivers) can be identified across road networks, provided VIN and license plates match, and the appropriate charges can be applied. Identification becomes even more important under the new EETS framework, where information must be shared across toll providers, borders, and jurisdictions.

Conversely, this also raises privacy concerns (Clarke and Wigan, 2011, Ghosh and Mahesh, 2016). Agreements to ensure data privacy are not yet fully aligned with the rollout of EETS systems, whilst ANPR and GNSS allow the recognition or continuous tracking of drivers but do not provide for user privacy. DSRC and RFID do not require continuous tracking, yet personal data are required for the system to operate accordingly. Privacy issues as such are part of EETS adoption and do not account for vehicles travelling outside of tolled infrastructures. Meanwhile, ownership taxation across Europe and most of the world, one way or the other, is based CO_2 emissions.

Moving to a future carved by environmental policies, with fuel prices destined to rise, inevitably requires charges and taxes to be (a) equitable and (b) respectful of data privacy. This means technological solutions must be provided or complemented to address both issues at once. An application specific overlay should stand to address in the best possible manner the widespread vehicles' usage, within national tolled road networks, congestion-based operated cities, and facilities, as well as cross-border charging and exchange of information. These solutions should ensure that distance travelled, or otherwise each individual's or company's impact on infrastructures and the environment, is accounted for across all activities, without sacrificing privacy.

([3]) means the exchange of data and payments between the operator of a recharging or refuelling point and a mobility service provider from which an end user purchases a recharging service (Proposal for a Regulation on Alternative Fuels Infrastructure)

5.4 BC based Tolling and Taxation

One such solution could be the application of BC technology or Distributed Ledger Technology, to be more precise. Its uses and advantages are investigated at a European level via the European BC Partnership (EBP) (EBP, 2022,EBSI, 2017) *"an initiative to develop an EU strategy on BC and build a BC infrastructure for public services"*. Current work is focused on building the European BC Services Infrastructure (EBSI) to facilitate cross-border collaboration under *"five key principles: public good, governance, harmonisation, open-source and compliant with EU regulations"*(GDPR, eIDAS, etc.). EBSI is conceived based on implementing a Self-Sovereign Identity model for Europe, creating trusted digital audit trails, automating compliance checks, proving data integrity, and supporting secure data sharing among European governments, businesses and individuals. Thus far, 25 live BC nodes have been established across EU Member states, with 11 nodes in the setup phase.

Research also supports the use of BC in privacy-preserving tolling architectures (Bartolomeu et al., 2020), as well as in conjunction with IoT and AI technologies to support distributed intelligence (**?**). The use of the technology has been investigated for Norway's Autopass (Repo, 2019), whereby the conducted literature review and design science methodology applied, found a public permissioned BC architecture feasible within the scope of Autopass' multi-stakeholder setting. More extensive research conducted in 2019 for the Ministry of Transport and Digital Infrastructure (Fridgen et al., 2019) in Germany on the opportunities of BC in mobility and logistics found the technology a suitable candidate for toll charging, and other uses moving towards an electric vehicle future, though it needs to be subject to regulations. The use of BC technology is also investigated as part of a wider energy (Wang and Su, 2020) point of view, especially e-mobility (Andoni et al., 2019), from the auto manufacturers perspective (Fraga-Lamas and Fernández-Caramés, 2019), or even the insurance field (Lamberti et al., 2018) as an enabler of dynamic or on-demand coverage.

Considering the work being carried out, it would not be farfetched to see EBSI and EETS working in tandem to promote the use of the technology as the basis of an interoperable, privacy preserving mechanism to allow electronic toll system harmonisation across Europe, support congestion schemes, and distance-based charging or taxation, by creating BC based wallets, acting as OBUs. In light of this, this report proposes a top-level architecture to address a multi-tenant construct accessible by the disparate entities comprising the tolling and taxation landscape.

Considering that vehicles are not readily equipped with BC enabled OBUs, that tolling, and taxation is already regulated at national and EETS level, and that distance-based charging is to become a reality in subsequent years, the proposed architecture is based on smartphones acting as OBUs considering their higher processing power and availability.

Within this proposed architecture, the following elements are included:

- **BC wallet OBU:** Drivers are to be equipped with a mobile app that binds them with the vehicle. The app should be GNSS and potentially DSRC enabled to foster positioning information and allow for enforcement and verification of a vehicle's true positioning. The driver or company's identity and the vehicle could be hashed and exported to an off-chain database or databases, depending on the ETS provider, ensuring privacy of individuals is preserved, whilst non-identifiable data can be exported directly. Distance based usage can be fostered via correlating positioning data with the hashed driver/vehicle information. A payment process is to be included in the app to allow for charging of the road user be it on toll roads or other charging zones, at the appropriate rate.
- **ANPR and DSRC Road-Side Readers (RSE)s:** The enforcement or verification mechanisms are to be addressed by ANPR or DSRC technologies against off-chain data, to preserve privacy where possible.
- **BC network:** A BC network architecture will be key for fostering the necessary smart contracts and interact with the mobile app in terms of identity management and hashing processes, communicating anonymised transactional payloads to the off-chain database/s. Smart contracts should address all transactional activities between drivers and the regulators, drivers and the toll system by monitoring positioning, distance and speed monitoring, cross border ETS traversing, providers the BC network, providers and drivers, providers and the off-chain database/s, as well as provision for consent mechanisms and disclosure in case of violations or any unlawful actions among others.
- **Multi-stakeholder ecosystems:** These ecosystems will be verified against the BC network to access the appropriate APIs and be able to access, under an anonymisation framework, off-chain data for post processing, charging and enforcement. Regulators will be able to issue registrations and ownership taxation based on real measurements and standards for emissions, vehicle type approval and distance travelled annually. Whilst ETS providers can access data to allow for all ITS processes to take place and

ensure road network management, location based smart contracts will allow for provider hand-over across ETS systems and jurisdictions.

— **Congestion charging zones:** This architecture empowers cities to roll-out quickly congestion charging schemes based on positioning and potentially time-based access to the required inner-city zones, single facilities, or ring roads. This process can easily be facilitated by service providers with initial investment in infrastructure.

— **Mobile data providers:** As with EETS OBUs, mobile data providers or mobile operators will be part of the overall ecosystem providing not only the communication channels but potential building on 5G deployments to create value added services for drivers, regulators and toll system providers.

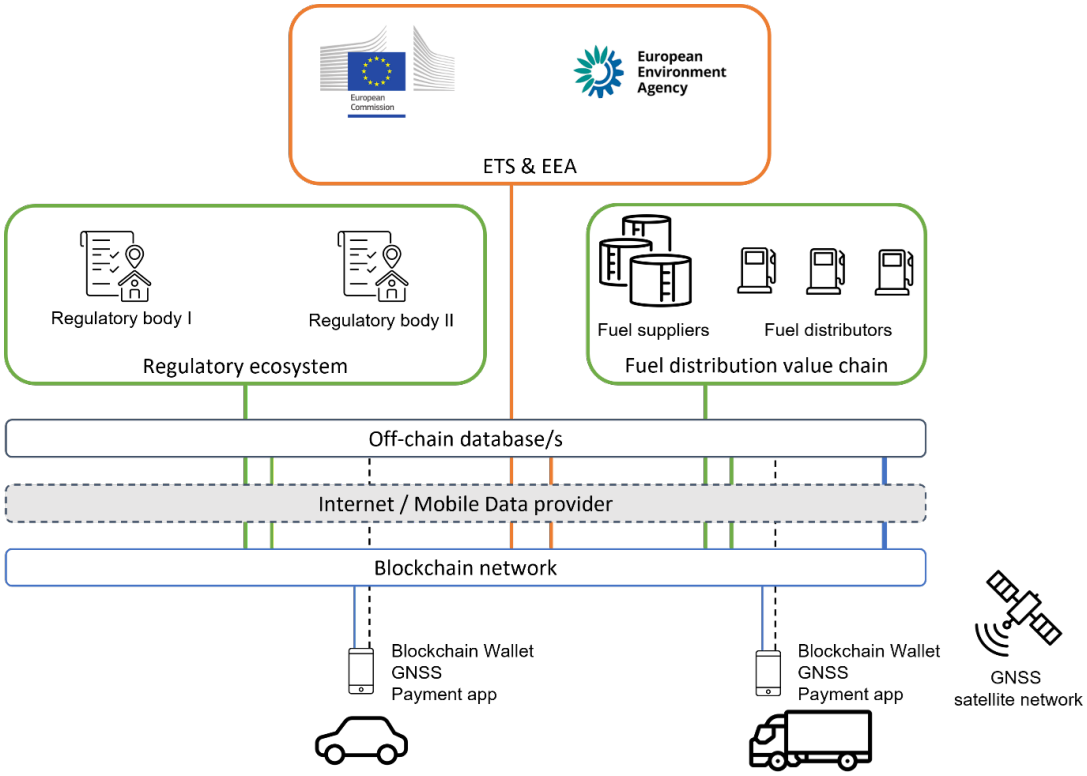
The proposed architecture assumes that such a BC network can be accepted by all interested parties, and it must be regulated at national as well as European level to come into force. Another major assumption is the use of smartphones, although this proposition addresses a potential proof of concept of such an implementation. A more robust schema would be for BC wallets to be fully integrated into vehicles by auto manufacturers or through the provision of open-source IoT devices that can run a wallet and interface with the vehicles On-Board Computer System, replacing the VIN identification codes, extending a vehicle to a cyber-physical entity.

The realisation of such an architecture could be based on the currently, under development EBSI framework, whereby vehicle digital wallets could be elaborated to interact with the infrastructure as well as the owners or individuals driving them. This would solidify the significance of the EBSI framework and drive support for future developments.

5.4.1 BC Technology and ETS

Extending the aforementioned framework, it could also encompass fuel distribution from the suppliers to the distributors and subsequently the drivers. With Fit for 55 focused on fuel distributors, and fuel prices destined to increase, one can identify a gap in equitable monitoring and taxation in both road transport, and buildings.

Figure 29: Architecture extension for fuel distribution in road transport



Source: JRC, 2022.

As with tolling and taxation Figure 53 provides a proposed extension of the architecture to incorporate fuel distribution. With new fuels researched and rolled out in the market, and the possibility of lower CO_2 emitting fuels or even net-zero fuels (et al, 2021) hitting the market over the coming years, taxation based on emissions

and type approval will no longer be an equitable way to address externalities. Meanwhile, such an architecture could provide the European Emissions Trading System and the European Environmental Agency with immutable monitoring data that can be time and location relevant, leveraging the same technology substrate as for EETS and the EBSI, as well as augmenting it to encompass transactions between suppliers, distributors, and vehicle owners. Additionally, the proposed BC enabled implementation is also backed by research to address not only processes but also battle fraudulent attempts. Consequently, data will empower the Social Climate Fund and national governments to exercise data driven policies and aid distribution.

For fuel suppliers and distributors to come into play, application specific implementations will be supported by the BC network at a software and/or IoT level, facilitating transactions with incorporated metadata for fuel type, CO_2 content, fuel quantity and other important parameters. The BC implementation can then provide an immutable digital audit trail from suppliers to consumption of fuels, along with enriched metadata on consumption conditions (speed, emissions, locality etc). In turn, this would facilitate regulators to tax accordingly in a more equitable manner becoming of the real-world conditions.

5.4.1.1 Proposed Implementation Platforms

A Distributed Ledger framework of choice for proof-of-concept implementation would be currently based on Hyperledger Fabric (Hyperledger, 2022a). TradeLens, the logistics sector platform supported by IBM and Maersk, demonstrates similarities with its structuring around the Fabric framework. The platform is a testament to the possibility of DLTs to support complex ecosystems whereby multiple organisations can be supported, data spill over can be avoided, and permissioned management can be facilitated. Another rationalisation is that EBSI incorporates Hyperledger Fabric in its core architecture hence any implementation could be easier adapted to the EBSI framework of services if needed (EBSI, 2022a).

Drivers or other clients can have access to smart contracts through applications. Each organisation needs to maintain one or multiple applications that interpret its business logic and provide the ability to clients to send transaction requests to the smart contracts by verifying their identities. Organisation administrators, which in the proposed proof of concept could be the regulators, are the only ones authorised to register clients in the organisation by issuing the appropriate client keys and certificates by using the corresponding Certificate Authority.

Overall, Hyperledger Fabric is a framework versatile enough to support a proof-of-concept moving forward. It has been proven to work in demanding global logistic environments, where the participating ecosystems include customs from various countries, logistics providers, shipping companies and harbour services. In other words, it is a proven framework that can be adequately adapted to work in complex ecosystems and across borders, which largely characterises road transport as well. In the second phase of this research work, a system level architecture will be elaborated, and a proof-of-concept example solution will be implemented.

5.5 Pilot Scenario Outline: Blockchain Based, Green Fuel Auditing and Certification

Applying BC solutions in the transport sector has value and a large potential impact in the transport sector. For example, to calculate the emissions-based "cost", will depend not only on the amount of fuel used but also how green that fuel was. The new certification scheme for renewable and low carbon fuels is part of the revisions to the renewable energy directive, RED II (EC, 2021i). To demonstrate how sustainability certification of green fuels can be achieved via a BC-based supply chain tracking system the following end-to-end outline of such a scenario has been performed, starting from the fuel producing side of the value chain, the fuel distributors, and gas stations, working its way down to the truck drivers traversing large distances where tolling, and re-fuelling are to be expected. It briefly includes an exporter and importer example to allow for understanding how transport work emissions may be reported across supply chains, as well as the relevant authorities involved.

To this end the following entities were foreseen as members of the complex and multi-stakeholder environments relevant to transport work:

Table 5: Actors within the proposed pilot scenario outline for Green Fuel Auditing and Certification

Fuel Production & Distribution	Biomass supplier	Biofuel Supply Chain
	Biomass distributor	
	Biofuel producer	
	Crude oil supplier	Diesel Supply Chain
	Crude oil distributor	
	Diesel producer	
Fuel Supply & Distribution	Fuel supplier	Fuel Distribution Supply Chain
	Fuel distributors A, B, C	
	Gas stations A, B	
Transport Work	Driver	Transport Work Supply Chain
	Importer	
	Exporter	
Toll Service Providers	Toll Providers A, B	Toll Service Provision Stakeholders
	Congestion Toll Provider	
Authorities & Organisations	Vehicle Tax Authority	Authorities & Organisations Ecosystem Stakeholders
	Emissions Trading System	

Source: JRC, 2022

Before diving into the steps taken within the frame of the use case, it is important to outline that a hypothetical BC4T blockchain service is considered to be in place, providing open APIs for ERP systems and IoT devices integration, in support of different systems and devices as well as all disparate stakeholders active in the proposed fuel production, distribution and auditing value chain.

5.5.1 Fuel Production & Distribution

The envisioned use case starts at the Biomass Supplier (for example, Rapeseed supplier). The biomass produced is loaded to a Biomass Distributor's truck, which is then unloaded to the Biofuel Provider in charge of extracting oil/liquefying the biomass and transforming it into biofuel. The main assumption at this stage is that the biomass load quantity is measured at the loading/unloading docks and subsequently reported via the ERP systems of the relevant stakeholders connected with the BC4T blockchain ecosystem.

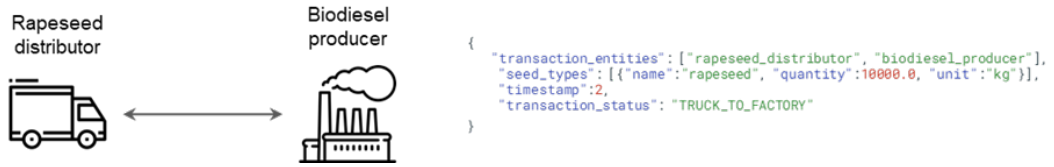
Figure 30: Biomass supplier to distributor transaction

Source: JRC, 2022.

The above transactions indicate that quantities are know for the production and distribution of biomass production. This could provide secondary benefits in national or connected international economies in terms of monitoring and potentially subsidising production of biofuel-oriented crops.

Subsequently the Biofuel Producer loads the Fuel Distributor's tanker vehicle to fulfil the Fuel Supplier's demands in biofuel. The transaction can potentially include a Certificate of renewable % of the biofuel content, as might be the case. The assumptions in this case are that fuel type is know in the tank, M2M connectivity at pump to tank exists, and that distributor's emissions are not taken into account in this use case. External services may exist which can issue the Certificate of renewable % content.

Figure 31: Biomass distributor to biofuel producer transaction



Source: JRC, 2022.

At this point in the use case, it is known that the Fuel Supplier's tank holds a known quantity of biofuel with an equally known % of renewable biofuel, i.e., the amount of natural biofuel in the mix.

A similar case applies to producing diesel quantities from crude oil sources, as follows:

Figure 32: Biofuel producer to fuel distributor transaction

Source: JRC, 2022.

And subsequently satisfying the Fuel Supplier's demands in diesel quantities, along with the required certification if applicable:

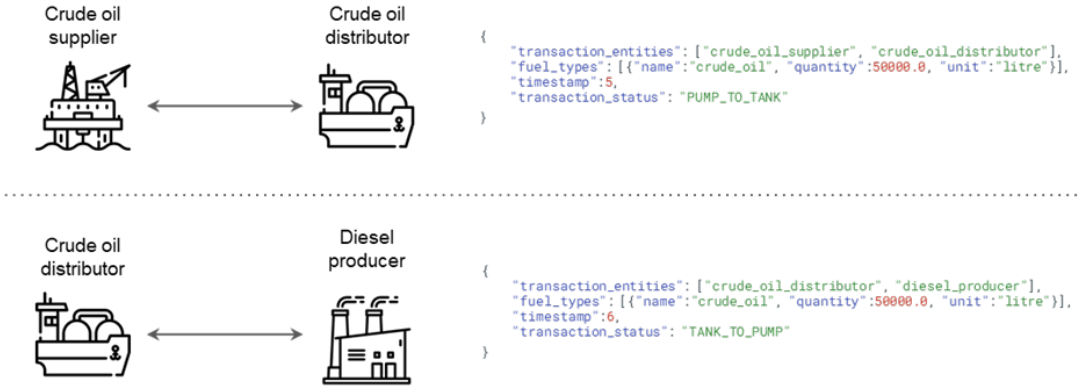
Figure 33: Fuel distributor to fuel supplier transaction

Source: JRC, 2022.

At this point the Fuel Suppliers are accountable and can be audited as far as the fuel types and quantities they provide to their regional or national markets.

A similar case applies to producing diesel quantities from crude oil sources, as follows:

Figure 34: Crude oil supplier to diesel producer supply chain transactions



Source: JRC, 2022.

And subsequently satisfying the Fuel Supplier's demands in diesel quantities, along with the required certification if applicable:

Figure 35: Diesel producer to fuel supplier supply chain transactions

Source: JRC, 2022.

At this point the Fuel Suppliers are accountable and can be audited as far as the fuel types and quantities they provide to their regional or national markets.

5.5.2 Fuel Supply & Distribution

With the upstream supply of fuels to the Fuel Supplier the downstream distribution to Gas Stations can take place. In the examined scenario the Fuel Supplier loads a Fuel Distributor's tanker vehicle, which proceeds to satisfy the Gas Station's demand in fuel. It is assumed that either ERP entries can be transacted or even more programmatically M2M connectivity at pump to tank exists. It is also assumed at this point that distributor's emissions are not considered and that the renewable content is already calculated for biofuel_mix by the Fuel Supplier.

Figure 36: Fuel supplier to gas station supply chain transactions

Source: JRC, 2022.

5.5.3 Transport Work & Tolling

With the upstream and downstream distribution of fuels already addressed, the scenario now focuses on transport work conducted, a typical use case in modern supply chains. Starting with a truck Driver connecting with a truck and going to a Gas Station, the truck states are logged (transacted) always on start/stop engine with fuel data and distance travelled updated each time. At this point it is assumed that the fuel type and quantity currently in the truck's tank is known based on past transactions and calculations and/or IoT data. In this example VIN data is used to tag the truck that performs the transport work, although equally SSI standards can be used instead, such as each truck having a DID associated to them. In fact, every IoT device and every entity in the supply chain would have a DID. In this report the benefits of having a digital twin that incorporates SSI frameworks have already been covered (the so called Self-Sovereign Digital Twin (SSDT)), for simplicity purposes VIN was used in this scenario outline, but for implementing this use case making use of SSI standards by having every entity associated to a DID is highly advised.

Figure 37: Start/stop truck state transactions

Source: JRC, 2022.

The Driver logs the state of the truck at engine start and after 400km travelled stopping to refuel logs the new state on engine stop, transacting distances and fuel consumption along the way appending the truck details that can support secondary calculations of emissions or other data points needed. This assumes that other services can have access to the transactional payloads as required, which will become more evident later in this scenario. More particular in refuelling it is important to reiterate the fuel mix as it affects emissions calculations among others. In this scenario fuel types are considered to be consumed proportionally, although other algorithmic approaches can be taken.

Figure 38: Refuelling and fuel mix transactions

Source: JRC, 2022.

The truck Driver then arrives at the Exporter to load goods. The truck states are logged always on start/stop engine. It is considered that in a supply the last truck state is also logged for supply chain emissions monitoring and reporting purposes (e.g., for Scope 3([4]) emissions reporting under the GHG protocol), thus the Exporter's ERP is connected to the BC4T services for transactional logging.

Figure 39: Driver loads goods from exporter's premises, truck states are transacted.

Source: JRC, 2022.

Leaving the Exporter's premises a truck Driver needs to transverse large distances to deliver goods, bound to implicate toll provision services. The following figure indicates such a case. It is assumed that entry location is instigated under a geofencing (mobile phone app), GNSS, and/or ANPR technology supported schema.

([4]) GHG Protocol Corporate Accounting and Reporting Standard (https://ghgprotocol.org/corporate-standard)

Figure 40: Driver to toll provider entry transaction

Source: JRC, 2022.

Transacting the truck state on toll area entry, is important as it can allow the toll providers to include emissions into pricing their services. This practise can incentivise the uptake on new low emission automotive technologies or penalise the lack thereof and lead to greener supply chains.

Figure 41: Emissions based toll pricing transactions

Source: JRC, 2022.

This scenario can be extended in more complex cases where a Driver enters a tolled area under a particular fuel mix in the tank, refuels within the tolled area and then exits under a different fuel mix. Transacting the states on engine start/stop, or other conditions envisaged, provides accurate data, and thus supports fairer pricing policies.

Figure 42: Tolled area entry on fuel mix A

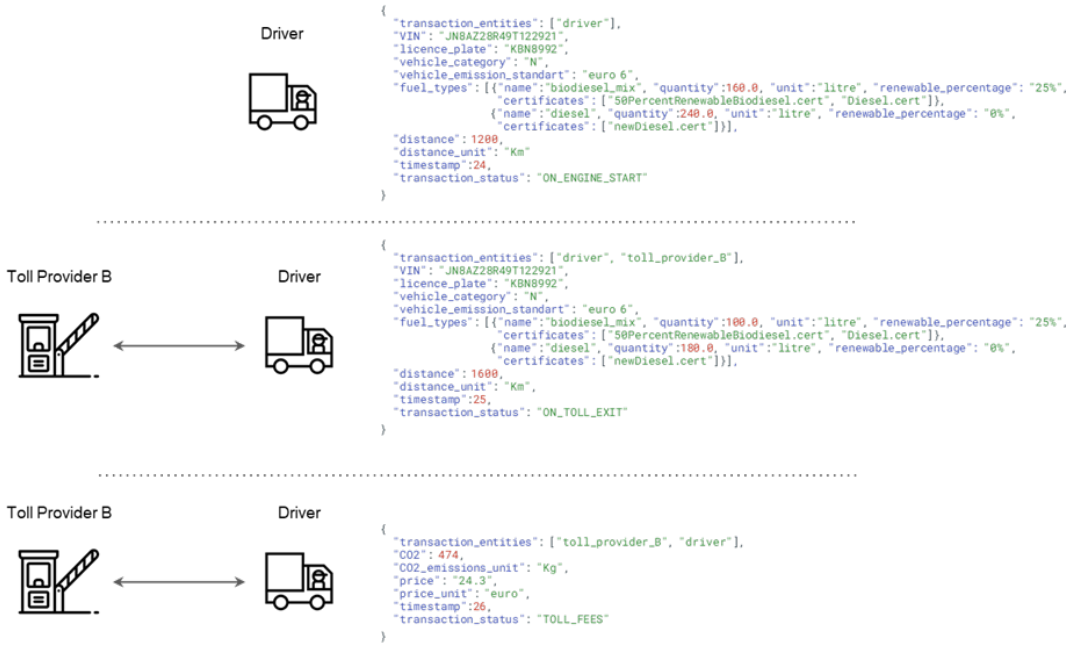
Source: JRC, 2022.

This scenario can be applied in any kind of tolled conditions, be it highway tolls or congestion tolling as in the following figure.

Figure 43: Refuelling within tolled area

Source: JRC, 2022.

Figure 44: Tolling price respecting entry and exit fuel mix changes



Source: JRC, 2022.

Figure 45: Driver to congestion toll provider transaction

Source: JRC, 2022.

Assuming the Driver enters a congestion tolled area to reach the designated Importer and deliver goods, under the current scenario the truck state is transacted to both Importer and Exporter with total fuel quantities consumed (per type) and distance travelled (for the transport work). The level of data granularity may be aligned to supply chain needs and be supported by a) supply chain functionality (i.e., application specific smart contracts) and b) emissions calculations that can take place off-chain and facilitate scope3 reporting for each stakeholder.

Figure 46: Transacting emission data within a supply chain

Source: JRC, 2022.

On congestion tolled area exit, in a similar manner to regular highway tolling, pricing can take place based on emissions and potentially other factors such a time of day, distance etc.

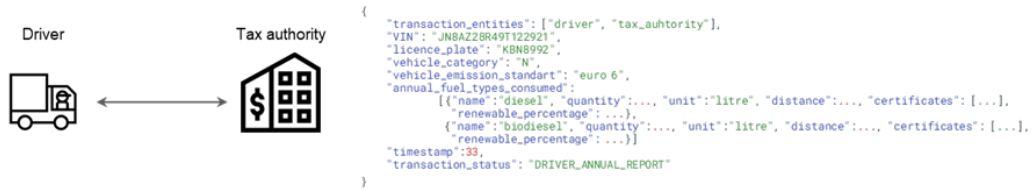
Figure 47: Congestion tolling charges transactions

Source: JRC, 2022.

5.5.4 Authorities & Organisations

Moving away from daily routines and transactional interaction, data collected on emissions from each entity can serve authorities and other organisations in transforming taxation into a data driven process. As an example, the truck Driver may report annually the fuel types and quantities consumed as well as annual distance travelled to the relevant vehicle tax authorities. The reporting could be more granular based on direct access to full truck logs. The relevant assumption of course is that the vehicle tax authority is an entity in the BC4T blockchain network and has access to external services and databases that allow calculations of total emissions for tax pricing purposes.

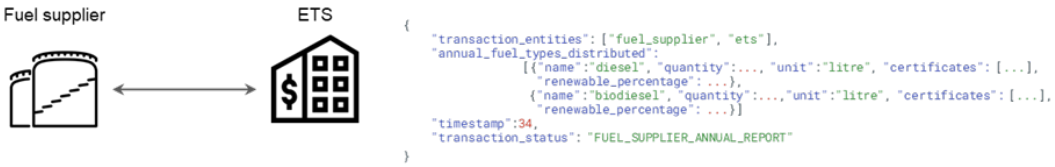
Figure 48: Annual driver to vehicle tax authorities transaction of total fuel consumption



Source: JRC, 2022.

The Fuel Suppliers may similarly report annually the fuel types and quantities distributed to the European Emissions Trading System (ETS), and/or national authorities. The reporting could be more granular based on direct access to full Fuel Suppliers' logs. The ETS would stand to benefit from the reporting depth and avoid greenwashing practises.

Figure 49: Fuel supplier to ETS transaction of fuel types and quantities distribution



Source: JRC, 2022.

The same goes for Gas Stations (or Gas Stations' owners) who may be required to report annually the fuel types and quantities distributed to the Emissions Trading System (ETS). The reporting could be more granular based on direct access to full Gas Stations' logs.

5.5.5 Conclusion of Proposed Pilot Scenario Outline

The proposed use case scenario it outlines end-to-end logging and subsequently facilitates auditing from fuel production to consumption. At its core it simply addresses the logging of how fuels traverse the value chains and is based on transactional logs of how fuel is distributed and consumed. Apparently open APIs for integrating ERP systems, IoT devices and even manual entries would be required. In addition, secondary off-chain services could surface as B2B or even B2C offerings working on analysing and handling the transactional payloads to allow for toll pricing calculations, emissions-based taxation, emissions-based public or private tendering for 3rd party logistics, 3rd party auditing, GHG reporting and many other applications.

EU organisations can facilitate blockchain powered passports/wallets, in a similar manner that the European Blockchain Service Infrastructure is now experimenting with educational certification wallets. Such solutions can serve the EU's Green Agenda and the future scope of the European Emissions Trading System, by onboarding market stakeholders even faster to the process of greening Europe and battling climate change.

5.6 Conclusions on Tolling, Taxation and ETS

Tolling and taxation of vehicles is undergoing a major shift in technologies and processes. The new EETS framework drives cross-border interoperability and leads the way to regulatory and technological harmonisation among EU Member states. In parallel, the Green Deal imperatives are extending the European Emissions Trading System to incorporate more market players and address more sectors, among which the road transport. Secondary efforts include the shift from time-based to distance-based tolling, which although affects heavy and light weight vehicles, paves the way to more equitable tolling, and taxation policies in the future.

Although the technological substrates are there, they are disjointed and do not foster an all-encompassing regulated environment at both EU and national levels. New paradigms are needed to showcase interoperability at large, reduce infrastructural needs and support standardisation. EETS, EU ETS and EBSI can work in tandem to regulate common interfacing between disparate actors and value chain stakeholders. Distributed Ledger technologies could provide this common interface under a privacy preserving prism. This report is part of the work conducted to identify the potential of, and to pilot BC based implementations as an additional enabler to the ecosystem of solutions proposed for the transport sector.

6 Conclusions

On the 3^{rd} of June 2021, the Commission presented its vision, targets, and avenues to achieve a successful digital transformation of Europe by 2030. A detailed policy plan was set out as being critical to achieving the transition towards a climate neutral, circular, and resilient economy. They further stated that *"The EU's ambition is to be digitally sovereign in an open and interconnected world, and to pursue digital policies that empower people and businesses to seize a human centred, sustainable and more prosperous digital future"* (EC, 2021e).

BC allows large groups of people and entities to reach an agreement, permanently store immutable information and thus digitise trust. By creating trust online, BC provides the infrastructure for a more fair, inclusive, secure and democratic digital economy; this characteristic of BC technology has significant implications on how people think about many of our economic, social and political Institutions, including Transportation.

There is currently no production ready Self-Sovereign Identity (SSI) management platform available in the market. However, if platforms like Polygon ID stick to their indicated roadmap, then there will be a production ready SSI platform by the end of 2022. The pilot studies carried out and reported in this report are one small part of what must be done to finally validate the use of BC not only in transport, but also in all aspects of our daily lives.

This report investigated the technical requirements and solutions for applying BC in transport applications, and in particular:

- To gather know-how on BC technology for the automotive and road transport sectors.
- To provide a policy relevant overview of the status in the development and deployment of BC implementations regarding road vehicles.
- To conceptualise prototypes linked to ongoing JRC policy support activities (i.e. digital identity, vehicle fuel consumption and emissions monitoring) serving as the basis for future research on these topics.
- To develop computer simulation and analysis tools necessary to test BC systems' applicability and likely performance for the above mentioned and possibly other future implementations.

In this context, the following Pilot cases were carried out:

1. Pilot 1: **Piloting an EU based vehicle identity management system based on SSI** and MS Vehicle Registration Authorities interacting with the EC. Developing a standardised system for identity management is the first step in implementing accurate digital Monitoring or tracking of transactions. Currently, there are no production ready decentralised solutions for SSI management. In this pilot, MOBI and the EU Commission tested the performance and scalability of Citopia and the ITN.
    - **Result:** It was found that the resultant performance was a magnitude of order faster than needed for example in the emissions monitoring scenario.
2. Pilot 2: **Evaluation of sharing CO_2 emissions from vehicles to a BC-based system** would be technically feasible and secure with the current available technological solutions. A vehicle fleet of 280 million vehicles was considered, interacting with 27 Member States, having the legal obligation to transmit once per year their CO_2 emissions to the EC. To ensure a realistic simulation, the study spread the reporting of the vehicles amongst 27 Member States, each one of them performing the full life cycle of connecting to the platform, discovering services, authenticating, sending the transaction, and disconnecting.
    - **Result:** With these parameters a maximum throughput of 257 transactions per second was achieved, with the system being steady and responsive. In addition, the project team developed a custom solution. This process had not only helped the project team to better understand the internal BC mechanisms, but it also led us to completely automate the deployment procedure, thus facilitating the execution of many experiments with different parameters. With recent upgrades, preliminary performance results of experiment 2 are very promising, with a fivefold increase in TPS on the new EPIC cluster. This massive increase is believed to be due to the use of SSDs which not only have much more storage space but have extremely fast read and write speeds when compared to the old disks used that were not solid-state. This new performance results is preliminary and needs to be verified in detail, afterwards it will be published in the form of a journal publication, to show that the bottleneck was arising from the storage disks and not the upgraded RAM and CPUs.

3. Pilot 3: **Exploring the implementation of combining the previous two use-cases, while also exploring a different SSI framework.** The final pilot which explored the fusion of pilot 1, use of a SSI management system, in combination with the data provenance and integrity attributes, achieved in pilot 2. The implementation and deployment of such as system is by far the most technically challenging part of such a study.

    — **Results:** The project team and their collaborators from CERTH have developed a fully working system that validates the solution approach from a functional viewpoint. These results will be published in a peer reviewed journal in collaboration with ITI. However, the new system for pilot 3 has only been deployed on the JRC infrastructure, so the next step is to run the performance simulations to give an idea of how feasible, resources and costs would be for this system is in normal operating and more realistic conditions.

4. Case study: **A case study was explored to review the current state of road tolling, taxation, and emissions trading system.** A high-level exploration followed on how BC technology can help reshape them and possible future applications of relevance to the EU and end users. The EC is currently working on policies and directives related to adopting interoperable electronic road toll systems and enabling cross border information exchange. Although the technological substrates are there, they are disjointed and do not foster an all-encompassing regulated environment at both EU and national levels.

    — **Result**: It was found that DLTs could provide this common interface under a privacy preserving prism. This report (printed in full in the Annex) is part of the work conducted to identify the potential of, and pilot BC based implementations as an additional enabler to the ecosystem of solutions proposed for the transport sector. This included a detailed outline of a proposed pilot scenario to provide green fuel certification via a BC-based, upstream and downstream supply chain tracking system.

Considerations must be made that the chosen DLTs are somewhat difficult to deploy considering the developing phases of implementation, maintenance, and orchestration. The personnel must be trained to participate in all three phases as the requirements are specific to each of the phases. This extends to the deployment of Smart Contracts to execute of the functionalities in these phases. This does not mean Hyperledger was a bad choice, although the use of other BC technologies such as Ethereum might have been easier to implement and deploy. The current SSI Frameworks on other ledgers, such as Ethereum and Polygon, are in a less advanced state and further away from a production ready state – although research and development of frameworks on other ledgers are advancing fast and could be production ready in the near future.

The pilot studies demonstrated that the approach chosen was technically feasible, and furthermore, connecting the BC system developed at the JRC on Hyperledger Fabric, in communication with another heterogeneous BC system built on Hyperledger Aries and Indy that deals with the SSI management, was a significant success as Hyperledger has no native way to connect these BC systems. The central issue is how to protect the entity (individual, object or association) in regards to data integrity and provenance.

The BC4T study also demonstrated that the use of BC based SSI frameworks does put users in control of their own data and identity. By the very nature of SSI frameworks, users are per se in full control of the generation of their own decentralised identity. This study also helps to demonstrate that the recommendations laid out by the proposal for a Regulation amending eIDAS and extending it to include a European Digital Identity and Wallet, is feasible and necessary, if we are to achieve the EC' goal to enter fully into a pan-European Digital Decade. As for eGovernment services, using BC to decentralise selected services would enable each Member State to manage their own services securely.

In addition, this report further demonstrated the capabilities of using a tamper resistant ledger for data integrity and provenance, leading to increased security, and removing single points of failure. Validating the use of BC for transport applications would be one small step towards achieving a full interoperability across heterogeneous systems across EU27. This report documents this work to achieve progress in realising the EU's ambition is to be digitally sovereign in an open, resilient, and interconnected world, taking Europe into the Digital Decade.

References

'Architecture · polkadot wiki," 2019.; last accessed march of 2021'. a. URL https://wiki.polkadot.network/docs/en/learn-architecture.

'Baseline-protocol; last accessed march of 2021'. URL https://docs.baseline-protocol.org/.

'Cardano (ada); last accessed march of 2021'. URL https://www.cardano.org/.

'Chorusone tendermint light client; last accessed march of 2021'. URL https://github.com/ChorusOne/tendermint-light-client.

'Cosmos: A network of distributed ledgers, e. buchman and j. kwon.; last accessed march of 2021'. a. URL https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md.

'Cosmos network (atom); last accessed march of 2021'. b. URL https://www.cosmos.network/.

'Decentralised identity foundation, 'universal resolver'; last accessed march of 2021'. URL https://dev.uniresolver.io/.

'G. wood, "polkadot: Vision for a hetrogeneous multi-chain framework," 2016.; last accessed march of 2021'. b. URL https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf.

'Hyperledger aries; last accessed march of 2021'. a. URL https://www.hyperledger.org/use/aries.

'Hyperledger avalon; last accessed march of 2021'. b. URL https://www.hyperledger.org/use/avalon.

'Hyperledger besus; last accessed march of 2021'. a. URL https://www.hyperledger.org/use/besu.

'Hyperledger burrow; last accessed march of 2021'. b. URL https://www.hyperledger.org/use/hyperledger-burrow.

'Hyperledger cactus; last accessed march of 2021'. a. URL https://www.hyperledger.org/use/cactus.

'Hyperledger caliper; last accessed march of 2021'. b. URL https://www.hyperledger.org/use/caliper.

'Hyperledger cello; last accessed march of 2021'. c. URL https://www.hyperledger.org/use/cello.

'Hyperledger explorer; last accessed march of 2021'. URL https://www.hyperledger.org/use/explorer.

'Hyperledger-fabric; last accessed march of 2021'. a. URL https://github.com/hyperledger/fabric#releases.

'Hyperledger fabric; last accessed march of 2021'. b. URL https://www.hyperledger.org/use/fabric.

'Hyperledger grid; last accessed march of 2021'. URL https://www.hyperledger.org/use/grid.

'Hyperledger-indy; last accessed march of 2021'. a. URL https://github.com/hyperledger/indy-node#about-indy-node.

'Hyperledger iroha; last accessed march of 2021'. b. URL https://www.hyperledger.org/use/iroha.

'Hyperledger quilt; last accessed march of 2021'. URL https://www.hyperledger.org/use/quilt.

'Hyperledger sawtooth; last accessed march of 2021'. URL https://www.hyperledger.org/use/sawtooth.

'Hyperledger transact; last accessed march of 2021'. URL https://www.hyperledger.org/use/transact.

'Hyperledger ursa; last accessed march of 2021'. URL https://www.hyperledger.org/use/ursa.

'Interledger protocol; last accessed march of 2021'. URL https://interledger.org/.

'Kylin network; last accessed march of 2021'. URL https://kylin.network/.

'Litentry network and whitepaper link; last accessed march of 2021'. a. URL https://www.litentry.com/.

'Litentry network docs; last accessed march of 2021'. b. URL https://docs.litentry.com/introduction/protocol.html.

'Merkle patricia tree; last accessed march of 2021'. URL https://eth.wiki/en/fundamentals/patricia-tree.

'Polkadot (dot); last accessed march of 2021'. c. URL https://www.polkadot.network/.

'Polygon (matic); last accessed march of 2021'. d. URL https://polygon.technology/.

'Quorum 101blockchains.com; last accessed march of 2021'. URL https://101blockchains.com/quorum-blockchain-tutorial/.

'Soverin, identity for all, the inevitable rise of self-sovereign identity; last accessed march of 2021'. URL https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

'Tendermint; last accessed march of 2021'. URL https://github.com/tendermint/tendermint.

'Understanding merckle trees; last accessed march of 2021'. URL https://101blockchains.com/merkle-trees/.

'Understanding the ethereum tree; last accessed march of 2021'. URL https://easythereentropy.wordpress.com/2014/06/04/understanding-the-ethereum-trie/.

'uport identity; last accessed march of 2021'. URL https://www.uport.me/?ref=hackernoon.com.

'Vitalik, "ethereum sharding faqs"; last accessed april of 2022'. URL https://eth.wiki/sharding/Sharding-FAQs.

'Xdai chain (stake); last accessed march of 2021'. URL https://xdaichain.com/.

'Chronicled demosmquorummblockchain integration at eea launch event; last accessed april of 2021'. 2017. URL https://www.econotimes.com/Chronicled-demos-Quorum-blockchain-integration-at-EEA-launch-event-565505.

'Hyperledger cactus wiki; last accessed march of 2022'. 2022. URL https://github.com/hyperledger/cactus/blob/main/whitepaper/whitepaper.md.

'Skale network (skl); last accessed march of 2022'. 2022. URL https://skale.network/.

Abraham, A., Theuermann, K. and Kirchengast, E., 'Qualified eid derivation into a distributed ledger based idm system', In '2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)', pp. 1406–1412. .

Abraham, M., Aithal, H. and Mohan, K., 'Blockchain and collaborative intelligence based next generation smart toll application', In '2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)', IEEE, pp. 206–207.

ACEA, 'European automobile manufacturers association, acea, tax guide 2021; last accessed april of 2022'. 2021. URL https://www.acea.auto/files/ACEA_Tax_Guide_2021.pdf.

ACEA, 'Vehicles in use europe 2022; last accessed april of 2022'. 2022. URL https://www.acea.auto/files/ACEA-report-vehicles-in-use-europe-2022.pdf.

Allen, C., 'The path for self-soverign identity; last accessed march of 2021'. 2016. URL http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Alliance, R., 'Rain allaince, rfid; last accessed april of 2022'. 2022. URL https://rainrfid.org/.

Alupotha, J., 'The rise of self-sovereign identity - hyperledger indy"; last accessed april of 2022'. 2018. URL https://wso2.com/blog/research/the-rise-of-self-sovereign-identity-hyperledger-indy/.

Amiri, M. J., Agrawal, D. and El Abbadi, A., 'On sharding permissioned blockchains', In '2019 IEEE International Conference on Blockchain (Blockchain)', pp. 282–285. .

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P. and Peacock, A., 'Blockchain technology in the energy sector: A systematic review of challenges and opportunities', *Renewable and Sustainable Energy Reviews*, Vol. 100, 2019, pp. 143–174. ISSN 1364-0321. . URL https://www.sciencedirect.com/science/article/pii/S1364032118307184.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y. et al., 'Hyperledger fabric: a distributed operating system for permissioned blockchains', In 'Proceedings of the thirteenth EuroSys conference', pp. 1–15.

Androulaki, E., De Caro, A., Neugschwandtner, M. and Sorniotti, A., 'Endorsement in hyperledger fabric', In '2019 IEEE International Conference on Blockchain (Blockchain)', pp. 510–519. .

Ashur, T. and Dhooghe, S., 'Marvellous: a stark-friendly family of cryptographic primitives'. Cryptology ePrint Archive, Report 2018/1098, 2018. https://eprint.iacr.org/2018/1098.

Bagchi, A., 'Conflicting nationalisms: the voice of the subaltern in Mahasweta Devi's Bashai Tudu', *Tulsa Studies in Women's Literature*, Vol. 15, No 1, 1996, pp. 41–50.

Barger, A., Manevich, Y. and Meir, H., 'Hardening permissioned blockchains with verifiable randomness', In '2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)', pp. 1–5. .

Bartolomeu, P. C., Vieira, E. and Ferreira, J., 'Pay as you go: a generic crypto tolling architecture', *IEEE Access*, Vol. 8, 2020, pp. 196212–196222.

Belchior, R., Vasconcelos, A., Guerreiro, S. and Correia, M., 'A survey on blockchain interoperability: Past, present, and future trends', *arXiv preprint arXiv:2005.14282*, 2020.

Ben Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M., 'Zerocash: Decentralized anonymous payments from bitcoin', In '2014 IEEE Symposium on Security and Privacy', pp. 459–474. .

Benzel, T., 'The science of cyber security experimentation: the deter project', In 'Proceedings of the 27th Annual Computer Security Applications Conference', pp. 137–148.

blockchair, 'Ethereum charts, transaction per second; last accessed april of 2022'. 2022. URL https://blockchair.com/ethereum/charts/transactions-per-second.

Blonk, W. A., 'Fair payment for infrastructure use: White paper of the european commission'. In 'Social Costs and Sustainable Mobility', Springer, 2000. pp. 7–13.

Brousmiche, K. L., Heno, T., Poulain, C., Dalmieres, A. and Hamida, E. B., 'Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned', In '2018 9th IFIP international conference on new technologies, mobility and security (NTMS)', IEEE, pp. 1–5.

Buck, R., 'In the future, anything that can be connected will be"; last accessed april of 2022'. 2017. URL http://www.norfolknetwork.com/future-anything-can-connected-will/.

Buterin, V., 'Chain interoperability; last accessed april of 2022'. 2016. URL https://allquantor.at/blockchainbib/pdf/vitalik2016chain.pdf.

Byrne, M., 'Polkadot is ready for a big 2022; last accessed april of 2022'. 2022. URL https://www.fool.com/investing/2022/01/04/polkadot-is-ready-for-a-big-2022/.

Callas, J., Donnerhacke, L., Finney, H. and Thayer, R., 'Rfc2440: Openpgp message format'. 1998.

Cameron, K., 'The laws of identity', *Microsoft Corp*, Vol. 12, 2005, pp. 8–11.

Cao, Y. and Yang, L., 'A survey of identity management technology', In '2010 IEEE International Conference on Information Theory and Information Security', IEEE, pp. 287–293.

Cardano, 'Cardano | docs; last accessed may of 2022'. 2022. URL https://docs.cardano.org/.

Castro, M. and Liskov, B., 'Practical byzantine fault tolerance and proactive recovery', *ACM Transactions on Computer Systems (TOCS)*, Vol. 20, No 4, 2002, pp. 398–461.

Castro, M., Liskov, B. et al., 'Practical byzantine fault tolerance', In 'OSDI', Vol. 99. pp. 173–186.

Cazzola, P. and Lassman, J., 'Decarbonising air transport: acting now for the future', 2021.

CHAISE, 'Chaise blockchain skills for europea; last accessed may of 2022'. 2022. URL https://chaise-blockchainskills.eu/.

Cipriani, E., Mannini, L., Montemarani, B., Nigro, M. and Petrelli, M., 'Congestion pricing policies: Design and assessment for the city of rome, italy', *Transport Policy*, Vol. 80, 2019, pp. 127–135.

Clarke, R. and Wigan, M., 'You are where you've been: The privacy implications of location and tracking technologies', *Journal of Location Based Services*, Vol. 5, No 3-4, 2011, pp. 138–155.

Clima, E. D., 'Effort sharing 2021-2030: targets and flexibilities; last accessed april of 2022'. 2021. URL https://ec.europa.eu/clima/eu-action/effort-sharing-member-states-emission-targets/effort-sharing-2021-2030-targets-and-flexibilities_en.

CNBC, 'More than $320 million stolen in latest apparent crypto hack; last accessed may of 2022'. 2022. URL https://www.cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html.

Coindesk, 'Axie infinity's ronin network suffers $625m exploit; last accessed may of 2022'. 2022. URL https://www.coindesk.com/tech/2022/03/29/axie-infinitys-ronin-network-suffers-625m-exploit/.

Commission, E., 'Smart cities. cities using technological solutions to improve the management and efficiency of the urban environment.; last accessed april of 2022'. 2018. URL https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en.

Commission, E., Centre, J. R., Kourtesis, D. and Fontaras, G., 'Collection of fleet-wide fuel and energy consumption data from road vehicles : investigation of a possible vehicle-to-cloud communication system for anonymous data collection', 2022. .

Consortium, W. W. W. et al., 'Verifiable credentials data model 1.0: Expressing verifiable information on the web', *https://www. w3. org/TR/vc-data-model/?# core-data-model*, 2019.

Cooper, D., 'Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile; last accessed april of 2022'. 2008. URL https://www.ietf.org/rfc/rfc5280.txt?

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W. T. et al., 'Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile.', *RFC*, Vol. 5280, 2008, pp. 1–151.

Cosmos, 'Cosmos | docs; last accessed may of 2022'. 2022. URL https://docs.cosmos.network/.

Dabrowski, M. and Pacyna, P., 'Generic and complete three-level identity management model', In '2008 Second International Conference on Emerging Security Information, Systems and Technologies', IEEE, pp. 232–237.

Dal Mas, F., Massaro, M., Verde, J. and Cobianchi, L., 'Can the blockchain lead to new sustainable business models?', *Journal of Business Models*, Vol. 8, 07 2020a, pp. 31–38. .

Dal Mas, F., Massaro, M., Verde, J. M. and Cobianchi, L., 'Can the blockchain lead to new sustainable business models?', *Journal of Business Models*, Vol. 8, No 2, 2020b, pp. 31–38.

Deloitte, 'Connected and autonomous vehicles. accelerating the future movement of people and goods"; last accessed april of 2022'. 2021. URL https://www2.deloitte.com/us/en/pages/consumer-business/solutions/connected-and-autonomous-vehicles-solutions.html.

djboris9 et al, 'hlfabric-k8scc, chaincode launcher and builder for hyperledger fabric on kubernetes; last accessed april of 2022'. 2022. URL https://github.com/postfinance/hlfabric-k8scc/graphs/contributors.

djrtwo, 'Github repo for ethereum 2.0 phase 0 – the beacon chain; last accessed april of 2022'. 2022. URL https://github.com/ethereum/consensus-specs/blob/676e216/specs/phase0/beacon-chain.md#time-parameters.

Dziuba, A., 'Iot in transportation: All you need to know about smart traffic control system using iot"; last accessed april of 2022'. 2020. URL https://relevant.software/blog/iot-in-transportation-smart-traffic-control-system/.

EBP, E. B. P., 'European blockchain partnership, technological and regulatory sandbox; last accessed april of 2022'. 2022. URL https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership.

EBSI, 'Home | ebsi n.d; last accessed april of 2022'. 2017. URL https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home.

EBSI, 'Ebsi architecture, explained.final draft 10/06/2021 ebsi is a market-friendly distributed blockchain network based on open standards and transparent governance model; last accessed april of 2022'. 2021a. URL https://ec.europa.eu/cefdigital/wiki/download/attachments/113541243/%28210610%29%28EBSI_Architecture_Explained%29%28v1.02%29.pdf.

EBSI, 'High-level scope (essif); last accessed april of 2022'. 2021b. URL https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=379913698.

EBSI, 'Ebsi architecture; last accessed april of 2022'. 2022a. URL https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Architecture.

EBSI, 'European ssi framework; last accessed april of 2022'. 2022b. URL https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=379913698&preview=/379913698/379913700/essif-v2.0.png.

EC, 'Ec better regulation, chapter vii guidelines on stakeholder consultation ; last accessed april of 2022'. URL https://ec.europa.eu/info/sites/default/files/better-regulation-guidelines-stakeholder-consultation.pdf.

EC, 'Stakeholder consultation guidelines 2014, public consultation document; last accessed april of 2022'. 2014a. URL https://ec.europa.eu/smart-regulation/impact/docs/scgl_pc_questionnaire_en.pdf.

EC, 'Commission proposes digital identiyt for all europeans; last accessed april of 2022'. 2021. URL https://ireland.representation.ec.europa.eu/news-and-events/news/commission-proposes-digital-identity-all-europeans-2021-06-03_en.

EC, 'Proposal for a regulation of the european parliament and of the council amending regulation (eu) no 910/2014 as regards establishing a framework for a european digital identity'. 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:281:FIN.

EC, E. C., 'Council directive 83/182/eec of 28 march 1983 on tax exemptions within the community for certain means of transport temporarily imported into one member state from another'. 1983. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31983L0182,.

EC, E. C., 'Directive 1999/62/ec of the european parliament and of the council of 17 june 1999 on the charging of heavy goods vehicles for the use of certain infrastructures'. 1999. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0062,.

EC, E. C., 'Directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications)'. 2002. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058.

EC, E. C., 'Standardisation - mandates request m/338; last accessed april of 2022'. 2003. URL https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=216.

EC, E. C., 'Directive 2004/52/ec of the european parliament and of the council of 29 april 2004 on the interoperability of electronic road toll systems in the community'. 2004. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0052,.

(EC), E. C., 'Proposal for a directive of the european parliament and of the council amending directive 2003/87/ec so as to improve and extend the greenhouse gas emission allowance trading system of the community, com (2008) 16 final, brussels, belgium'. 2008.

EC, E. C., 'Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)'. 2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

EC, E. C., 'Commission decision of 6 october 2009 on the definition of the european electronic toll service and its technical elements (notified under document c(2009) 7547)'. 2009a. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0750,.

EC, E. C., 'Commission implementing decision of 13 august 2012 on the approval by the commission of sampling plans for the weighing of fisheries products in accordance with article 60(1) and 60(3) of council regulation (ec) no 1224/2009 and of control plans for the weighing of fisheries products in accordance with article 61(1) of regulation (ec) no 1224/2009'. 2009b. https://eur-lex.europa.eu/eli/dec_impl/2012/474/oj,.

EC, E. C., 'Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec'. 2014b. https://eur-lex.europa.eu/eli/reg/2014/910/oj.

EC, E. C., 'Commission regulation (eu) 2018/1832 of 5 november 2018 amending directive 2007/46/ec of the european parliament and of the council, commission regulation (ec) no 692/2008 and commission regulation (eu) 2017/1151 for the purpose of improving the emission type approval tests and procedures for light passenger and commercial vehicles, including those for in-service conformity and real-driving emissions and introducing devices for monitoring the consumption of fuel and electric energy'. 2018.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1832.

EC, E. C., 'Com(2019) 640 final communication from the commission the european green deal'. 2019a.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN,.

EC, E. C., 'Commission delegated regulation (eu) .../... on classification of vehicles, obligations of european electronic toll service users, requirements for interoperability constituents and minimum eligibility criteria for notified bodies'. 2019b.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com:C(2019)8369,.

EC, E. C., 'Commission implementing regulation (eu) 2019/2072 of 28 november 2019 establishing uniform conditions for the implementation of regulation (eu) 2016/2031 of the european parliament and the council, as regards protective measures against pests of plants, and repealing commission regulation (ec) no 690/2008 and amending commission implementing regulation (eu) 2018/2019'. 2019c.
https://eur-lex.europa.eu/eli/reg_impl/2019/2072/oj.

EC, E. C., 'Commission implementing regulation (eu) 2020/204 of 28 november 2019 on detailed obligations of european electronic toll service providers, minimum content of the european electronic toll service domain statement, electronic interfaces, requirements for interoperability constituents and repealing decision 2009/750/ec'. 2019d.
https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2020%3A043%3ATOC&uri=uriserv%3AOJ.L_.2020.043.01.0049.01.ENG,.

EC, E. C., 'Commission implementing regulation (eu) 2020/204 of 28 november 2019 on detailed obligations of european electronic toll service providers, minimum content of the european electronic toll service domain statement, electronic interfaces, requirements for interoperability constituents and repealing decision 2009/750/ec'. 2019e.
https://eur-lex.europa.eu/resource.html?uri=cellar:a0392e39-1da6-11ea-95ab-01aa75ed71a1.0003.02/DOC_1&format=PDF,.

EC, E. C., 'Directive (eu) 2019/520 of the european parliament and of the council of 19 march 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the union'. 2019f.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.091.01.0045.01.ENG,.

EC, E. C., 'Regulation (eu) 2019/1242 of the european parliament and of the council of 20 june 2019 setting co2 emission performance standards for new heavy-duty vehicles and amending regulations (ec) no 595/2009 and (eu) 2018/956 of the european parliament and of the council and council directive 96/53/ec'. 2019g.
https://eur-lex.europa.eu/eli/reg/2019/1242/oj.

EC, E. C., 'Regulation (eu) 2019/631 of the european parliament and of the council of 17 april 2019 setting co2 emission performance standards for new passenger cars and for new light commercial vehicles, and repealing regulations (ec) no 443/2009 and (eu) no 510/2011'. 2019h.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0631.

EC, E. C., 'Regulation (eu) 2019/631 of the european parliament and of the council of 17 april 2019 setting co2 emission performance standards for new passenger cars and for new light commercial vehicles, and repealing regulations (ec) no 443/2009 and (eu) no 510/2011'. 2019i.
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007R0715.

EC, E. C., 'Commission implementing regulation (eu) 2021/392 of 4 march 2021 on the monitoring and reporting of data relating to co2 emissions from passenger cars and light commercial vehicles pursuant to regulation (eu) 2019/631 of the european parliament and of the council and repealing commission implementing regulations (eu) no 1014/2010, (eu) no 293/2012, (eu) 2017/1152 and (eu) 2017/1153'. 2021a.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0392.

EC, E. C., 'Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions 2030 digital compass: the european way for the digital decade'. 2021b.
https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118,.

EC, E. C., 'European commission, taxation and customs, taxes in europe database v3; last accessed april of 2022'. 2021c. URL https://www.acea.auto/files/ACEA_Tax_Guide_2021.pdf.

EC, E. C., 'European electronic toll service (eets); last accessed april of 2022'. 2021d. URL https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/european-electronic-toll-service-eets.

EC, E. C., 'Europe's digital decade: Commission sets the course towards a digitally empowered europe by 2030; last accessed april of 2022'. 2021e. URL https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983.

EC, E. C., 'Opinion of the european economic and social committee on the proposal for a decision of the european parliament and of the council amending directive 2003/87/ec as regards the notification of offsetting in respect of a global market-based measure for aircraft operators based in the union'. 2021f. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AE4342,.

EC, E. C., 'Proposal for a directive of the european parliament and of the council amending directive 2003/87/ec as regards aviation's contribution to the union's economy-wide emission reduction target and appropriately implementing a global market-based measure'. 2021g. https://op.europa.eu/en/publication-detail/-/publication/049ae7e8-e668-11eb-a1a5-01aa75ed71a1/language-en,.

EC, E. C., 'Proposal for a directive of the european parliament and of the council amending directive 2003/87/ec establishing a system for greenhouse gas emission allowance trading within the union, decision (eu) 2015/1814 concerning the establishment and operation of a market stability reserve for the union greenhouse gas emission trading scheme and regulation (eu) 2015/757'. 2021h. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN,.

EC, E. C., 'Proposal for a directive of the european parliament and of the council amending directive (eu) 2018/2001 of the european parliament and of the council, regulation (eu) 2018/1999 of the european parliament and of the council and directive 98/70/ec of the european parliament and of the council as regards the promotion of energy from renewable sources, and repealing council directive (eu) 2015/652'. 2021i. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0557,.

Eckert, J., López, D., Azevedo, C. L. and Farooq, B., 'A blockchain-based user-centric emission monitoring and trading system for multi-modal mobility*', In '2020 Forum on Integrated and Sustainable Transportation Systems (FISTS)', pp. 328–334. .

EEA, 'Total greenhouse gas emission trends and projections in europe, european environment agency; last accessed april of 2022'. 2021. URL https://www.eea.europa.eu/ims/total-greenhouse-gas-emission-trends.

Eliasson, J., 'Is congestion pricing fair? consumer and citizen perspectives on equity effects', *Transport Policy*, Vol. 52, 2016, pp. 1–15.

Enterprise, A. L., 'The internet of things in transportation build a secure foundation to leverage iot for improved passenger experiences, safety and efficiency"; last accessed april of 2022'. 2020. URL https://www.al-enterprise.com/-/media/assets/internet/documents/iot-for-transportation-solutionbrief-en.pdf.

EPA, 'Smartway program; last accessed april of 2022'. 2021. URL https://www.epa.gov/smartway/learn-about-smartway.

EPP, 'Low-income families and middle class homeowners mustn't pay for green deal, tax guide 2021; last accessed april of 2022'. 2021. URL https://www.eppgroup.eu/newsroom/news/low-income-families-and-home-owners-mustn-t-pay-green-deal.

Ericsson, 'Ericsson mobility report"; last accessed april of 2022'. 2020. URL https://www.ericsson.com/assets/local/reports-papers/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf.

et Accenture, W. E. F. W., 'The known traveller unlocking the potential of digital identity for secure and seamless travel; last accessed april of 2022'. 2018. URL https://www.accenture.com/_acnmedia/pdf-70/accenture-wef-the-known-traveller-digital-identity.pdf.

et al, C.-B., 'hyperledger-landscape; last accessed may of 2022'. 2022. URL https://github.com/hyperledger-landscape/hl-landscape/blob/master/landscape.yml.

et al, E. C., 'Directive 2003/87/ec of the european parliament and of the council of 13 october 2003 establishing a scheme for greenhouse gas emission allowance trading within the community and amending council directive 96/61/ec', *Official Journal of the European Union*, Vol. 50, No 275, 2003, pp. 32–46.

et al, J. L., 'Controllable co_2 electrocatalytic reduction via ferroelectric switching on single atom anchored in2se3 monolayer', *Nature Communications*, Vol. 12, No 1, 2021, pp. 1–10. .

ETS, E., 'Eu emissions trading system (eu ets); last accessed april of 2022'. 2021a. URL https://www.eea.europa.eu/ims/total-greenhouse-gas-emission-trends.

ETS, E., 'Eu emissions trading system (eu ets), market stability reserve; last accessed april of 2022'. 2021b. URL https://ec.europa.eu/clima/eu-action/eu-emissions-trading-system-eu-ets/market-stability-reserve_en.

ETS, E., 'Eu emissions trading system (eu ets), market stability reserve; last accessed april of 2022'. 2021c. URL https://ec.europa.eu/clima/eu-action/eu-emissions-trading-system-eu-ets_en.

EuroParl, 'Legislative train schedule - fit for 55 package under the european green deal?; last accessed april of 2022'. 2020. URL https://www.europarl.europa.eu/legislative-train/theme-a-european-green-deal/package-fit-for-55.

European Commission, E., 'Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions', *A roadmap for moving to a competitive low carbon economy in*, Vol. 2050, 2011.

EuroStat, 'How are emissions of greenhouse gases by the eu evolving?; last accessed april of 2022'. 2018. URL https://ec.europa.eu/eurostat/cache/infographs/energy/bloc-4a.html.

Eyerys, 'Ford, gm, bmw and renault joining blockchain research group; last accessed april of 2022'. 2018. URL https://www.eyerys.com/articles/timeline/ford-gm-bmw-and-renault-joining-blockchain-research-group.

Fedrecheski, G., Rabaey, J. M., Costa, L. C., Ccori, P. C. C., Pereira, W. T. and Zuffo, M. K., 'Self-sovereign identity for iot environments: a perspective', In '2020 Global Internet of Things Summit (GIoTS)', IEEE, pp. 1–6.

Fedrecheski, G., Rabaey, J. M., Costa, L. C. P., Calcina Ccori, P. C., Pereira, W. T. and Zuffo, M. K., 'Self-sovereign identity for iot environments: A perspective', In '2020 Global Internet of Things Summit (GIoTS)', pp. 1–6. .

Ferdous, M. S., Chowdhury, F. and Alassafi, M. O., 'In search of self-sovereign identity leveraging blockchain technology', *IEEE Access*, Vol. 7, 2019, pp. 103059–103079.

for Business Inovation & Skills, H. D., 'Smart cities: Background paper; last accessed april of 2022'. 2013. URL https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246019/bis-13-1209-smart-cities-background-paper-digital.pdf.

for the Space Programme EUSPA, E. U. A., 'What is gnss?; last accessed april of 2022'. 2022. URL https://www.euspa.europa.eu/european-space/eu-space-programme/what-gnss.

Forbes, 'The sharing economy is still growing, and businesses should take note"; last accessed april of 2022'. 2019. URL https://www.forbes.com/sites/forbeslacouncil/2019/03/04/the-sharing-economy-is-still-growing-and-businesses-should-take-note/?sh=62196caf4c33.

Forbes, 'The 5 biggest internet of things (iot) trends in 2021 everyone must get ready for now "; last accessed april of 2022'. 2020. URL https://www.forbes.com/sites/bernardmarr/2020/10/26/the-5-biggest-internet-of-things-iot-trends-in-2021-everyone-must-get-ready-for-now/?sh=ef3d7ee41fd9.

Forbes, 'The 5 biggest connected and autonomous vehicle trends in 2022"; last accessed april of 2022'. 2021a. URL https://www.forbes.com/sites/bernardmarr/2021/12/20/the-5-biggest-connected-and-autonomous-vehicle-trends-in-2022/?sh=17025548525f.

Forbes, 'The role of blockchain in the development of the ev industry; last accessed july of 2022'. 2021b. URL https://www.forbes.com/sites/naveenjoshi/2021/12/21/the-role-of-blockchain-in-the-development-of-the-ev-industry/?sh=7e4f7c2e3862.

Forbes, “mobility as a service’ concept promises to revolutionize transport accessibility”; last accessed april of 2022’. 2021c. URL https://www.forbes.com/sites/gusalexiou/2021/05/23/mobility-as-a-service-concept-promises-to-revolutionize-transport-accessibility/?sh=20f603d57fe6.

Forum, E. B., ‘Blockchain and the gdpr; last accessed april of 2022’. 2018. URL https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

Forum, I. T., ‘Big data and transport’, , No 8, 2015. . URL https://www.oecd-ilibrary.org/content/paper/5jlwvzdb6r47-en.

Foundation, E., ‘Ethereum | docs; last accessed may of 2022’. 2022a. URL https://ethereum.org/en/developers/docs/.

Foundation, E., ‘Ethereum 2.0 | docs; last accessed may of 2022’. 2022b. URL https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/.

Foundation, H., ‘Hyperledger fabric | docs; last accessed may of 2022’. 2022c. URL https://hyperledger-fabric.readthedocs.io/en/release-2.2/.

Foundation, T. L., ‘Review of four hyperledger libraries- aries, quilt, ursa, and transact; last accessed may of 2022’. 2022d. URL https://training.linuxfoundation.org/blog/review-of-four-hyperledger-libraries-aries-quilt-ursa-and-transact/.

Fraga-Lamas, P. and Fernández-Caramés, T. M., ‘A review on blockchain technologies for an advanced and cyber-resilient automotive industry’, *IEEE Access*, Vol. 7, 2019, pp. 17578–17598. .

Fridgen, G., Guggenberger, N., Hoeren, T., Prinz, W., Urbach, N., Baur, J., Brockmeyer, H., Gräther, W., Rabovskaja, E., Schlatt, V., Schweizer, A., Sedlmeir, J. and Wederhake, L., ‘Opportunities and challenges of dlt (blockchain) in mobility and logistics’. May 2019. URL https://eref.uni-bayreuth.de/55481/.

Fynn, E., Bessani, A. and Pedone, F., ‘Smart contracts on the move’, In ‘2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)’, IEEE, pp. 233–244.

G, F., I, N. F., N, A., D, G., R, G., G, J., E, K., I, K., A, L., T, M., G, O., M, S., I, S. and G, S., ‘Blockchain solutions for the energy transition, experimental evidence and policy recommendations’, Scientific analysis or review, Anticipation and foresight KJ-NA-31008-EN-N (online), Luxembourg (Luxembourg), 2022. . URL https://publications.jrc.ec.europa.eu/repository/handle/JRC128651.

Gabay, D., Akkaya, K. and Cebe, M., ‘Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs’, *IEEE Transactions on Vehicular Technology*, Vol. 69, No 6, 2020, pp. 5760–5772. .

Gaia-X, ‘Gaia-x | about; last accessed may of 2022’. 2022. URL https://www.gaia-x.eu/what-is-gaia-x.

Garoffolo, A., Kaidalov, D. and Oliynykov, R., ‘Zendoo: a zk-snark verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains’, In ‘2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)’, IEEE, pp. 1257–1262.

Ghosh, P. and Mahesh, T., ‘A privacy preserving mutual authentication protocol for rfid based automated toll collection system’, In ‘2016 International Conference on ICT in Business Industry & Government (ICTBIG)’, IEEE, pp. 1–5.

Giacomelli, I., Madsen, J. and Orlandi, C., ‘Zkboo: Faster zero-knowledge for boolean circuits’. Cryptology ePrint Archive, Report 2016/163, 2016. https://eprint.iacr.org/2016/163.

GlobalTranz, ‘What is the impact of big data in the transportation & supply chain industries? 11 possibilities with big data”; last accessed april of 2022’. 2016. URL globaltranz.com/big-data-in-the-transportation/.

Gorenflo, C., Lee, S., Golab, L. and Keshav, S., ‘Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second’, In ‘2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)’, pp. 455–463. .

Guan, Z., Wan, Z., Yang, Y., Zhou, Y. and Huang, B., ‘Blockmaze: An efficient privacy-preserving account-model blockchain based on zk-snarks’, *IEEE Transactions on Dependable and Secure Computing*, 2020, pp. 1–1. .

Haddouti, S. E. and Kettani, M. D. E.-C. E., ‘Towards an interoperable identity management framework: a comparative study’, *arXiv preprint arXiv:1902.11184*, 2019.

Hafid, A., Hafid, A. S. and Samih, M., 'Scaling blockchains: A comprehensive survey', *IEEE Access*, Vol. 8, 2020, pp. 125244–125262. .

Hamilton, C. J. and Eliasson, J., 'Vertical separation as means to establish interoperability in road tolling in europe', *Transportation Research Part C: Emerging Technologies*, Vol. 19, No 6, 2011, pp. 1019–1032.

Helm, 'Home page | helm, the package manager for kubernetes; last accessed april of 2022'. 2022. URL https://helm.sh/.

Hileman, G. and Rauchs, M., '2017 global blockchain benchmarking study', *Available at SSRN 3040224*, 2017.

HLF, 'Glossary | hlf docs; last accessed april of 2022'. 2020a. URL https://hyperledger-fabric.readthedocs.io/en/latest/glossary.html.

HLF, 'hyperledger-fabricdocs documentation release master v1.2; last accessed april of 2022'. 2020b. URL https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/release-1.2/hyperledger-fabric.pdf.

HLF, 'hyperledger-fabricdocs documentation release master v1.4; last accessed april of 2022'. 2021. URL https://readthedocs.org/projects/hyperledger-fabric/downloads/pdf/release-1.4/.

Hyperledger, 'Hyperledger blockchain performance metrics white paper; last accessed april of 2022'. 2018. URL https://www.hyperledger.org/learn/publications/blockchain-performance-metrics.

Hyperledger, 'Hlf docs v2.2; last accessed april of 2022'. 2020. URL https://hyperledger-fabric.readthedocs.io/en/release-2.2/ledger/ledger.html.

Hyperledger, 'Hlf docs version release 2.4; last accessed april of 2022'. 2022a. URL https://hyperledger-fabric.readthedocs.io/en/release-2.4/network/network.html.

Hyperledger, 'Hyperledgerfarbic sdk for node.js; last accessed april of 2022'. 2022b. URL https://hyperledger.github.io/fabric-sdk-node/release-2.2/module-fabric-network.html.

IBM, 'Road to the future: Blockchain for transportation mobility; last accessed april of 2022'. 2018. URL https://www.ibm.com/blogs/blockchain/2018/07/road-to-the-future-blockchain-for-transportation-mobility/.

IBM, 'Connected and autonomous vehicle development for travel industry"; last accessed april of 2022'. 2021. URL https://www.ibm.com/blogs/aws/connected-and-autonomous-vehicle-development-for-travel-industry/.

iden3 Team, 'Home | mobi; last accessed april of 2022'. 2022. URL https://iden3.io/.

INATBA, 'International association for trusted blockchain applications (inatba); last accessed may of 2022'. 2022. URL https://inatba.org/.

Institute, M. G., 'Digital identification: A key to inclusive growth"; last accessed april of 2022'. 2019. URL https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

Iota, 'Iota wiki | specifications; last accessed may of 2022'. 2022. URL https://wiki.iota.org/IOTA-2.0-Research-Specifications/6.4Finalization.

Istio, 'Istio, simplify observability, traffic management, security, and policy with the leading service mesh.; last accessed april of 2022'. 2022. URL https://istio.io/.

Jones, J. S., 'Blockchain technologies set to help grow electric vehicle adoption; last accessed july of 2022'. 2018. URL https://www.smart-energy.com/industry-sectors/energy-grid-management/blockchain-technologies-set-to-help-grow-electric-vehicle-adoption/.

Kiayias, A. and Zindros, D., 'Proof-of-work sidechains', In 'International Conference on Financial Cryptography and Data Security', Springer, pp. 21–34.

Kline, E., Bartlett, G., Lawler, G., Story, R. and Elkins, M., 'Capturing domain knowledge through extensible components', In 'International Conference on Testbeds and Research Infrastructures', Springer, pp. 141–156.

Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E. and Ford, B., 'Omniledger: A secure, scale-out, decentralized ledger via sharding', In '2018 IEEE Symposium on Security and Privacy (SP)', IEEE, pp. 583–598.

Kubernetes, 'Home page | kubernetes; last accessed april of 2022'. 2022. URL https://kubernetes.io/.

Kubespray, 'Kubespray deplyer github repo; last accessed april of 2022'. 2022. URL https://github.com/kubernetes-sigs/kubespray.

Lamberti, F., Gatteschi, V., Demartini, C., Pelissier, M., Gomez, A. and Santamaria, V., 'Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage', *IEEE Consumer Electronics Magazine*, Vol. 7, No 4, 2018, pp. 72–81. .

Li, D., Han, D., Weng, T.-H., Zheng, Z., Li, H., Liu, H., Castiglione, A. and Li, K.-C., 'Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey', *Soft Computing*, Vol. 26, No 9, 2022, pp. 4423–4440.

Li, W., Guo, H., Nejad, M. and Shen, C. C., 'Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach', *IEEE Access*, Vol. 8, 2020, pp. 181733–181743. .

Liu, X., Farahani, B. and Firouzi, F. *Distributed Ledger Technology*, Springer International Publishing, Cham. ISBN 978-3-030-30367-9, 2020. pp. 393–431. . URL https://doi.org/10.1007/978-3-030-30367-9_8.

Lopez, D. and Farooq, B., 'A multi-layered blockchain framework for smart mobility data-markets', *Transportation Research Part C: Emerging Technologies*, Vol. 111, 2020, pp. 588–615.

Ma, C., Li, J., Ding, M., Shi, L., Wang, T., Han, Z. and Poor, H. V., 'When federated learning meets blockchain: A new distributed learning paradigm', *arXiv preprint arXiv:2009.09338*, 2020.

MAERSK, 'Maersk, tradelens; last accessed april of 2022'. 2022. URL https://www.maersk.com/apa-tradelens.

Mandaroux, R., Dong, C. and Li, G., 'A european emissions trading system powered by distributed ledger technology: An evaluation framework', *Sustainability*, Vol. 13, No 4, 2021. ISSN 2071-1050. URL https://www.mdpi.com/2071-1050/13/4/2106.

Manevich, Y., Barger, A. and Assa, G., 'Redacting transactions from execute-order-validate blockchains', In '2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)', IEEE, pp. 1–9.

Massiani, J., Marcucci, E., Rotaris, L. and Danielis, R., 'A medium term evaluation of the ecopass road pricing scheme in milan: economic, environmental and transport impacts', *A Medium Term Evaluation of the Ecopass Road Pricing Scheme in Milan: Economic, Environmental and Transport Impacts*, 2012, pp. 49–83.

Mckinsey, 'What every utility ceo should know about blockchain; last accessed july of 2022'. 2018. URL https://www.mckinsey.com/~/media/McKinsey/Industries/Electric%20Power%20and%20Natural%20Gas/Our%20Insights/What%20every%20utility%20CEO%20should%20know\%20about%20blockchain/What-every-utility-CEO-should-know-about-blockchain-web-final.pdf.

Miller, H. J., Shaw, S.-L. et al., 'Geographic information systems for transportation: principles and applications', Oxford University Press on Demand, 2001.

MOBI, 'The new economy of movement, business white paper, mobi; last accessed april of 2022'. 2021. URL https://dlt.mobi/wp-content/uploads/2021/09/MOBI-WP_V3.0.pdf.

MOBI, 'Mobi | about; last accessed april of 2022'. 2022a. URL https://dlt.mobi/about/.

MOBI, 'Mobi | join the community; last accessed april of 2022'. 2022b. URL https://dlt.mobi/join/.

MOBI, 'Mobi technology stack; last accessed april of 2022'. 2022c. URL https://dlt.mobi/mobi-technology-stack/.

Mühle, A., Grüner, A., Gayvoronskaya, T. and Meinel, C., 'A survey on essential components of a self-sovereign identity', *Computer Science Review*, Vol. 30, 2018, pp. 80–86.

Nakamoto, S. and Bitcoin, A., 'A peer-to-peer electronic cash system', *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, Vol. 4, 2008.

Nations, U., 'How blockchain technology could boost climate action; last accessed april of 2022'. 2017. URL https://unfccc.int/news/how-blockchain-technology-could-boost-climate-action.

Nations, U., 'Un supports blockchain technology for climate action; last accessed april of 2022'. 2018. URL https://cop23.unfccc.int/news/un-supports-blockchain-technology-for-climate-action.

Nayak, S., Narendra, N. C., Shukla, A. and Kempf, J., 'Saranyu: Using smart contracts and blockchain for cloud tenant management', In '2018 IEEE 11th International Conference on Cloud Computing (CLOUD)', pp. 857–861. .

New Zealand, E. P. A., 'Liquid fossil fuels, information for owners, importers and large purchasers of liquid fossil fuels such as petrol, jet fuel and fuel oils.; last accessed april of 2022'. 2022. URL https://www.epa.govt.nz/industry-areas/emissions-trading-scheme/industries-in-the-emissions-trading-scheme/liquid-fossil-fuels/.

Ng, H., 'Distributed consensus: Performance comparison of paxos and raft'. 2020.

Observatory, E. B., 'About | eublockchain n.d; last accessed april of 2022'. 2017. URL https://www.eublockchainforum.eu/about.

Observatory, T. E. B., 'Blockchain innovation in europe"; last accessed april of 2022'. 2018. URL https://theblockchaintest.com/uploads/resources/EUBlockchain%20-%20Blockchain%20Innovation%20in%20Europe-Thematic%20Report%20-%202018%20-%20Aug.pdf.

Okwuibe, G. C., Li, Z., Brenner, T. and Langniss, O., 'A blockchain based electric vehicle smart charging system with flexibility**this project is sponsored by oli systems gmbh, stuttgart.', *IFAC-PapersOnLine*, Vol. 53, No 2, 2020, pp. 13557–13561. ISSN 2405-8963. . URL https://www.sciencedirect.com/science/article/pii/S2405896320311241. 21st IFAC World Congress.

Ongaro, D. and Ousterhout, J., 'In search of an understandable consensus algorithm (extended version)'. 2013.

Paffumi, E., De Gennaro, M. and Martini, G., 'European-wide study on big data for supporting road transport policy', *Case Studies on Transport Policy*, Vol. 6, No 4, 2018, pp. 785–802.

Panait, A.-E. and Olimid, R. F., 'On using zk-snarks and zk-starks in blockchain-based identity management', In 'Innovative Security Solutions for Information Technology and Communications', , edited by D. Maimut, A.-G. Oprina, and D. SauveronSpringer International Publishing, Cham. ISBN 978-3-030-69255-1, pp. 130–145.

Parliment, E., 'Vote to amend regulation (eu) 2019/631 on co2 emission standards for cars and vans; last accessed july of 2022'. 2022. URL https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1706841&t=d&l=en.

petermetz et al, 'Hyperledger cactus home; last accessed may of 2022'. 2022. URL https://wiki.hyperledger.org/display/cactus.

Pinto, A. M., 'An introduction to the use of zk-snarks in blockchains', In 'Mathematical Research for Blockchain Economy', , edited by P. Pardalos, I. Kotsireas, Y. Guo, and W. KnottenbeltSpringer International Publishing, Cham. ISBN 978-3-030-37110-4, pp. 233–249.

Polkadot, 'Polkadot | docs; last accessed may of 2022'. 2022. URL https://wiki.polkadot.network/docs/research.

Pollan, M., 'The omnivore's dilemma', Penguin Group, New York, 2006.

Pollitt, M. G., Dolphin, G. G. et al., 'Should the eu ets be extended to road transport and heating fuels?', Tech. rep., 2021.

Poston, T., 'A draft of history', edited by K. A. Hauke, University of Georgia Press, Athens, 2000.

Prometheus, 'Prometheus, from metrics to insight power your metrics and alerting with the leading open-source monitoring solution.; last accessed april of 2022'. 2022. URL https://prometheus.io/.

Puricelli, S., Cardellini, G., Casadei, S., Faedo, D., Van den Oever, A. and Grosso, M., 'A review on biofuels for light-duty vehicles in europe', *Renewable and Sustainable Energy Reviews*, Vol. 137, 2021, p. 110398.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M. and Holt, J., 'Decentralized identifiers (dids) v1.0', *Draft Community Group Report*, 2020.

Repo, A., 'Utilizing blockchain technology in a road toll architecture', 2019.

Reuters, 'Toyota invests in u.s. car-sharing service"; last accessed april of 2022'. 2016. URL https://www.reuters.com/article/us-toyota-carsharing-idUSKCN12S14I.

Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 'On blockchain and its integration with iot. challenges and opportunities', *Future Generation Computer Systems*, Vol. 88, 2018, pp. 173–190. ISSN 0167-739X. . URL https://www.sciencedirect.com/science/article/pii/S0167739X17329205.

Rincon, K., 'General motors launches car-sharing program "maven""; last accessed april of 2022'. 2018. URL https://www.reuters.com/article/us-toyota-carsharing-idUSKCN12S14I.

Robinson, P., 'Consensus for crosschain communications', *arXiv preprint arXiv:2004.09494*, 2020.

Robinson, P., Ramesh, R. and Johnson, S., 'Atomic crosschain transactions for ethereum private sidechains', *Blockchain: Research and Applications*, Vol. 3, No 1, 2022, p. 100030.

Ryu-Shinzaki, 'Github issue: Memory leak when gateway.connect and gateway.disconnect are called repeatedly; last accessed april of 2022'. 2021. URL https://github.com/hyperledger/fabric-sdk-node/issues/529.

Salman, D., 'Faqs | polkadot; last accessed april of 2022'. 2022. URL https://wiki.polkadot.network/docs/faq.

Selmoune, A., Cheng, Q., Wang, L. and Liu, Z., 'Influencing factors in congestion pricing acceptability: a literature review', *Journal of Advanced Transportation*, Vol. 2020, 2020.

Services, I., 'Iota services | about; last accessed may of 2022'. 2022. URL https://www.iota-services.com/what-is-iota/.

Services, O. B., 'Smart cities and digital identity: India's move towards a digital-first future; last accessed april of 2022'. 2018. URL https://www.orange-business.com/en/blogs/smart-cities-and-digital-identity-indias-move-towards-digital-first-future.

Siaterlis, C., Genge, B. and Hohenadel, M., 'Epic: A testbed for scientifically rigorous cyber-physical security experimentation', *IEEE Transactions on Emerging Topics in Computing*, Vol. 1, No 2, 2013, pp. 319–330.

Siemens, 'ehighway – electrification of road freight transport; last accessed april of 2022'. 2021. URL https://www.mobility.siemens.com/global/en/portfolio/road/ehighway.html.

Simoni, M. D., Kockelman, K. M., Gurumurthy, K. M. and Bischoff, J., 'Congestion pricing in a world of self-driving vehicles: An analysis of different strategies in alternative future scenarios', *Transportation Research Part C: Emerging Technologies*, Vol. 98, 2019, pp. 167–185.

Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A. and Choo, K.-K. R., 'Sidechain technologies in blockchain networks: An examination and state-of-the-art review', *Journal of Network and Computer Applications*, Vol. 149, 2020, p. 102471.

Sovrin, 'Sovrin, the inevitable rise of self soveregin identity"; last accessed april of 2022'. 2017. URL https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

Stokkink, Q. and Pouwelse, J., 'Deployment of a blockchain-based self-sovereign identity', In '2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)', IEEE, pp. 1336–1342.

Surname, F., 'JRC technical reports template', Tech. rep., Joint Research Centre, Via Enrico Fermi 2749, Ispra, VA, Italy, Nov. 2015.

Sutton, M., 'Ford's bike share investment bears fruit with bay area launch"; last accessed april of 2022'. 2017. URL https://cyclingindustry.news/fords-bike-share-investment-bears-fruit-with-bay-area-launch/.

Team, C., 'Circom zk toolkit; last accessed april of 2022'. 2022a. URL https://github.com/Fluidex/plonkit.

Team, E. W., 'Renewable ev charging using web 3 technology; last accessed july of 2022'. 2022b. URL https://www.energyweb.org/renewable-ev-charging/.

Team, P., 'Introducing polygon id, zero-knowledge identity for web3; last accessed april of 2022'. 2022c. URL https://blog.polygon.technology/introducing-polygon-id-zero-knowledge-own-your-identity-for-web3/.

Terzi, S., Savvaidis, C., Votis, K., Tzovaras, D. and Stamelos, I., 'Securing emission data of smart vehicles with blockchain and self-sovereign identities', In '2020 IEEE International Conference on Blockchain (Blockchain)', pp. 462–469. .

Terzi, S., Savvaidis, C., Votis, K., Tzovaras, D. and Stamelos, I., 'Securing emission data of smart vehicles with blockchain and self-sovereign identities', In '2020 IEEE International Conference on Blockchain (Blockchain)', IEEE, pp. 462–469.

Thakkar, P., Nathan, S. and Viswanathan, B., 'Performance benchmarking and optimizing hyperledger fabric blockchain platform', In '2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)', IEEE, pp. 264–276.

Times, F., 'Daimler hedges on car-sharing future with turo investment"; last accessed april of 2022'. 2018. URL https://www.ft.com/content/8e32c3ec-9290-11e7-a9e6-11d2f0ebb7f0.

to ITN, M. C., 'Mobi's itn contributors private github repository; last accessed may of 2022'. 2022. URL https://github.com/itn-trust/itn/tree/master/deploy.

torkelo et al, 'Grafana, the open-source platform for monitoring and observability; last accessed april of 2022'. 2022. URL https://github.com/grafana/grafana.

TransUnion, 'Digital identity - a key driver of canada's digital economy"; last accessed april of 2022'. 2018. URL https://www.transunion.ca/blog/digital-identity.

Unal, D., Hammoudeh, M., Khan, M. A., Abuarqoub, A., Epiphaniou, G. and Hamila, R., 'Integration of federated machine learning and blockchain for the provision of secure big data analytics for internet of things', *Computers & Security*, Vol. 109, 2021, p. 102393.

US Department of Transportation, V. C., 'What blockchains could mean for government and transportation operations; last accessed april of 2022'. 2018. URL https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/news/62156/blockchains-government-and-transportationjanuary-2018.pdf.

vehicles, T. C. I. . R., 'Iso 3779:2009 road vehicles — vehicle identification number (vin) — content and structure; last accessed april of 2022'. 2009. URL https://www.iso.org/standard/52200.html.

Vosough, S., de Palma, A., Lindsey, R. et al., 'Pricing vehicle emissions and congestion externalities using a dynamic traffic network simulator', Tech. rep., THEMA (THéorie Economique, Modélisation et Applications), Université de . . . , 2022.

Wang, Q. and Su, M., 'Integrating blockchain technology into the energy sector — from theory of blockchain to research and application of energy blockchain', *Computer Science Review*, Vol. 37, 2020, p. 100275. ISSN 1574-0137. . URL https://www.sciencedirect.com/science/article/pii/S1574013720300241.

WEF, W. E. F., 'What exactly is the sharing economy?"; last accessed april of 2022'. 2017. URL https://www.weforum.org/agenda/2017/12/when-is-sharing-not-really-sharing/.

WEF, W. E. F., '4 key areas where ai and iot are being combined "; last accessed april of 2022'. 2021a. URL https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/.

WEF, W. E. F., 'Self-sovereign identity: the future of personal data ownership?"; last accessed april of 2022'. 2021b. URL https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/.

Wiki, 'Automatic number-plate recognition wiki; last accessed april of 2022'. 2022. URL https://en.wikipedia.org/wiki/Automatic_number-plate_recognition.

Wu, W., Liu, E., Gong, X. and Wang, R., 'Blockchain based zero-knowledge proof of location in iot', In 'ICC 2020 - 2020 IEEE International Conference on Communications (ICC)', pp. 1–7. .

ycharts, 'Ethereum average block time; last accessed april of 2022'. 2022. URL https://ycharts.com/indicators/ethereum_average_block_time.

Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A. and Knottenbelt, W., 'Xclaim: Trustless, interoperable, cryptocurrency-backed assets', In '2019 IEEE Symposium on Security and Privacy (SP)', IEEE, pp. 193–210.

List of abbreviations and definitions

AI Artificial Intelligence

AIP Aries Interoperability Profile

ALB Automatic Lane Barrier

ANPR Automated Number Plate Recognition

API Application Programming Language

AWS Amazon Web Services

BC Blockchain

BC4T Blockchain for Transport

BFT Byzantine Fault Tolerant

BoB Blockchain of Blockchains

CA Certificate Authority

CCTV Closed-Circuit Television

CEN European Committee for Standardisation

CENELEC The European Electrotechnical Committee for Standardisation

CERTH Center for Research and Technology Hellas

CEX Centralised Exchange

CO2 Carbon Dioxide

CPU Central Processing Unit

CSR Certificate Signing Request

DAO Decentralised Autonamous Organisation

Dapp Decenatralised Application

DDo DID Documents

DeFi Decentralised Finance

DEX Decentralised Exchange

DID Decentralised IDentity

DIMS Digital Identity Management Systems

DL Distributed Ledger

DLT Distributed Ledger Technology

DoS Denial of Service

DRIVES Distributed Registry for Intelligent Vehicle Ecosystem Sustainability

DSRC Dedicated Short-Range Communications

EBP European Blockchain Partnership

EBSI European Blockchain Service Infrastructure

EC European Commision

EEA European Environment Agency

EETS European Electronic Toll Service

eID Electronic IDentity

eIDAS electronic IDentification, Authentication, and trust Services

EPIC Experimental Platform for Internet Contingencies

ERC Ethereum Request for Comment

ESSIF European Self-Sovereign Identity Framework

ETS Emission Trading System

ETS-BRT Emission Trading System for Buildings and Road Transport

ETSI European Telecommunications Standards Institute

FEPS Flow Executions Per Second

GB Giga-Bytes

GDP Gross Domestic Product

GDPR General Data Protection Regulation

GHG Green House Gase

GNSS Global Navigation Satellite Systems

GRPC Google Remote Procedure Call

GPS Global Positioning System

HDV Heavy-Duty Vehicle

HLC Hyperledger Cactus

HLF Hyperledger Fabric

HLI Hyperleger Indy

HLQ Hyperledger Quilt

HOT High Occupancy Toll

HTLC Hash Time-locked Contracts

HTTP HyperText Transfer Protocol

IBFT Istanbul Byzantine-Fault Tolerant

IC Issue credential

ID IDentity

IDM IDentity Management

IoT Internet of Things

JRC Joint Research Centre

JWT JSON Web Token

KYC Know Your Customer

LEZ Low Emission Zones

LPS Lane Processor System

MaaS Mobility-as-a-Service

MOBI Mobility Open Blockchain Initiative

MS Member State

MSP Membership Service Provider

MTS MOBI Web3 Technology Stack

MTT MOBI Trusted Trip

NFC Near-Field Communication

NOC Network Operations Centre

NPoS Nominated Proof of Stake

OBE On-Board Equipment

OBFCM On-Board Fuel and/or energy Consumption Monitoring device

OBU On-Board Unit

OEM Original Equipment Manufacturer

PBFT Practical Byzantine Fault Tolerance

PII Personal Identifiable Information

PKC Public Key Certificate

PoC Proof of Concept

PoS Proof of Stake

PoW Proof of Work

RAM Random Access Memory

RBFT Redundant Byzantine Fault Tolerance

REST REpresentational State Transfer

RFC Request for Comments

RFID Radio Frequency IDentification

RSE Road-Side Readers

SI Self-Issue

SKL Skale Network

SSD Solid State Drive

SSI Self-Sovereign Identity

SSIMS SSI Management System

TFI Toll Fee Indicator

TLS Transport Layer Security

TMS Traffic Management System

TPS Transactions Per Second

TTP Trusted Third Parties

UN United Nations

UUID Universally Unique IDentifier

VC Verifiable Claim or Credential

VCVS Verfiable Credential Verification Service

VDS Vehicle Detection Sensor

VID Vehicle IDentity

VIN Vehicle Identification Number

VPN Virutal Private Network

W3C-CCG World Wide Web Consortium Credentials Community Group

XCMP Cross-Chain Message Passing

ZKP Zero-Knbowledge Proof

ZKRP Zero-Knbowledge Range Proof

zk-SNARKs Zero-Knowledge Succinct Non-interactive Arguments of Knowledge

zk-STARKs Zero-knowledge Scalable Transparent Argument of Knowledge

List of figures

List of tables

Annex 1. Tolling and Taxation in Transport

Tolling schemes come in various flavours with each country deciding how they are applied. They are mostly in place to support infrastructural maintenance and financing. Though most countries have tolling systems across their entire highway network, there are cases where they are only applied for certain parts of the infrastructure, like for tunnels in the Netherlands and Montenegro, or bridges in Denmark. Another distinction is how tolling fees are applied based on the vehicle type, where pricing may affect all vehicle types, but increase based on tonnage (e.g., passenger vehicles vs trucks), or applied solely on heavier vehicles typically transporting goods.

Tolls are not taxes per se, or at least are not treated as such across the world. Tolls are typically user fees, and thus applied for stretches of roads, tunnels, bridges, and other road infrastructures, whilst taxation of vehicles is determined state side. Taxation is applied commonly as Taxes on Acquisition, like registration tax and registration fees, and Taxes on Ownership, which are typically annual circulation taxes. Each country has its own taxation scheme, and they are based either on a vehicle's base price (ad-valorem based taxes), and/or vehicle type, reflecting engine size, fuel type and fuel consumption. The environmental burden of fuel consumption is also becoming an important factor in refactoring taxation regulations, with each country determining the timing and framework within which adaptations are taking place.

Tolling and taxation in transport are multifactorial, determined by fiscal policies, infrastructure maturity and even more complex ones when considering cross-border transport work. Moving forward, the proliferation of electric/connected vehicles, the mandates for climate action globally, and the availability of new key enabling technologies are expected to affect policy making, taxation harmonisation and interoperability. The European Union in particular, is already working on policies and directives to facilitate the interoperability of electronic road toll systems and facilitating cross-border exchange of information, whilst considering extending the European Emission Trading System (ETS) to cover transport emissions by 2030, in turn affecting national taxing schemes.

Tolling Systems and Collection Methods

Tolling systems have evolved over the years away from turnpikes, and topical constraints to systemic approaches across entire countries. Over time they proven to be a reliable source of financing for governments implementing such systems, providing the opportunity to extend the construction and support the maintenance of road infrastructures, bridges, tunnels, and roadside facilities. The predictive nature of annual nature of tolling systems also led to easing the financial burden of governments, via allowing for long term public-private collaborations, has supportive for regional road network development subsidisation, and in some cases is even considered a leverage to decongest certain areas, such as city centres, or even reduce emissions by raising toll fees. There are three main types of tolling system currently implemented globally.

There are three main types of tolling system currently implemented globally.

1. **Open toll systems:** comprise mainline toll plazas. They are typically implemented for highway traffic, along predefined distances or geographically (e.g., prefecture based), whereby vehicles are obstructed by barriers and tolling takes place in various forms, most common of which is a flat fee per type of vehicle. When open toll systems are in place, provisions are made for local traffic, which can be diverted to use auxiliary roads of the highway infrastructure or outside of it. They are based on manual and/or electronic collection of toll fees.

2. **Closed Toll Systems:** are based on entry and exit tolling. Under a closed toll system charging is commonly based on distance travelled and/or type of vehicle. They are based on toll booths, albeit by being placed in entry or exit points the required infrastructure is less demanding than open systems. They are based on manual and/or electronic collection of toll fees.

3. **Open Road Toll Systems:** can be considered a hybrid between the previous main two systems, in terms of tolling schemes. They do not require toll booths or plazas, as they rely on technology to identify vehicles and collect the appropriate fees. They are more versatile in terms of infrastructural requirements, leveraging a number of enabling technologies, with drivers participating via electronic means that allow them to interact with the infrastructure and the tolling system.

The toll collection methods exercised can be unique in nature or a combination of several methods, depending on the toll system in place. Collection methods are added in the mix, as technology is progressively integrated, and when toll systems are transitioning to facilitate new externalities in favour of the public, adapt to environmental requirements, or even in compliance with new directives and regulations. The following are the main four modalities identifiable in global road networks:

1. **Manual toll collection :** comprise mainline toll plazas. They are typically implemented for highway traffic, along predefined distances or geographically (e.g., prefecture based), whereby vehicles are obstructed by barriers and tolling takes place in various forms, most common of which is a flat fee per type of vehicle. When open toll systems are in place, provisions are made for local traffic, which can be diverted to use auxiliary roads of the highway infrastructure or outside of it. They are based on manual and/or electronic collection of toll fees.
2. **Automatic Toll Collections:** is based on the use of Automated Coin Machine (ACM) in a typical plaza-based configuration. ACMs accept both coins and tokens issued by the operating agency in charge of network management. Alternatively, they can be based on installed credit/debit card payment processors. Although this method reduces part of the required staff, and can lead to reduced time and operational cost, it still requires vehicles to stop and potentially congest at toll booths.
3. **Electronic Toll Collection (ETC):** is based on enabling technologies to identify a vehicle equipped with a valid account accessible via an encoded data tag or transponder as it moves through a toll lane, to then automatically post a debit or charge to the account holder. Several key infrastructural requirements are not required under an ETC based toll collection method, like toll plazas, however it requires the right application of technology at defined checkpoints and the cooperation of drivers equipped with the appropriate transponders or other technology. ETC not only increases the throughput, due to the absence of barriers, but can also be rolled out, extended, or even reconfigured much easier.
4. **Mixed Toll Collection:** is a mix of manual, automatic and/or electronic toll collection can be rolled out in certain transitionary phases of a toll system to ease the unobstructed operation and cashflow to the managing authority or partnership.

Regardless of whether tolling is applied in roadways, tunnels, bridges or other transport infrastructures, the aforementioned systems and methods of collection are applicable and are currently used around the world. The following sub-section attempts to outline the kind of technologies currently in use per system in an effort to map the technological landscape in the field.

Tolling Technologies

Tolling is moving fast towards all electronic open road systems, whereby key enabling technologies are leveraged in the transition towards better control, scalability, and adaptability along the lines of a changing landscape, and new imperatives. Thus, in this subsection the architectures investigated are approached under the polarised prism of legacy vs electronic toll collection technologies, or in other words those technologies that support manual and automatic collection methods and those that support an all-electronic open road system and collection method.

Legacy Toll Collection Technologies

In open and closed systems, manual and automatic toll collection methods are employed. The prerequisite is a decentralised infrastructure of toll plazas and booths, with local equipment and networked with a centralised data centre.

Architecturally a toll plaza or booth comprises the structure canopy, overhead signage, toll booth, offices and storage housing, emergency lanes, and parking side lanes. Peripheral electronics supporting operations include digital signage, traffic lights and Closed-Circuit Television (CCTV) cameras inclusive of recording systems. Each booth is typically equipped with the following elements:

— **Lane Processor System (LPS)** including a toll collection computer, toll collector visual display unit (VDU), toll collector terminal, receipt printer, digital input output module, swipe card reader, panic button, intercom, alarm, or siren.

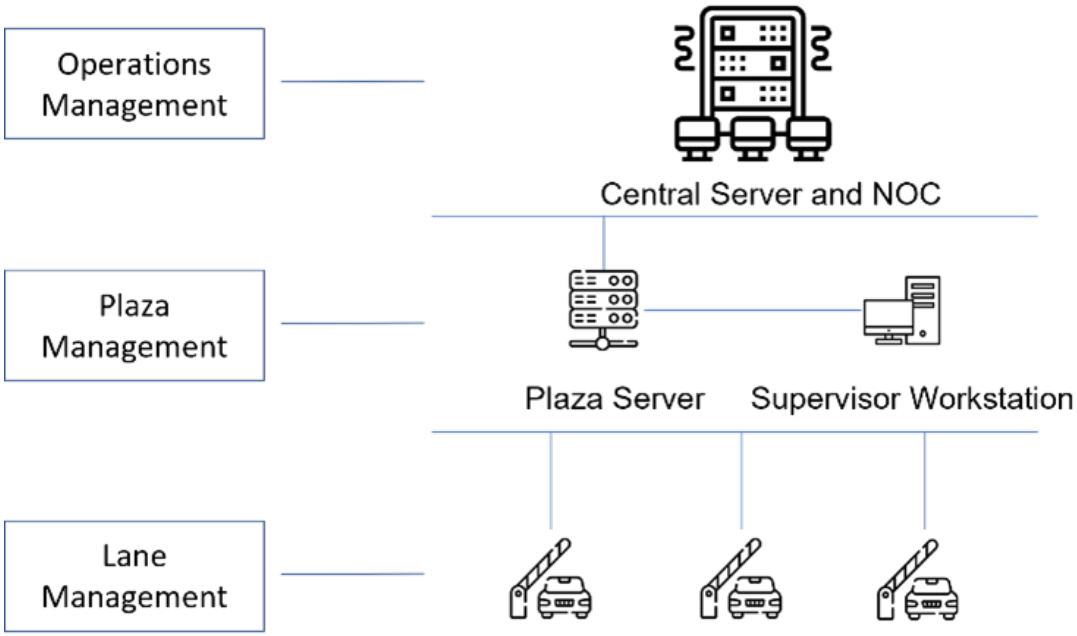
— **Automatic Lane Barrier (ALB)** responding to the collectors input automatically to allow passage.

— **Toll Fee Indicator (TFI)** displaying the tolling fee to the driver.

— **Vehicle Detection Sensor (VDS)** detecting the approaching vehicle, automating processes and safety actions including barrier movement.

Depending on the system it may also support a vehicle classification system with height sensor, and smart card readers on designated lanes. The electronics of each booth are subsequently connected to the toll plaza control centre and subsequently all data are fed back to a centralised server, typically at the provider's Network Operations Centre or NOC.

Figure 50: Overview of typical Manual/Automatic Toll Network Configuration



Source: JRC, 2022.

Figure 50 depicts an overview of a typical network configuration of manual/automatic toll plaza. Based on the figure each toll plaza acts as a node in the network and conveys data back to providers's NOC, which includes a Traffic Management System (TMS) to collect and analyse the data from the road network under management. As such these systems are two tier systems based on local and central response to changing conditions in the network. Greece is one of the European countries currently using legacy system implementation across its road network and toll operation providers, although it is in a transitionary phase, evident by the introduction of electronic technologies, such as DSRC.

Electronic Toll Collection Technologies

Electronic tolling technologies used for the charging and pricing schemes are proliferating across and especially promoted within the European Union, via specific Directives, in an effort to harmonise European road networks and systems and help policy making, support sustainable mobility, whilst ensuring road networks can be maintained and extended as per national planning. Some of the main contenders in the field are Dedicated Short-Range Communications (DSRC), Radio Frequency Identification (RFID), Global Navigation Satellite Systems (GNSS), Automated Number Plate Recognition (ANPR), as well as smartphone embedded technologies. In most cases two or more technologies are employed in tandem, to ensure enforcement. Generally, they replace traditional plaza or booth-based implementations, lower infrastructural costs, and hence allow for easy adaptation to changing conditions and regulations, while they support quick roll outs of cloud based intelligent toll collection systems.

Dedicated Short-Range Communications (DSRC)

DSRC is a communication protocol, and set of standards, intended for highly secure, high-speed wireless communication, and used for unidirectional and bidirectional data transfer between vehicles and infrastructure. It was first introduced in the United States in 1999 and was intended to be used by Intelligent Transport Systems (ITS). The European Union and Japan adopted it in 2003, followed by Singapore and other countries for electronic toll collection, the European Committee for Standardisation (CEN), resulted in "EN 12253:2004 Dedicated Short-Range Communication – Physical layer using microwave at 5.8 GHz" standard.

DSRC (Miller et al., 2001) is operationally based on the adoption of On-Board Unit (OBU) or otherwise referred to as onboard equipment (OBE) with read/write capabilities, and the installation of roadside readers. The placement of RSEs is defined by policies of charging and pricing, whilst the infrastructure must be able to support the network setup. DSRC systems are also implemented during transitionary phases on pass-through lanes fostered by toll plazas. Alongside DSCR technology-based systems ANPR technologies are leveraged to prevent fraud, with cameras typically mounted on toll plazas, gantries, or used by operating authorities in a portable manner.

The European Union selected DSRC as one of two main technologies to support the European Electronic Toll Service (EETS), along GNSS, under Regulation (EU) 2020/204 (EC, 2019c) , and is currently one of the most adopted across European countries, and in place to offer interoperability throughout the European Union. DSRC systems are currently in place either as roadside implementations or integrated in toll plazas in countries like Italy (Telepass), Spain (Via-T), Portugal (Via Verde) and Greece (e-Pass) and others.

Radio Frequency Identification (RFID)

RFID is based on roadside equipment (RSEs) and onboard units (OBUs) or RFID "tags". In a similar manner RSEs are placed in toll plazas or roadside gantries. They emit a signal in the ultra-high frequency band of 860-960 MHz and the tags, equipped with a chip and antenna, transmit the information of the account holder back for appropriate identification and charging. Tags can be passive or active battery based, whereby the difference lies in the distance need to the RSE to be activated. Passive tags are more commonly used, because of the lower costs, operate at a distance of 10m and are typically installed in plazas, under a barrier-based configuration. Active tags can reach up to 100m between the RSE and Tag and can facilitate Open Road Systems.

RFID is mainly implemented in the United States (multiple schemes), India (FASTag), Philippines (Autosweep) and other Asian countries, and in many ways the technology is similar to DSRC, though costs for RFID RSEs and OBU/Tags is significantly lower. It operates at a lower frequency band, and the security is not as strict in the corresponding standards. Enforcement is based on a combination with ANPR systems and in some cases, there is interoperability between the two technologies and systems, allowing drivers to be charged based on RFID identity or vehicle plate. In Europe RFID has not been adopted nor is currently among the proposed technologies for the EETS, however there is lobbying towards adoption by the RAIN Alliance (Alliance, 2022).

Automated Number Plate Recognition (ANPR)

ANPR is considered a mature technology. An ANPR system is based on reading the license plate, which does not require any OBU or tag, however it is based on the availability and continues update of large licence plate database accessible by the road network toll system provider. The cameras utilised are application specific industrial digital cameras, meant to capture high-quality images of license plates and vehicles regardless of the environmental or road layout conditions, or vehicle speed. These images are then communicated to the provider's back-office information systems, compared to the database, and depending on the use of the system either enforce charging policies or work in tandem with other toll technologies for charging enforcement. ANPR cameras are placed along side road lanes, toll plazas, gantries and exits/entries depending on the toll system in place, and usually require modifications of the roadside infrastructure.

The performance of ANPR-based toll collection schemes however is not as standardised as with DSRC or other technologies as it can be affected by weather conditions (fog, snow, rainfall), by unclear (dirty, customised, hidden) license plates or dense traffic conditions. Although these shortcomings drive research on machine vision and other technologies to mitigate accuracy loss, ANPR is commonly a supportive technology alongside RFID, DSRC and others. In addition to accuracy issues ANPR is subject to privacy limitations and concerns, especially in a cross-border, cross-jurisdiction setting, whereby license plates databases cannot be shared with providers. This has led to ANPR systems widely adopted as an enforcement mechanism, especially in speed limits, whereby a license plate is recorded between two fixed points and the average speed is calculated, offering a distinct advantage over speed cameras, in determining the real average speed of a vehicle. Such implementations are found in Australia, Austria, Belgium, Dubai (UAE), France, Italy, The Netherlands, Spain, South Africa, the UK, and Kuwait (Wiki, 2022) and others.

Global Navigation Satellite Systems (GNSS)

GNSS refers to satellite constellations transmitting positioning and timing data to GNSS receivers. Examples of GNSS include Europe's Galileo, the USA's NAVSTAR Global Positioning System (GPS), Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS) and China's BeiDou Navigation Satellite System (for the Space Programme EUSPA, 2022).

GNSS-based schemes involve a vehicle's geophysical position information to toll based on time or distance for a specific road network. The first successful demonstration of GNSS tolling was implemented in 1994 during the ETC field trials on the A555 motorway between Bonn and Cologne (Germany) using the American NavStar GPS System. The successful outcomes have given Europe the proof to propose in 1998 the use of GNSS as a distance based tolling mechanism (Blonk, 2000).

For GNSS toll systems to work, vehicles must be equipped with GNSS OBUs that also facilitate a mobile data communication channel, via GSM/GPRS, with the toll system provider's back-office, where positioning data are continuously monitored, and map-matching software allows for distance-based charging. GNSS is typically combined with DSRC, RFID and/or ANPR to handle satellite and mobile network coverage, violations and enforce tolling charges, hence typical GNSS OBUs are offered with a combination of technologies as a fully integrated unit. The advantage of GNSS is that no roadside infrastructure is required, and any modifications to charging schemes can be fully implemented at the providers' back-office ITS system.

GNSS is currently the basis for the Heavy-Duty Vehicle (HDV) tolling schemes in Belgium, Germany, Hungary, Russia, Slovakia, with Bulgaria and the Czech Republic already implementing it. It is also one of the technologies, along DSRC, mandated by the EETS and which must be implemented by all Member States from 19^{th} October 2021, to ensure interoperability across countries mostly for heavy duty transport work, and allow for road pricing policies based on time, distance, and place. The transitionary period is underway in all European countries.

Smartphones

The penetration of smartphone technologies and the extended cellular networks, constitute smartphones as a prime candidate for tolling systems. As devices they can double as OBUs, based on their embedded GNSS and GSM components, thus fitting the GNSS schema, but also via RFID Near-Field Communication (NFC) embedded modules. This leads to two distinct advantages in their use, as they eliminate the need for in vehicle OBUs, lower the cost of initial investment, expedite the roll out phase of tolling systems, whilst allow for other value-added services to be implemented by the toll system and road network providers. Users must install a mobile application, which ensures positioning and other data are transmitted to the provider's back-office, to facilitate toll charging. A user's credit/debit card or mobile provider account can be connected to the mobile app, removing the top-up process, offering convenience, and easy onboarding. In some countries like Austria, Slovakia and Bulgaria, smartphones are the basis to register for an e-vignette scheme, based on time-based tariffs, whilst in Portugal the C2S project made use of smartphones to pay tolls integrated with a OBU through NFC integrated with DSRC or GNSS/GSM infrastructure.

As with all EETS proposed technologies various operational issues, still apply. Smartphones are interoperable across Europe and most of the world, offering superior user interfaces and significant onboard processing power, that is why they are included in Directive 2019/520 /EC (EC, 2019f). However, satellite and mobile network coverage, can affect performance that is why supporting technologies are still needed, like ANPR cameras for enforcement and identification, in either fixed or mobile configurations.

In general smartphones can become the de facto "on board" technology of choice, due to processing power, versatility, and market penetration. This would mean that mobile and toll system providers must closely collaborate to achieve a full compliance with EETS regulations, facilitate road network wide coverage and satisfy cross border interoperability, and roaming of data communication channels.

EU Tolling Directives and Regulations

On the 29^{th} of April 2004 the European Parliament and the Council of the European Union issued Directive 2004/52/EC (EC, 2004) on the interoperability of electronic road toll systems in the Community. The directive had the scope of "laying down the conditions necessary to ensure the interoperability of electronic road toll systems in the Community. It applies to the electronic collection of all types of road fees, on the entire Community Road network, urban and interurban, motorways, major and minor roads, and various structures such as tunnels, bridges and ferries". It was complementary directive to the national electronic tolling services in order to ensure cross border interoperability of the than electronic tolling in force, hence did not require no electronic systems to adapt.

The directive for the first time officially mandated that all electronic toll systems brought into force on or after the 1^{st} of January 2007, should include the GNSS, GSM/GPRS and DSRC technology stacks, inclusive of the necessary OBUs, and those tolling services should be interoperable and independent of decisions taken by member states. It went on to address the setup of a European Electronic Toll Service (EETS), the features of the service, the stirring committee (Electronic Toll Committee)T and the implementation steps towards standardisation.

Following initial roll outs the Directive was substantially amended and replace by Directive 2019/520 on the 19^{th} of March 2019. This time it not only put forward the need for faster EETS deployment in Member states but also

in neighbouring countries to the extend possible. It stipulated the relevance of the Directive in distanced-based tolling rather time-based tolling, distance, the need for open and public standards to achieve harmonisation across Europe, provided distance from national legal frameworks, put forth the necessary amendments required in support of national EETS providers within competing frameworks as well as to alleviate privacy issues, the use of onboard equipment (OBEs) in support of GNSS systems proliferation, whilst made provisions for DSRC and ANPR technologies within national contexts among others.

It went on to define EETS providers' registration processes, rights, and obligations and other procedural aspects of compliance to EETS, but also outlined the technical provisions, safeguard clauses and other administrative issues in route to interoperability. But one of the most important considerations regarded the data exchange of EETS users between Member states, in compliance with applicable data protection regulations, for the first time mandating data driven toll policy making across Europe. Member states were instructed to adopt and publish the laws, regulations, and administrative provisions in compliance with the Directive by the 19^{th} of October 2021.

This effort led to the adoption of Regulation (EU) 2020/204 on the 28th of November 2019 detailing the obligations of EETS providers in accordance with Directive 2019/520. It outlined the providers' obligations, and detailed conformity requirements including processes, technologies, and standards. This was also addressed to manufacturers of the said technologies, which required their technical documentations to assess the interoperability constituent's conformity, as well as an analysis of and assessment of the risks involved. In general, it created a framework for conformity compliance across the board in an effort to ensure the implementation of interoperable standards and processes in tolling systems across Europe.

Meanwhile, Directive 1999/62/EC (EC, 1999) of 17^{th} June 1999 adopted a "polluter pays" principle for trucks, buses and vans, via several revisions up to July 2020 . According to the action plan proposed all heavy-duty vehicles (trucks, long-haulers) would fall under distance-based road usage charging starting from 2023, whilst light-duty vehicles (vans, buses) will be included from the end of 2027, with passenger cars soon to follow, though not expressly addressed. This effort comes in an attempt to encourage more environmentally friendly vehicles adoption, and a move away from time-based charging, driving lower CO_2 emissions from road transport. So far distance-based charging has been implemented for heavy vehicles based on weight and distance in New Zealand (RUC), Switzerland (LSVA), Germany (LKW-Maut), Austria (Go-Maut), Czech Republic, Slovakia, Poland, and in several US states.

In conclusion reaching to a point where EETS has now been regulated for all Member states has been a decade long process of technology development, testing, piloting, and standardisation to facilitate real world roll outs and tolling systems interoperability. A recap of all major milestones includes (EC, 2021d):

- **Commission Implementing Regulation (EU) 2020/204** of 28^{th} November 2019 (EC, 2019d) on detailed obligations of European Electronic Toll Service providers, minimum content of the European Electronic Toll Service domain statement, electronic interfaces, requirements for interoperability constituents and repealing Decision 2009/750/EC
- **Directive (EU) 2019/520** of the European Parliament and of the Council of 19^{th} March 2019 on the interoperability of electronic road toll systems and facilitating cross-border exchange of information on the failure to pay road fees in the Union (EC, 2019f).
- **C/2019/9080 Commission Implementing Regulation** (EC, 2019e)
- **C/2019/8369** Commission Delegated Regulation (EC, 2019b)
- **Commission Decision 2009/750/EC** on the definition of the EETS and its technical elements (EC, 2009a);
- **COM(2012)474:** Implementation of the EETS; (EC, 2009b)
- **Directive 2004/52/EC** of the European Parliament and of the Council on the interoperability of electronic road toll systems in the Community (EC, 2004).
- **M/338 Standardisation request** to CEN, The European Electrotechnical Committee for Standardisation (CENELEC) and European Telecommunications Standards Institute (ETSI) in support of interoperability of electronic road toll systems in the EU (EC, 2003).

The importance of a Europe wide interoperable EETS, apart from the strict framework of tolling schemes and cross-border collaboration among EETS providers and Member states, further aligns with the Green Deal goals of lowering emissions from road transport by 2030.

Congestion Charging

Congestion charging or pricing stems from the field of economy with Nobel-laureate William Vickrey proposing in 1959 that drivers should be charged higher and by electronic means when using busy urban roads. Congestion pricing addressed the demand side issues of road usage and was a strategy offered by economists to address traffic congestion, with implementations over the years found exclusively in urban areas, in and around city centres. The first successful implementation was with the Singapore Area Licensing Scheme in 1976, which though adapted and evolved is still in place today.

The concept of congestion charging addresses externalities, in that demand driven traffic can cause congestion but also increase noise, accident rates, and pollutants, an issue high in today's agenda of climate action. Congestion pricing can be fixed per type of vehicle, variable as in pre-set higher at times of increased congestion times, or dynamic by responding to in real time to traffic conditions. As congestion charging schemes have been increasing over the years, they are classified into four different types: cordon areas which is typically a restricted area within the city centre; area wide congestion pricing applied in wider urban settings; urban toll rings; and corridor or single facility congestion pricing.

Cordon and area wide congestion charging schemes are currently in place in several cities worldwide among them the aforementioned Electronic Road Pricing scheme in Singapore since 1998, the London Congestion Charge scheme since 2003, the Stockholm congestion tax, the Milan Area C, and high-occupancy toll lanes in the United States. Similar schemes have been implemented in several smaller European cities too like Durham in the U.K., Znojmo in Czech Republic, and Valletta in Malta where heavy traffic affected the old historical city centres, especially during touristic periods. Often congestion charging schemes are implemented as or complemented by Low Emission Zones (LEZs), i.e., areas where the most polluting vehicles are more heavily regulated. Such more specialised schemes are implemented in Graz, Brussels, Madrid, and other European cities, whereas Pollution Emergency zones are also instituted in Lyon, Barcelona, Vienna, Geneva etc. with alert systems in place allowing the cities to inform of speed limit (hence increase in emissions) violations or react in cases of significant reductions in air quality.

The Milan case is especially interesting. In January 2008 Milan implemented ECOPASS a one-year trial program in an attempt to facilitate pollution-based charging depending on the vehicle's engine emissions standard entering the city centre. The preliminary results were encouraging (Massiani et al., 2012) showing a reduction in vehicles entering the cordon area, increase in public transport efficacies and reduced air pollution. However, the program was short lived as it did not manage to reduce real congestion as vehicle owners replaced older vehicles with ones, with engine emissions requirements within the exempt levels, hence the program was heavily criticised and was finally replaced in January 2012 by Area C. Area C started off as a pilot and was finally adopted to introduce conventional congestion charging, which increased tolling revenues, in turn re-invested in sustainable mobility solutions within the city.

Norway on the other hand is a prime example of the use of congestion pricing implemented in toll rings and urban corridors. The first program was implemented in Bergen as early as 1986, Oslo in 1990 and Trondheim in 1991. Although at that time the roll out was intended to act as a revenue driver for road infrastructure, in 2011 the program was extended to address traffic congestion in most Norwegian cities, as well as act a as relief mechanism for greenhouse emissions. The Norwegian electronic toll collection system is called AutoPASS and is part of the joint venture EasyGo (Hamilton and Eliasson, 2011).

Single facilities are another field of application for congestion pricing. Express lanes in highways called High Occupancy Toll (HOT) lanes, were initially conceived as a measure to increase vehicle occupancy, reduce traffic congestion, and expedite adoption of vehicles of specific engine emission standards. HOT lanes have been introduced mainly in the United States and Canada, whilst in Europe the Autoroute A1 in Northern France is one of the few cases of congestion pricing implemented outside of urban areas. Other applications involve bridges and tunnels like the San Francisco Bay bridge, the Sydney Harbour bridge, and other similar facilities, in place to alleviate heavy traffic during peak hours.

Congestion pricing has not been around long enough to allow for comprehensive studying. Reports from the cities that have implemented congestion pricing schemes show traffic volume reductions, yet longitudinal studies have not been performed in a changing landscape of policy updates (Cipriani et al., 2019, Vosough et al., 2022, Selmoune et al., 2020), and equity (Eliasson, 2016) considerations. These issues are further exacerbated with the advent of electrification and autonomous vehicles (Simoni et al., 2019) which will add more dimensions to the subject either in urban or non-urban settings. Although congestion charging schemes are not referenced in EETS, congestion needs addressing to ensure quality of life within modern cities, safety and alleviate

environmental consequences.

Transport Taxation Landscape

At present there is rudimentary legislation in the EU on vehicle taxation, thus there is lack of harmonisation across Member states, apart from Directive 83/182/EEC (EC, 1983) which addressed tax exemptions for certain means of transport across borders, and a proposal for a Directive 5^{th} July 2005 presented a proposal for a Directive, COM(2005) 261 (EC, 1983), to require Member States to re-structure their passenger car taxation systems. As such, vehicle taxation falls largely under national regulatory frameworks, thus this section attempts to identify the various taxes in place, typically classed within the following three broad categories: Acquisition Taxes, Ownership Taxes, and Motoring Taxes (ACEA, 2021).

Acquisition taxes are calculated in various manners across Member states and are one off charges upon vehicle purchase, while in most countries, additional registration taxes and registration fees are in place. Austria imposes 20% VAT on acquisition and registration tax based on CO_2 emissions, Greece 24% VAT and registration tax based on a combination of net retail price and CO_2 emissions, Germany 19% VAT and 30 euros registration fees, Lithuania 21% VAT plus registration fees based on vehicle type, and so do all countries impose their own taxes. Acquisition VAT percentage in Europe for 2021 ranged between 17% in Luxembourg to 27% in Hungary.

Ownership or circulation taxes are charged annually and are typically separated between passenger and commercial vehicles. The taxation schemes in place are more diverse than acquisition taxes but they generally fall into the following categories:

— Passenger cars taxed based on various combinations of the following characteristics

- Engine power (kW), engine size, fiscal power (hp), cylinder capacity (cc), CO_2 emissions, fuel type, gross vehicle weight (GVW), age, province

— Commercial vehicles again taxed under a combination of any of the following

- Gross vehicle weight (GVW), maximum permissible weight (MPW), engine power (kW), fuel consumption, number of axles and suspension type, CO_2 emissions, exhaust emissions group, number of seats (buses/vans), payload

Estonia, Lithuania, and Slovenia do not take into account any of the aforementioned characteristics for passenger cars yet do impose in some cases a flat fee ownership tax. Slovenia in particular did not have ownership taxation in place for commercial vehicles too up until January 1^{st}, 2021, when the Motor Vehicle Charges Act - Zakon o dajatvah za motorna vozila (Official Gazette of the Republic Of Slovenia No. 54/17 and 112/21) was legislated (EC, 2021c).

Motoring taxes typically include excise duty on fuels including vat, and in some case tolls on roads or bridges, and euro-vignette system although these are considered usage charges. In terms of excise duties on fuels these are calculated per 1000 litres and separate rates apply for unleaded petrol and diesel across the EU. Some examples include France where the tax is €683 and €594 per 1000 litres respectively, The Netherlands with €813 and €522, and Hungary with the lower taxes at €345 and €317. The range of motoring taxes is between €345 and €317 in Hungary and €728 and €617 respectively in Italy. The average EU motoring tax cost is calculated at €359/1000l for unleaded petrol and €330/1000l for diesel fuels.

Taxes within these three categories are typically around the world, but with other regions exhibiting much lower taxes as is the case for fuel taxation of petrol in the Canadian and US states which averages at €200/1000l. In the case of EU Member states however these taxes are a main revenue stream, along other transport related secondary charges. In total the European countries monitored, achieved in 2020 a fiscal income of €398.4 billion, ranging form €6.2b for Ireland to €99.9 billion for Germany, revenues that are in turn expected to support sustainable mobility initiatives, maintain infrastructures and mitigate environmental issues caused by transport work.

Emissions trading in the EU

In 1997 the Kyoto Protocol set legally binding emissions reduction targets, or caps, for 37 industrialised countries. Europe was among the first to react with policy instruments to meet the proposed targets, and in 2003 Directive 2003/87/EC (EC, 2021f) was adopted. This led to the setup in 2005 the European Emissions Trading System or ETS is the world's first international emissions trading system build around a cap-and-trade scheme of CO_2 emissions. During Phase I, from 2005 to 2007, only power generation and energy intensive industries were

covered for CO_2 reductions and free trading of emission allowances. In Phase II, from 2008 to 2012, the ETS expanded outside of the EU Member states, established a Union registry replacing national ones, the CO_2 emissions cap was reduced, international trade was facilitated, and the aviation sector was added. Phase III, lasting from 2013 to 2020, also unified the CO_2 caps moving away from national ones, more polluting sectors were added, and allowances were set aside for funding new renewable and climate action initiatives. Currently in Phase IV, that will last from 2021 to 2030, the EU via the ETS is on its way to achieve climate neutrality by 2050 and 55% reduction in greenhouse emissions by 2030 (ETS, 2021c).

Overview of ETS

The European Emissions Trading System (ETS) is cornerstone system to tackle climate change and it's based on a strict 'cap-and-trade' principle (ETS, 2021a). This implies that it sets a particular amount, or cap, of annual greenhouse gases that must be followed by all entities participating in the system. This cap is gradually reduced in light of future goals set by the Committee and especially the reduction of total greenhouse gases to 55% in 2030 with respect to 1990's emissions.

As a trading mechanism it allows participating entities currently including energy production, energy intense industrial players, and aviation to trade emission allowances with each other. At years end emissions monitored or calculated and any surplus is removed by the Market Stability Reserve (ETS, 2021a), established in January 2019, to provision for system resilience in case of major market shocks. Alongside the Market Stability Reserve, and to gradually extend the entities participating in the ETS a free allocation mechanism is in place. This allows more entities to enter the ETS emissions auctioning process but makes provision for them to gradually increase their involvement with a percentage of their emissions requirements freely allocated to them, avoiding unintended negative economic consequences.

The ETS covers large power stations, large industrial plants, large district heating plants and aviation, representing about 40% of total EU emissions. The total EU greenhouse gas emissions by 2018, was significantly reduced due to ETS pressure to reduce emissions, new technological advantages, and roll outs especially within the renewable energy fields, and partly due to the Effort Sharing (Clima, 2021) legislation involving non ETS sectors. The following infographic sourced by Eurostat (EuroStat, 2018) outlines the contribution per source in 2018. Figure 51 illustrates the share per source of greenhouse gas emissions, where the energy sector, manufacturing industries, and aviation (part of transport) comprise over 40% of total EU emissions. Particularly in transport 2018 figures increased by 9.8% compared to 1990, although 2020 reports show that transport work along other sources show a steep decline, strongly related to COVID-19 measures.

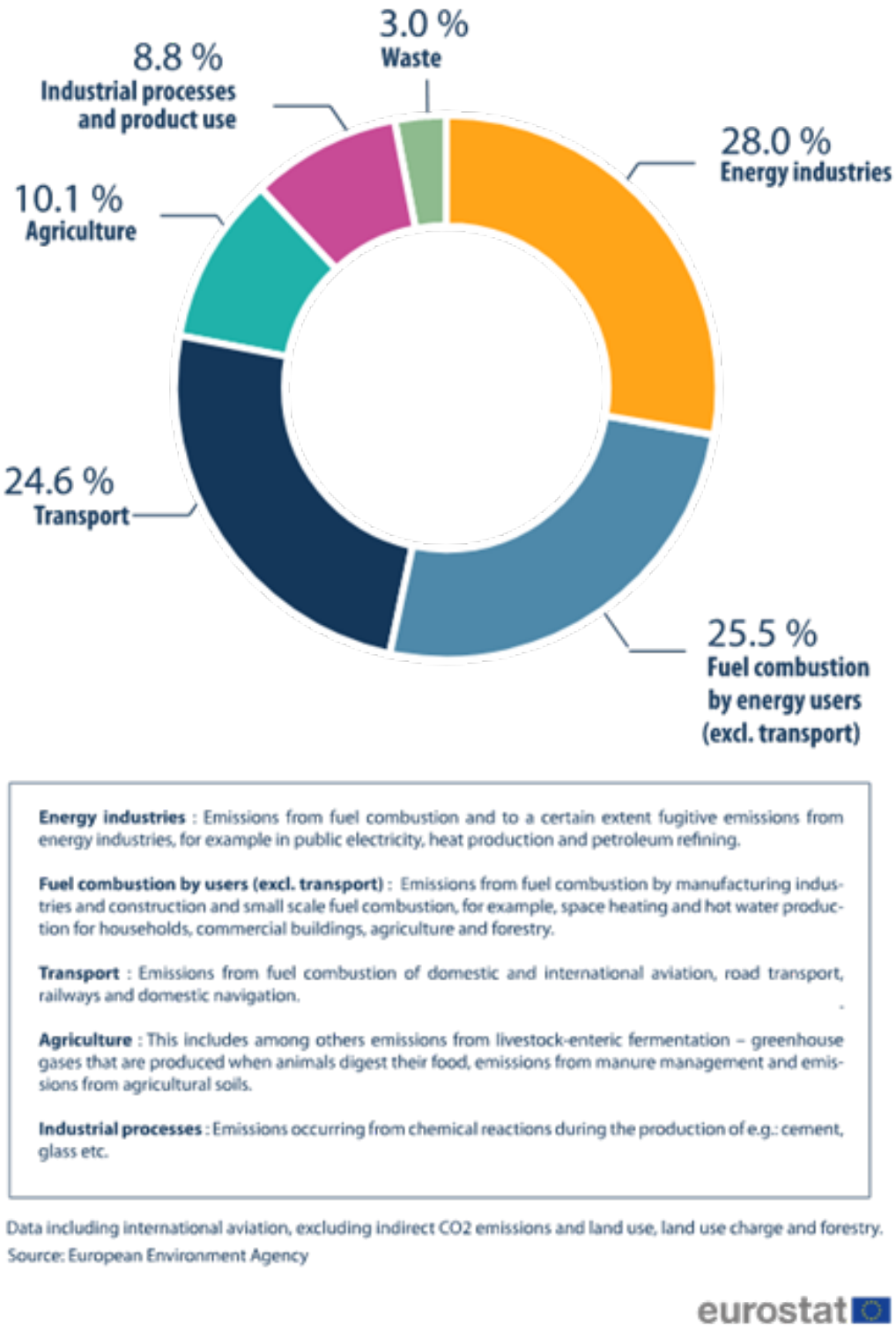
As the ETS is entering its fourth phase it is setting more ambitious goals to reduce the emissions from the currently covered sectors and future ones to 61% by 2030, compared to 2005 levels, almost doubling the targeted emissions reduction from 2.2% annually to 4.2%, whilst also removing gradually the current free allowances for aviation. Furthermore, a proposal (EC, 2021g) submitted in July 2021, aimed at extending ETS coverage to include emissions from maritime transport too, while emissions from fuels used in road transport and buildings will be covered by a new emissions trading mechanism.

Trading Road Transport Emissions

The European Green Deal (EC, 2019a) set out in December 2019, is Europe's commitment to tackle climate and environmental challenges. Within the scope of achieving the goals put forward, in July 2021 it revised its goals for 2030 and adopted a package of proposals (EC, 2021h) to make the EU's policies fit for reducing net greenhouse gas emissions by 55% by 2030, compared to 1990 levels. Within this set of proposals, a new emissions trading system (EuroParl, 2020) for road transport and buildings (ETS-BRT) was suggested to be brought in force by 2025, along with a Social Climate Fund of €72.2 billion. As greenhouse gases are emitted by households and vehicle owners, the proposed regulated entities are fuel distributors for whom a monitoring and reporting system already exists under Directive (EU) 2020/262. The timeline suggested is for distributors to report fuel distribution annually starting from 2024, to allow for a data driven cap on emissions to be placed by 2026, with the targeted emissions reduction reaching 43% by 2030 compared to 2005 levels.

This effort is expected to raise fuel prices; thus, the Social Climate Fund will be in place to address any incurred social impacts. Although the updated targets were generally deemed as aiming in the right direction and were welcomed by the EU parliament members, the rise in fuel prices raised concerns of how low-income households and small businesses will be able to cope (EPP, 2021). The Fit for 55 package did not include the necessary legislative proposals to address national level consequences, thus social impacts might not be equitable (Pollitt et al., 2021) when the proposed measures come into force, unless externalities at national

Figure 51: EU Greenhouse gas emissions data by source in 2018



Source: Eurostat, 2018

levels are foreseen and addressed.

Meanwhile in the United States, where transportation as a sector, accounts for 29% of total GHG emissions, the focus on road transport is on greener vehicles and greener supply chains with the US Environmental Protection Agency launching the SmartWay (EPA, 2021) program, whilst the EPA's emissions trading system is focused primarily on the energy and industrial sectors. Since 2010 New Zealand's ETS addressed transport emissions (New Zealand, 2022) in a similar manner to the proposed Fit for 55 package by including fuel suppliers, although with several exemptions in place in line with the Kyoto protocol. China on the other hand just

launched its national ETS in 2021 and is currently focused solely on regulating power generation. Overall, the EU ETS is the largest and most successful emissions trading system globally, with other ETS not exhibiting policies for road transport specifically, thus addressed by national policies and emissions taxation. This demonstrates the ambition of the EU Green Deal program, but also highlights the lack of paradigms and the potential socioeconomic impact of introducing a cap-and-trade system on road transport emissions, within the proposed strict timeframe. Conversely, the Green Deal framework exercises a direct pressure to innovate, driving new technological advancements in the automotive industry (Siemens, 2021), as well as new lower emission fuels (Puricelli et al., 2021) in the market.

Vehicles as Identities

All vehicles have their unique Vehicle Identification Number (VIN). It is composed of 17 characters, imprinted on the engine and other parts of a vehicle, which not only act as a "fingerprint" but also convey a vehicle's features and specifications. VIN can be used to track a vehicle's history, from manufacturing and registration to warranty and insurance. In essence this asset has an enriched identity. Unfortunately, this identity is subject to fraud via removal, tampering, and cloning and liability can be attested to dealerships, or even owners.

The issue of correctly identifying a vehicle is cornerstone to tolling systems, whereby VIN is encoded to OBUs. Auto manufacturers are obliged to provide a VIN database for toll providers to access and subsequently correctly classify a vehicle for tolling pricing. This would mean that vehicles (and drivers) can be identified across road networks, provided VIN and license plates match, and the appropriate charges can be applied. Identification becomes even more important under the new EETS framework, where information must be shared across toll providers, borders, and jurisdictions.

Conversely, this also raises privacy concerns (Clarke and Wigan, 2011, Ghosh and Mahesh, 2016). Agreements to ensure data privacy are not yet fully aligned with the roll out of EETS systems, whilst ANPR and GNSS allow the recognition or continuous tracking of drivers but do not provision for user privacy. DSRC and RFID do not require continuous tracking yet personal data are required for the system to operate accordingly. Privacy issues as such are part of EETS adoption and do not account for vehicles travelling outside of tolled infrastructures. Meanwhile ownership taxation across Europe and most of the world, on way or the other, is based CO_2 emissions.

Moving to a future carved by environmental policies, with fuel prices destined to rise, inevitably requires charges and taxes to be (a) equitable and (b) respectful of data privacy. This means technological solutions must be provided or complemented to address both issues at once. An application specific overlay that stands to address as widespread as possible vehicles' usage, within national tolled road networks, congestion-based operated cities, and facilities, as well as cross-border charging and exchange of information. These solutions should ensure that distance travelled, or otherwise each individual's or company's impact on infrastructures and the environment, is accounted for across all activities, without sacrificing privacy.

BC based Tolling and Taxation

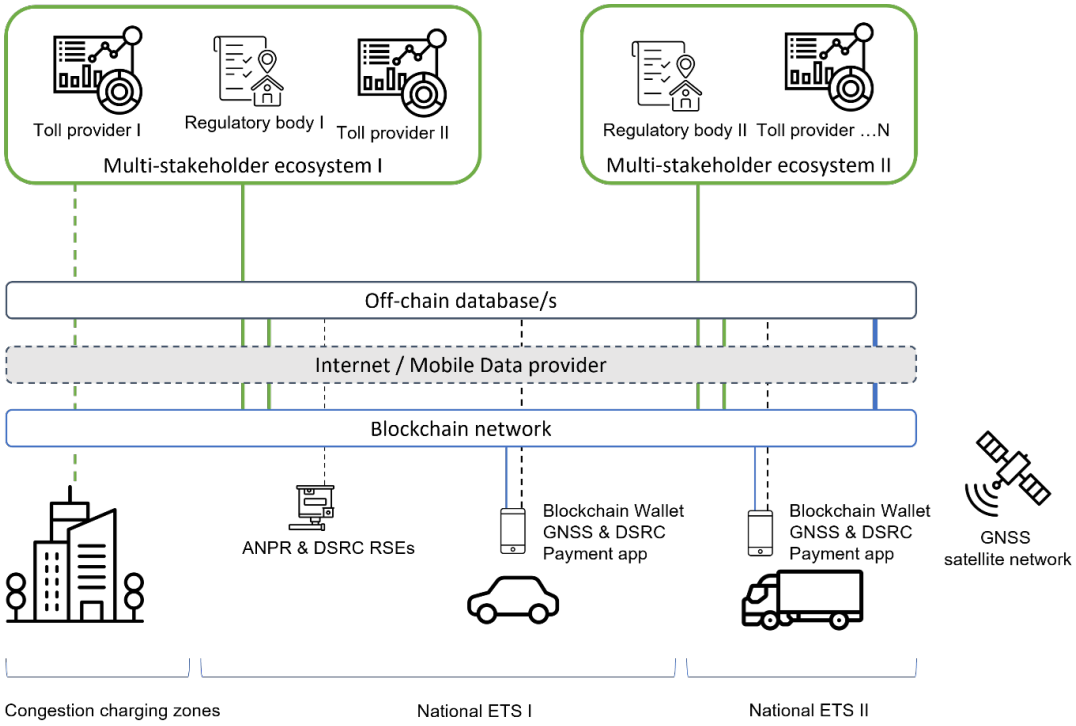
One such solution could be the application of BC technology or Distributed Ledger Technology to be more precise. In fact, its uses and advantages are investigated at a European level via the European BC Partnership (EBP) (EBP, 2022, EBSI, 2017) to facilitate cross-border collaboration under "five key principles: public good, governance, harmonisation, open source and compliant with EU regulations" (GDPR, eIDAS, etc.)". EBSI is conceived on the basis of implementing a Self-Sovereign Identity model for Europe, create trusted digital audit trails, automate compliance checks, prove data integrity, and support secure data sharing among European governments, businesses and individuals. Thus far 25 live BC nodes have been established across EU Member states, with 11 nodes in setup phase.

Research is also supporting the use of BC in privacy-preserving tolling architectures (Bartolomeu et al., 2020), as well as in conjunction with IoT and AI technologies to support distributed intelligence (**?**). The use of the technology has been investigated for Norway's Autopass (Repo, 2019), whereby the conducted literature review and design science methodology applied, found a public permissioned BC architecture feasible within the scope of Autopass' multi-stakeholder setting. More extensive research conducted in 2019 for the Ministry of Transport and Digital Infrastructure (Fridgen et al., 2019) in Germany, on the opportunities of BC in mobility and logistics, found the technology a suitable candidate for toll charging, and other uses moving towards an electric vehicle future, though it needs to be subject to regulations. The use of BC technology is also being investigated as part of a wider energy (Wang and Su, 2020) point of view, especially e-mobility (Andoni et al., 2019), from the auto manufacturers perspective (Fraga-Lamas and Fernández-Caramés, 2019), or even the insurance field (Lamberti et al., 2018) as an enabler of dynamic or on-demand coverage.

Considering the work being carried out it would not be far fetched to see EBSI and EETS working in tandem to promote the use of the technology as the basis of an interoperable, privacy preserving mechanism to allow electronic toll system harmonisation across Europe, support congestion schemes, and distance-based charging or taxation, by creating BC based wallets, acting as OBUs. In light of this, this report proposes a top-level architecture to address a multi-tenant construct accessible by the disparate entities comprising the tolling and taxation landscape.

Considering that vehicles are not readily equipped with BC enabled OBUs, that tolling, and taxation is already regulated at national and EETS level, and that distance-based charging is to become a reality in subsequent years, the proposed architecture is based on smartphones acting as OBUs considering their higher processing power and availability. The following figure outlines the top-level characteristics of such an implementation under an Open Road Toll system.

Figure 52: Top level design of a BC enabled tolling and taxation architecture



Source: JRC, 2022.

Figure 52 considers a multi layered architecture based on an open road toll system. It follows broadly the current EETS framework with an added layer of privacy preserving logic across the board. Within this proposed architecture the following elements are included:

- **BC wallet OBU:** Drivers are to be equipped with a mobile app that binds them with the vehicle. The app should be GNSS and potentially DSRC enabled to foster for positioning information and to allow for enforcement and verification of a vehicles true positioning. The identity of the driver or company and the vehicle could be hashed and exported to an off-chain database or databases, depending on the ETS provider, ensuring privacy of individuals is preserved, whilst non identifiable data can be exported directly. Distance based usage can be fostered via correlating positioning data with the hashed driver/vehicle information. A payment process is to be included in the app to allow for charging of the road user be it on toll roads or other charging zones, at the appropriate rate.
- **ANPR and DSRC RSEs:** The enforcement or verification mechanisms are to be addressed by ANPR or DSRC technologies against off-chain data, to preserve privacy where possible.
- **BC network:** A BC network architecture will be key for fostering the necessary smart contracts and interact with the mobile app in terms of identity management and hashing processes, communicating anonymised transactional payloads to the off-chain database/s. Smart contracts should address all transactional activities between drivers and the regulators, drivers and the toll system by monitoring

positioning, distance and speed monitoring, cross border ETS traversing, providers the BC network, providers and drivers, providers and the off-chain database/s, as well as provision for consent mechanisms and disclosure in case of violations or any unlawful actions among others.

- **Multi-stakeholder ecosystems:** These ecosystems will be verified against the BC network, to access the appropriate APIs and be able to access, under an anonymisation framework, off-chain data for post processing, charging and enforcement. Regulators will be able to issue registrations and ownership taxation on real emissions based on emissions standards, vehicle type approval and distance travelled annually, whilst ETS providers can access data to allow for all ITS processes to take place and ensure road network management. Location based smart contracts will allow for provider hand-over, across ETS systems and jurisdictions.
- **Congestion charging zones:** This architecture empowers cities to roll-out quickly congestion charging schemes based on positioning and potentially time-based access to the required inner-city zones, single facilities, or ring roads. This process can easily be facilitated by service providers with initial investment in infrastructure.
- **Mobile data providers:** As with EETS OBUs, mobile data providers or mobile operators will be part of the overall ecosystem providing not only the communication channels, but potential building on 5G deployments to create value added services for drivers, regulators and toll system providers.

The proposed architecture assumes that such a BC network can be accepted by all interested parties. As such it must be regulated at national as well as European level to come in force. Another major assumption is the use of smartphones, although this proposition addresses a potential proof of concept of such an implementation. A more robust schema would be for BC wallets to be fully integrated in vehicles by auto manufacturers, replacing the VIN identification codes, extending a vehicle to a cyber-physical entity.

The realisation of such an architecture could be based on the currently, under development, EBSI framework, whereby vehicle digital wallets could be elaborated to interact with the infrastructure as well as the owners or individuals driving them. This would solidify the significance of the EBSI framework and drive support for future developments.

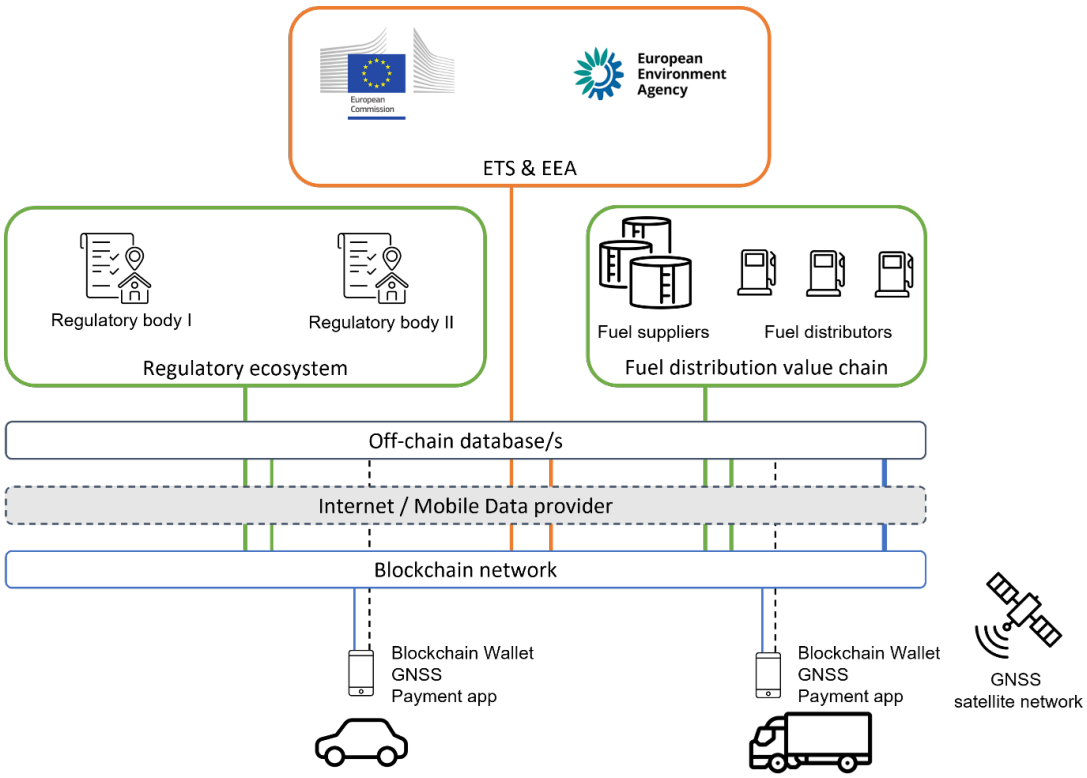
BC Technology and ETS

Extending the aforementioned framework, it could also encompass fuel distribution from the suppliers to the distributors and subsequently the drivers. With Fit for 55 focused on fuel distributors, and fuel prices destined to increase, one can identify a gap in equitable monitoring and taxation in both road transport, and buildings.

As with tolling and taxation Figure 53 provides a proposed extension of the architecture to incorporate fuel distribution. With new fuels researched and rolled out in the market, and the possibility of lower CO_2 emitting fuels or even net-zero fuels (et al, 2021) hitting the market over the coming years, taxation based on emissions, and type approval will no longer be an equitable way to address externalities. Meanwhile, such an architecture could provide the European Emissions Trading System and the European Environmental Agency with immutable monitoring data, that can be time and location relevant, leveraging the same technology substrate as for EETS and the EBSI, as well as augmenting it to encompass transactions between suppliers, distributors, and vehicle owners. Such as proposed BC enabled implementation is also backed by research (Mandaroux et al., 2021) to address not only processes but also battle fraudulent attempts. Consequently, data will empower the Social Climate Fund and national governments to exercise data driven policies and aid distribution.

For fuel suppliers and distributors to come into play application specific implementations will be supported by the BC network at a software and/or IoT level, facilitating transactions with incorporated metadata for fuel type, CO_2 content, fuel quantity and other important parameters. The BC implementation can then provide an immutable digital audit trail from suppliers to consumption of fuels, along with enriched metadata on consumption conditions (speed, emissions, locality etc). This would in turn facilitate regulators to tax accordingly in a more equitable manner becoming of the real-world conditions.

Figure 53: Architecture extension for fuel distribution in road transport



Source: JRC, 2022.

Next Steps

A Distributed Ledger framework of choice for proof-of-concept implementation would be Hyperledger Fabric. As demonstrated by IBM and Maersk through the application of the logistics sector TradeLens (MAERSK, 2022) platform, based on the Fabric framework, DLTs can now support complex ecosystems whereby multiple organisations can be supported, data spill over can be avoided and permissioned management can be facilitated. Another rationalisation is that EBSI incorporates Hyperledger Fabric in its core architecture hence any implementation could be easier adapted to the EBSI framework of services if needed.

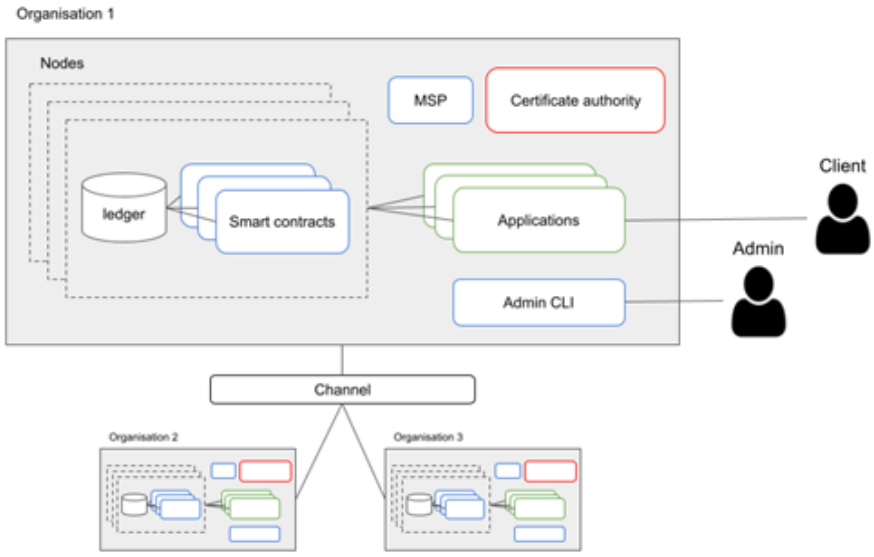
In a nutshell under the Hyperledger Fabric framework (Hyperledger, 2022a), networks form the technical infrastructure that provides ledgers and smart contract services to applications managed by different organisations, as would be the case for the proposed architecture (EBSI, 2022a). In most cases, "multiple organisations come together to form a channel on which transactions are invoked on smart contracts", whilst permissions are determined by a set of policies that are agreed upon when a channel is originally configured.

Organisations, such as regulators, service providers, Fuel suppliers and distributors, conceptually form entities which have access to channels and can issue identities to participants, so that every transaction's source is identifiable. The identities of BC nodes, the clients or the administrators must be created by a CA associated with each organisation. CAs play a key role in the network because they dispense certificates to be used to identify components that belong to an organisation. These certificates are stored in a set of folders called Membership Service Provider (MSP).

Drivers or other clients can have access to smart contracts through applications. Each organisation needs to maintain one or multiple applications that interpret its business logic and provide the ability to clients to send transaction requests to the smart contracts by verifying their identities. Organisation administrators, which in the proposed proof of concept could be the regulators, are the only ones authorised to register clients in the organisation by issuing the appropriate client keys and certificates, by using the corresponding Certificate authority.

Overall, Hyperledger Fabric is a framework versatile enough to support a proof-of-concept moving forward. It has been proven to work in demanding global logistic environments, where the participating ecosystems include customs from various countries, logistics providers, shipping companies and harbour services. In other words, it is a proven framework that can be adequately adapted to work in complex ecosystems and across

Figure 54: Hyperledger Fabric conceptual network structure



Source: JRC, 2022.

borders, which largely characterises road transport as well. In the second phase of this research work a system level architecture will be elaborated and proof-of-concept example solution will be implemented.

Conclusions on Tolling and Taxation

Tolling and taxation of vehicles is undergoing a major shift in technologies and processes. The new EETS framework drives cross-border interoperability and leads the way to regulatory and technological harmonisation among EU Member states. In parallel the Green Deal imperatives are extending the European Emissions Trading System to incorporate more market players and address more sectors, among which the road transport. Secondary efforts include the shift from time-based to distance-based tolling, which although affects heavy and light weight vehicles, paves the way to more equitable tolling, and taxation policies in the future.

Although the technological substrates are there, they are disjointed and do not foster an all-encompassing regulated environment at both EU and national levels. New paradigms are need to showcase interoperability at large, reduce infrastructural needs and support standardisation. EETS, EU ETS and EBSI can work in tandem to regulate common interfacing between disparate actors and value chain stakeholders. Distributed Ledger technologies could provide this common interfacing under a privacy preserving prism. This report is part of the work conducted to identify the potential of, and pilot BC based implementations as an additional enabler to the ecosystem of solutions proposed for the transport sector.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union