Operational Concepts for Distributed Ledger in ITS Use Cases

Blockchain for ITS Research and Deployment Technical Services Support

www.its.dot.gov/index.htm

Final – October 10, 2023
FHWA-JPO-23-119

U.S. Department of Transportation

Produced by Noblis under 693JJ321D000021 Task Order 693JJ322F00408N
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Notice

Technical Report Documentation Page

1. Report No.	3. Recipient's Catalog No.	3. Recipient's Catalog No.
FHWA-JPO-23-119		

4. Title and Subtitle	5. Report Date
Operational Concepts for Distributed Ledger in ITS Use Cases Blockchain Research and Deployment Technical Services Support	October 2023
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Tram Vo (Citopia), Chris Ballinger (Citopia), Kellen Shain, Ned Schweikert, Amy O'Hara, Atizaz Ali, Caden Young, Andrew Dudash, James O'Hara, and Karl Wunderlich	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Noblis, Inc. 500 L'Enfant Plaza SW, Suite 900 Washington, DC 20024	**11. Contract or Grant No.**

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Intelligent Transportation Systems Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	**14. Sponsoring Agency Code** HOIT-1

15. Supplementary Notes

Robert Sheehan - TOCOR

16. Abstract

This report expands on the work from a prior report *Potential Categories for the Application of Blockchain in Intelligent Transportation Systems (ITS)* (FHWA-JPO-23-987) by conducting a gap analysis on five selected distributed ledger applications from this report. The gap analysis was conducted by first determining the current state of these applications, (1) Multimodal Trip Planning and Fare Payment System, (2) Transportation-based Virtual Power Plant with Payment, (3) Freight Management, (4) Use-based Fees, and (5) Security and Credential Management (SCMS), and then determining the desired/future state of these applications based on stakeholder feedback and literature reviews. Gaps were then identified by determining what steps, if any, could be taken to get from the current state to the future state for a given application. Sixteen use cases were developed, providing real-world scenarios to illustrate how a distributed ledger could potentially or is currently being used to advance the current state of the five applications to their desired/future state. This document prepares technologists to evaluate and implement blockchain and distributed ledger-based solutions to make transportation infrastructure safer, more efficient, and with a positive environmental impact.

17. Keywords	18. Distribution Statement
Distributed Ledger Technology, Decentralization, Smart Contracts, Blockchain, intelligent transportation systems, architecture	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		82	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

List of Tables

List of Figures

Executive Summary

With the push towards electric vehicles, autonomous vehicles, and reduced emissions, ITS is challenged to build infrastructure that incentivizes, facilitates, and monetizes modern transportation options. This report identifies several ways to build this infrastructure:

- Reduce multi-leg trip payments to a single fare, to encourage mass transit.
- Enable parking facilities to setup paid charging and allow parked electric vehicles to discharge their batteries, with compensation, to reduce power grid strain.
- Provide more granular tracking of freight to simplify invoices for logistics companies.
- Implement usage-based transportation infrastructure or fees to prevent congestion and provide an income source independent of gas taxes.
- Automatically track performance of autonomous vehicles to increase safety in the event of malfunctions.

These applications are possible but for a distributed system this large the overhead is too expensive to implement manually, and an automated system would struggle to validate the accuracy, confidentiality, and integrity of data across all parts of the network. Distributed Ledger Technology (DLT) is a natural fit that can automate the bookkeeping of these applications while guaranteeing—with high confidence—the integrity of the data being used.

This report provides a thorough exploration of each of the above applications, references related research and prior work in this space, highlights the gaps between the state-of-the-art application prototypes and a fully realized system, and ties each application directly to the needs to over a dozen stakeholders, including parking authorities, building owners, emergency response teams, NGOs, utility companies, local DOTs.

This document prepares technologists to evaluate and implement blockchain and distributed ledger-based solutions to make transportation infrastructure safer, more efficient, and with a positive environmental impact.

Overview of Selected Distributed Ledger Technology Applications

U.S. DOT selected five applications out of the fifteen identified in the Task 2 report: *Potential Categories for the Application of Blockchain in Intelligent Transportation Systems (ITS)*. Each of the five applications is summarized below and includes the rationale for each application's selection.

Multimodal Trip Planning and Fare Payment System

The Multimodal Trip Planning and Fare Payment System application is a distributed ledger-based multimodal trip planning application that allows users to plan, book, and pay for a multi-leg trip or journey from an origin to a destination. Data from multiple mobility service providers is integrated into a

decentralized ledger based on data sharing agreements via smart contracts. This allows users to plan and book their multimodal trip from a variety of options integrated in the distributed ledger application, rather than booking multiple trips on different platforms.

Transportation-based Virtual Power Plant with Payment

The Transportation-based Virtual Power Plant with Payment application is a distributed ledger-based virtual power plant that would allow utility companies to authorize electric vehicle (EV) owners, property owners, and other energy consumers to use and pay for electricity as well as act as energy providers during periods of high demand. The application tracks when energy is being drawn or returned, creating a history of credits and debits that are recorded on a decentralized ledger. With this, users can monitor these transactions which enhances the transparency and traceability of the application.

Freight Management

The Freight Management application uses distributed ledgers to track packages and verify freight contracts. Entries within the distributed ledger can be used to record package status and relevant terms and contracts to ensure accuracy, mutual agreement, and ease of reference for every stage of a freight trip. This application also enables interaction with Internet of Things (IoT) devices that can automatically monitor shipping conditions and calculate any relevant impact to final invoices. This application has been deployed and is already available for companies to use.

Usage-based Fees (UBF)

The Usage-based Fees (UBF) application would use a distributed ledger-based platform for assessing and collecting UBF for vehicle miles traveled (VMT). This would allow states and/or the Federal government to shift away from the present gasoline tax structure used to fund infrastructure projects. The DLT platform would enable automated collection through smart contracts and may be flexibly adapted to various activities, factors, and use cases. The distributed ledger platform can also be used to provide incentive to the users for using public transit and other shared mobility options and/or reduce the assessed UBF based on socio-economic indicators.

Security and Credential Management (SCMS)

This application would be used to augment misbehavior detection among Security Credential Management Systems (SCMS) used to identify malfunctioning or malevolent connected vehicle (CV) on-board units (OBUs) or roadside units (RSUs). An SCMS provisions certificates to field and vehicle devices which allow other devices to know that device is trustworthy. If a vehicle OBU or RSU device is misbehaving, the device's current and future certificates are added to a Certificate Revocation List (CRL) and blacklisted by the SCMS registration authority (RA). The loss of certificates lets other devices know that the OBU/RSU messages are not to be trusted and the devices receiving those messages will not act on them. The use of distributed ledger would allow for scalability of the CRL, permitting segmentation across states and allowing for flexibility as users travel within and between states.

Users and User Needs

Identification of Users

This report listed the users and stakeholders that were identified as relevant in the Task 2 Report and sorted them into six categories for the purpose of identifying high-level trends and to ensure that the User Needs accurately represent the needs of all stakeholders. The six categories that were used are Public Institutions, such as State and local DMVs; Logistics-Focused Organizations, such as logistics companies; Vehicle-Focused Organizations, such as manufacturers; Vehicle Operators, such as end users; Infrastructure-Focused Organizations, such as building owners; and Non-Transportation Institutions, such as utility companies.

Identification of User Needs

User needs provide the foundation of subsequent systems engineering processes and are of critical importance to ensure that solutions effectively and completely target gaps in the existing system. User needs may be used to derive system requirements and key design elements.

A user need is an expression of a required capability of the system, stated in a way that is uniquely identifiable, describes a major desired capability, is solution-free, and captures its own rationale. These needs were identified and developed in relation to the selected distributed ledger applications. Section 3.3 contains a table listing 66 User Needs identified in this project, organized by User Need ID.

Gap Analysis

Current State of Distributed Ledger Applications

- **Multimodal trip planning and fare payment system:** This application has been deployed using other technologies, but a distributed ledger-based application has yet to be implemented. There is an existing use case in ITS for a distributed ledger-based platform, a Mobility as a Service (MaaS) marketplace, which integrates mobility data from multiple service providers and optimizes trip planning for travelers, while ensuring fair revenue allocation to providers and increased transparency for all parties.
- **Transportation-based virtual power plant:** This application is currently being piloted by IBI Group, SWTCH Energy Inc., and Slate Asset Management. The IBI Group-led Smart City Sandbox launched a distributed ledger-based, electric vehicle-to-building pilot. This pilot study, active in Toronto, utilizes distributed ledger technology to explore viability of vehicle-to-grid (V2G) charging for multi-tenant office buildings where EV owners can lend electricity to the building during peak hours.
- **Freight management:** Distributed ledger-based freight management systems are offered as products by some logistics firms, and several high-profile partnerships have been successfully instituted, such as with Walmart Canada. However, such solutions are still somewhat novel and the capabilities and integration with distributed ledger technologies are under development and expansion.
- **Usage-based fees:** This application is currently being piloted; however, the pilot has been deployed without a distributed ledger. This mileage-based user fee pilot application is deployment ready with strong concerns about privacy, equity, and administrative costs.

- **Security and Credential Management:** This SCMS application is currently a conceptual use case as current SCMS systems do not utilize DLT.

Desired State of Distributed Ledger Applications

- **Multimodal trip planning and fare payment system:** This application will connect users to various surface transportation modes and providers in a geographic area and allow them to make a single secure payment when booking their trip in advance. Users will receive optimized trip plans based on their needs which saves them time while helping to reduce their carbon footprint. Distributed ledger will automate the fare revenue allocation process amongst providers using smart contracts.
- **Transportation-based virtual power plant:** The application will display nearby vehicle-to-grid charging locations and offer financial incentives to EV owners who utilize the two-way charging technology to share their electrical power.
- **Freight management:** A distributed ledger freight management application will provide a standardized digital process for tracking products which saves times and improves data accuracy. Real time measurements and calculations will be collected from internet of things (IoT) devices to verify that the product arrived in the agreed upon condition. Additionally, manufacturers will be able to upload proof of authenticity to the app to prevent fraud and identify counterfeit products/drugs.
- **Usage-based fees:** Data from various VMT tracking technologies such as smart phones apps, fueling stations, and on-board telemetric devices, will be consolidated to get an accurate VMT value. Users will be informed of accurate taxes and fees associated with the usage-based taxation system. Lastly, there will be lower administrative costs due to distributed ledger managing automated payments and VMT data collection and tracking.
- **Security and Credential Management:** This application will provide a misbehavior detection and reporting capability that provides a mechanism for local devices to quickly identify devices that are no longer trustworthy while still supporting a nationwide certificate revocation. The application detailed below would allow local devices to write and verify misbehavior into a distributed ledger which would be available for all local devices to use as a way to determine if a local device is no longer trustworthy. The Misbehavior Authority can then track the distributed ledger and generate CRL updates like the existing system.

Current Gaps of Distributed Ledger Applications

- **Multimodal trip planning and fare payment system:** To get from the current state to the desired state of a distributed ledger-based multimodal trip planning application, the only aspect missing from existing projects is the lack of general transit feed specification (GTFS) and general bikeshare feed specification (GBFS) standards adoption by transit agencies and mobility service providers.
- **Transportation-based virtual power plant:** While this application is functioning as it should, to reach desired state, many more buildings and homeowners must be encouraged to adopt this technology and participate in an EV charging infrastructure. Additionally, the accessibility of the EV charging stations must meet the standards and regulations of the FHWA National Electric Vehicle Infrastructure Standards and Requirements.

- **Freight management:** Solutions are still somewhat novel and the capabilities and integration with distributed ledger technologies are under development and expansion. Some areas still under development are the scaling of the system and the immutability of data.
- **Usage-based fees:** To reach the desired state of a distributed ledger-based usage-based fee application, the primary challenges learned from the STSFA pilots must be addressed. The challenges of the current system include concerns of privacy, equity, and administrative costs. To address these challenges, the system would need to have the ability to protect users' personal data, provide users the option to turn off location sharing, retrieve data from various VMT tracking devices, fund the incentives for users, and obtain acceptance from the public.
- **Security and Credential Management:** The gaps addressed by the SCMS DLT misbehavior reporting application would be the need for a real time mechanism for CV devices to determine trustworthiness of other CV devices in real time. The current system relies on a central MA that can take days to update the CRL and then weeks to have all devices download and apply the CRL update, providing a large timeframe when a misbehaving device would be able to keep operating.

Use Cases

Multimodal Trip Planning and Fare Payment System Use Cases

- **Universal Wallet for Interoperability, Identity and Payment Credentials:** A key functionality of a universal wallet is its ability to facilitate users in searching, booking, and paying for a range of mobility services within a single digital platform. It eradicates the need for individual applications, logins, or payment systems. The interoperability enabled by a universal wallet eliminates the need for all providers to join a single platform, often run by a competitor, and the resulting tendency for "winner take all" outcomes.
- **Data Privacy for Ecosystem Stakeholders:** A privacy-preserving approach leveraging distributed ledger and integrating DIDs and VCs addresses these issues by creating an environment where sensitive data is protected and unnecessary exposure of information is minimized. This is facilitated through zero-knowledge proof (ZKP) techniques that allow the validation of necessary information without exposing the actual data. Within this framework, each traveler has a unique SSDT that is recognized across all services, thereby reducing the need to expose personal information at every interaction. Transactions are acknowledged with VCs, negating the need for each provider to directly handle or store sensitive customer data.
- **Ability to Verify/Validate Identities and Transactions with a Zero Trust Architecture:** Implementing Zero Trust Architecture (ZTA), underpinned by W3C DIDs, anchored on public distributed ledgers and leveraging VCs, offers a compelling solution. The ZTA paradigm operates under a 'never trust, always verify' approach, and the use of these novel technologies minimizes the risk of data breaches and internal threats. By granting least privilege access and continuously verifying identities and devices, a ZTA approach amplifies a multimodal transportation system's security posture.

Transportation-based Virtual Power Plant Use Cases

- **Grid Load Balancing Leveraging EV Batteries:** Endowing EVs and their owners, as well as grid operators and their assets, with DIDs anchored on a public distributed ledger enables the

integration of the EV's battery system and chargers with several layers of grid control systems for managing load through control of charging, both unidirectional and bi-directional.

- **Global Battery Passport:** A battery passport is nothing but a presentation of data points about a particular battery – i.e., who manufactured it, its physical and chemical composition, its current State of Health (SOH), whether it was refurbished or repurposed from another battery, etc. The battery passport has many uses. For example, regulators can reference a battery passport to verify whether that particular battery is composed of an adequate proportion of recycled material. Likewise, battery passports enable battery owners to query their battery's SOH.
- **Battery State of Health:** Vehicle owners can use the battery SOH data to determine when to replace a battery and assess their EV's value based on remaining capacity. Battery performance, especially the SOH, will be a key parameter that will influence consumers' vehicle buying choices. Battery SOH (current state and history) can be included in the distributed ledger so that the data becomes tamper evident against possible fraud in order to conflate the value of batteries and electric vehicles.

Freight Management Use Cases

- **Industry-Wide Service Performance Based Reputation System for Carriers:** Shippers, third-party logistics providers (3PL), and fourth-party logistics providers (4PL) hire carriers to move their shipments. Before hiring the carriers, they must screen them for performance metrics such as reputation, safety history, financial performance, etc. Shippers use the FMCSA database to screen based on safety and out-of-service flags. They use various commercially available credit reports to understand the financial status of carriers. However, they do not have a system by which they can screen the carriers for their on-time delivery/pickup performance.
- **Multijurisdictional Automated Cargo Clearance at Ports:** At marine ports, multiple government and non-government entities operate to facilitate inflow, storage, cargo loading/unloading, outflow, safety screening/inspections of cargo, payments, and customs clearance. In most ports, these entities operate in silos and share data on a limited basis although they all have a common mission to process cargo in the minimum amount of time without compromising the security and illegal movement of goods. An automated one-stop clearance system will allow all these entities to collaboratively share data with each other or with the system such that 1) all the entities are accountable to perform their duties in a timely fashion, 2) it provides traceability and visibility to the cargo owners, and 3) entities can share risk related information with each other to screen potential bad actors in the marine port value chain.
- **Actual Weight-Based Road Usage Charging of Trucks:** Road Usage Charging (RUC) based on actual traveled distance using odometer data or telematics is a widely known concept and has been piloted in several states in the US. In the freight industry, it is prudent to track the amount of weight a given truck carries over a reported distance. In order to implement weight-based RUC, the shipper must provide information about the weight, shipment info, truck identity, etc., to the state agency, which must then reconcile the truck's mileage with the weight information. The use of a distributed ledger can enhance efficiency in this process and allow trucking companies to view details about their charges by querying smart contracts or similar on-chain logic execution mechanisms.

Usage-based Fees Use Cases

- **Dynamic and Decentralized Curb Management:** This proposed solution envisions a system where zones can be dynamically altered from parking lanes to loading lanes to traffic lanes based on real-time conditions or the time of day. Furthermore, it introduces an efficient method for monitoring usage, reserving space, and enabling online payments without sharing user PII or the need for a mega platform provider.
- **Dynamic and Decentralized Tolling and Road Usage Charging (RUC):** A dynamic, decentralized tolling and RUC system, integrated with vehicle telematics, can capture all pertinent data required to accurately determine the marginal cost of a given vehicle's trip and, by proxy, determine the optimal fee. Moreover, it could automate the onerous identity/transaction authentication/validation costs that drive a high cost of collection in today's operating RUC systems.
- **Usage-Based Insurance (UBI):** Modern geolocation technologies, combined with vehicle identifiers, ZKPs, and distributed ledger networks, enable new and better ways of underwriting auto collision and liability risk without sharing PPI. With a better understanding of risk, better underwriting will improve insurance product pricing for consumers and align incentives to improve driver behavior, saving lives and reducing injuries.

Security and Credential Management Use Cases

- **Distributed Ledger Approach to Misbehavior Detection Reporting:** This use case identifies an approach for reporting misbehavior within a connected vehicle system by having misbehavior detection devices writing observed misbehavior to the distributed ledger where other devices within range would verify that misbehavior report and write it to the distributed ledger. Local devices could then utilize the distributed ledger to determine trust in local devices based on their certificates. A misbehavior authority would monitor this distributed ledger and generate a certificate revocation list (CRL) or separate untrusted device distributed ledger (which would utilize the linkage authorities to remove trust for all certificates associated with a misbehaving device.
- **Use of Federated Certificate Authority to Register Object Identifiers:** Vehicle-to-Everything (V2X) communication relies on wireless objects exchanging information in real time. The objects exchanging information must trust each other to do so. It would be computationally infeasible for the objects to verify messages from other objects every time messages are exchanged. A Federated Certificate Authority (FCA) is an innovative approach to digital identity and security in decentralized systems. It's a collective of member organizations that jointly provide trust services in a decentralized manner. In a typical FCA setup, each participating entity operates one or more nodes that are part of the overall network. These nodes have the ability to issue, validate, and revoke certificates within their domain of authority.
- **Federated Certificate Authority for Secure API Access Management:** APIs (Application Programming Interfaces) have become essential tools, they act as bridges connecting various components of modern transportation systems, be it vehicle-to-infrastructure communication, telematics data sharing, or fleet management solutions. In this context, every component, whether it's an application within a car's onboard system or a microservice in a traffic management solution, is granted a distinct identity by the FCA. These certificates act as digital identities, authenticating each component when it tries to access or communicate via an API.

- **Federated Certificate Authority for Secure Multi-Party Computation:** Intersection safety is of paramount importance in the domain of contemporary transportation. Secure Multi-Party Computation (SMPC) allows for a collaborative computation among various vehicles and infrastructure components based on shared data, without the revelation of individual inputs. This collaborative approach is especially beneficial for complex scenarios such as traffic flow optimization at intersections, where discrete data sharing is necessary without compromising on individual data privacy. The efficacy of SMPC, however, hinges on the trustworthiness of the participants, which is addressed by the Federated Certificate Authority (FCA).

Conclusions and Next Steps

This report expands on the work from the Task 2 report: *Potential Categories for the Application of Blockchain in Intelligent Transportation Systems (ITS)* by conducting a gap analysis on five selected distributed ledger applications from this report. The gap analysis was conducted by first determining the current state of these applications, (1) Multimodal Trip Planning and Fare Payment System, (2) Transportation-based Virtual Power Plant with Payment, (3) Freight Management, (4) Use-based Fees, and (5) Security and Credential Management (SCMS), and then determining the desired/future state of these applications based on stakeholder feedback and literature reviews. Gaps were then identified by determining what steps, if any, could be taken to get from the current state to the future state for a given application. Sixteen use cases were developed, providing real-world scenarios to illustrate how a distributed ledger could potentially or is currently being used to advance the current state of the five applications to their desired/future state.

The use cases and gap analysis presented in this report have been validated with internal USDOT stakeholders prior to publication. These materials will be used to develop a comprehensive research plan structured to further explore the application of distributed ledger to ITS solutions and provide inputs to ITS JPO Program Areas. This research plan is expected to be completed in late 2023 and remain an internal USDOT document. ITS JPO will collaborate with modal partners, where appropriate, to conduct the necessary research activities.

1. Introduction

The purpose of this document is to build off the previous Task 2 report: *Potential Categories for the Application of Blockchain in Intelligent Transportation Systems (ITS)*[1]. In that document, 15 potential distributed ledger technology (DLT) applications for ITS are summarized. These summaries assessed the possibilities of integrating DLT, into real-world transportation scenarios. DLT is an umbrella term that encompasses any system that relies on a shared database to process, record, and verify transactions in an open network just like a record keeping where several parties add records to a database and each party's copies are kept in sync (Abrol 2022).

This document will be an Operational Concept report of potential use cases for five selected applications detailed in the prior report. This report will serve as a foundation document for future research including system development or pilot demonstration.

1.1 Background

Across the connected mobility ecosystem, there are thousands of service providers and governmental agencies with unique databases, processes, and regulations for handling business data and customer personally identifiable information (PII). The digitization of business processes has undergone a significant transformation in recent years, accelerated by the COVID-19 pandemic. However, such rapid transformation has not been without its consequences. The centralized systems that dominate today's internet are vulnerable to exploitation — 40% of online traffic originates from malicious bots, with cybercrime causing $10.5T in damage annually by 2025 (almost 10% of the projected 2025 global GDP, with an annual accelerating growth rate of 15%) (Baseline Technical Steering Committee 2022). This means that the cost of trust is growing exponentially for organizations around the globe, threatening the profitability of new and existing digital businesses.

Currently, it is impossible to automate business processes across organizations and jurisdictions without connecting to centralized platforms and/or databases. However, the sheer amount of stakeholders involved means that the frictional cost of trust is extremely high, and centralized systems lack the interoperability and data security needed to address the challenges facing the ecosystem. Digital transactions today rely on identities issued by centralized platforms to prove their credentials. However, in addition to being vulnerable to fraud, identity theft, and data leaks, centralized approaches to identity management fail to address the trust problems created by the rise of decentralized services, IOT, and artificial intelligence (AI). As digitization continues to progress, it will become increasingly challenging —

[1] https://rosap.ntl.bts.gov/view/dot/68176

and costly — to verify data authenticity, secure digital perimeters, and ensure cross-jurisdictional regulation compliance.

Overcoming these challenges needs a decentralized, distributed framework, “Zero Trust”, in which every entity is required to always authorize every other entity for every single digital interaction. Distributed ledgers have been called a “trust machine”, a technology for replacing trust services — including but not limited to authority, identity verification, assurance, and settlement — traditionally offered by banks, escrows, fiduciaries, accountants, registries, and, more recently, digital mega-platforms.

1.1.1 Distributed Ledger Technology

To identify potential distributed ledger applications in the transportation and ITS industry, it is important to review some basic definitions and terminologies related to distributed ledger technology. Several distributed ledger technology definitions have emerged since its inception. For this document, the resources from International Business Machines (IBM) are utilized to define distributed ledger, the importance of distributed ledger, key elements of a distributed ledger, types of distributed ledger as well as benefits of distributed ledger (“What is Blockchain Technology?” n.d.).

Simply put, a distributed ledger is made up of blocks, which contain information, and are chronologically connected. Peer-to-peer nodes contain copies of the distributed ledger. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. New blocks are created when new information is added. The information in those blocks is secure because a distributed ledger is a shared, immutable ledger that requires a consensus on data accuracy from all network members. A distributed ledger facilitates the process of recording transactions and tracking assets in a business network, and all validated transactions stored are immutable because each link in the distributed ledger is verified by a cryptographic signature. To modify any block, every subsequent block must be modified as well. A small change to earlier part of the ledger would be immediately detectable. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a distributed ledger network through unique digital identifiers, reducing risk and cutting costs for all involved.

1.1.2 Key Elements of a Distributed Ledger

DLT, immutable records, and smart contracts are the key elements of a distributed ledger. In a distributed and decentralized ledger, all network participants have access to the distributed ledger and its immutable record of transactions. This means that no participant can change or alter a transaction after it has been recorded to the shared ledger. The access can be restricted based on permissions granted by the ledger administrators. Smart contracts refer to a set of rules, simple if/then statements, that are stored on a distributed ledger and executed automatically once the predetermined conditions are met. They are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss. Within these agreements, participants must determine how transactions and their data are represented on the distributed ledger, agree on the if/then rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

1.1.3 Types of Distributed Ledger Networks

There are four main types of distributed ledger networks: public, private, permissioned, and consortium distributed ledger. A public distributed ledger network is one with no authorized authority, that anyone can

join. While anyone can join this distributed ledger network, a public distributed ledger is still secure due to the number of nodes validating transactions and the immense computational cost to create fake transactions. If an attacker wanted to modify a distributed ledger, they would need to change the block containing that record, as well as those linked to it to avoid detection. In addition to security, the advantages to a public distributed ledger are openness and transparency for users, while the disadvantages are scalability and potential of excessive energy consumption.

In contrast, a private distributed ledger network is a decentralized, peer-to-peer network controlled by one authority. This authority controls who is, and is not, allowed to join the distributed ledger. Private distributed ledgers can be more secure because of this. However, due to the limited number of nodes, there is a higher risk of someone on the inside disturbing the distributed ledger. A benefit of this distributed ledger is that it is faster and easier to scale.

A permissioned or hybrid distributed ledger network is a combination of a public and private distributed ledger. This type of network places restrictions on who is allowed to participate in the network and in what transactions. Participants need to obtain an invitation to join, making this type of distributed ledger network very secure.

Lastly, a consortium distributed ledger is controlled by multiple organizations who have the authority to determine who may submit transactions or access the data. Similar to a private distributed ledger, a consortium distributed ledger controls who is, and is not, allowed to join the distributed ledger, also making it secure. This type of distributed ledger is ideal for businesses when all participants need to be permissioned and have shared responsibility for the distributed ledger.

1.1.4 The Potential for Distributed Ledger in ITS and Transportation

Centralized nature of existing transportation/ITS applications often leads to insufficiencies resulting in limited coordination among mobility service providers, unauthorized access to data leading to data breaches and tampering, vulnerability to cyberattacks, as well as increased time to resolve payment conflicts. For example, mobility service providers often operate in silos (i.e., less integrated with other modes of transportation) with centralized access to the mobility data leading to fewer trip options for the public (end users). Users must book and pay for multiple legs of a one-way journey using different applications due to lack of coordination among modes. This can lead to unpleasant mobility experience and discourage the use of shared mobility options, including transit.

Further, many of the current ITS applications involve maintaining centralized databases (i.e., real-time traffic data, incidents, crashes, asset management, etc.), real-time transactions (i.e., transit fares, digital tickets, parking fee, etc.), as well as credential management (i.e., security credential management system [SCMS] for connected and autonomous vehicles). Centralized databases are often prone to cyberattacks and fraud.

Due to these limitations of centralized means at scale, distributed ledger technologies called Web3[2] and standards created by the World Wide Web Consortium (W3C) for Self-Sovereign Digital Twins (SSDTs) have been proposed to facilitate decentralized solutions at scale. An SSDT is a digital representation of a physical object or system that can automatically generate standardized W3C Verifiable Credentials (VCs). SSDTs can authenticate their identity and selectively disclose pertinent information/data (as VCs) without the need to connect to centralized databases. SSDTs enable trusted multiparty business automation through:

- Verification and validation of identities and transactions
- Creation of regulation-compliant data privacy solutions for users and providers
- The ability to obtain information/data at the moment of a transaction and monetize connected data without the need to open up databases or store the data
- Platform-agnostic “universal translators” that work with any legacy system to avoid having to build new infrastructure and thousands of bespoke Application Programming Interfaces (APIs)

These Web3 transactions work best in large and complicated networks where the frictional cost of trust is high. Within a single or small group of organizations, there are simpler and cheaper ways to establish trust, data provenance, and transaction integrity. As a result, distributed ledger proof-of-concepts (POCs) developed by a single or small group of organizations, while often technically successful, cannot scale up. Scaling up requires:

- A “minimum viable community” operating with shared standards (e.g., data schemas, communication protocols, settlement methods, and ways of verifying participant identities).
- Community owned and operated federated network infrastructure.

While almost anything can be put on a distributed ledger, most things should not be put on-chain. Sensitive personal and business information should be stored off-chain. Distributed ledgers make for inefficient databases, as distributed ledger-based trust alternatives impose significant overhead and must be used judiciously. Understanding where to use distributed ledgers requires an understanding of the limits of centralized data and platform solutions — as well as the advantages offered by distributed ledgers. Using SSDTs with W3C Decentralized Identifiers (DIDs) anchored to distributed ledgers and VCs in federated networks enables the best of both worlds: tamper-evident, redundancy, and transparency; data privacy and security (instead of connecting to databases, data is pushed to the edge for

[2] Web 3.0, also known as Web3, is the third generation of the World Wide Web. Web 3.0 is meant to be decentralized, open to everyone (with a bottom-up design and built on top of distributed ledger technologies and developments in the Semantic Web, which describes the web as a network of meaningfully linked data (Burdova 2022).

transactions); and fraud resistance of public distributed ledgers combined with the speed, efficiency, and low cost of cloud data storage.

This document provides an overview of selected DLT-based applications in transportation, identifies user groups and their needs, determines gaps in functionality for these applications in ITS, and detailed Use Case(s). The applications in this report were previously selected based on a literature review of existing distributed ledger applications, a review of relevance to U.S. DOT's strategic goals and research plans, and input from U.S. DOT.

1.2 Organization of the Report

This document is organized into the following chapters:

Section 1: Introduction – This section provides an overview of this document.

Section 2: Overview of Selected Distributed Ledger Technology Applications – This section summarizes the selected distributed ledger applications, based on the one-page summaries from the Task 2 Report.

Section 3: Users and User Needs – This section identifies the user groups relevant to each application and describes their needs.

Section 4: Gap Analysis – This section conducts an analysis of each application to determine the gaps between their current states and their desired states.

Section 5: **Use Cases** – This section provides example use cases for each application to describe their function and how the distributed ledger applications could bridge the gaps identified in Section 4.

Section 6: Conclusions and Next Steps – This section provides summary remarks and next steps for this project.

Appendix A: References – References cited in this document.

2 Overview of Selected Distributed Ledger Applications

As noted in the Introduction, U.S. DOT selected five applications out of the 15 identified in the Task 2 report: *Potential Categories for the Application of Blockchain in Intelligent Transportation Systems (ITS)*. Each of the five applications is summarized below and includes the rationale for each application's selection. For detailed information on the 15 applications, please see the Task 2 report.

2.1 Multimodal Trip Planning and Fare Payment System

The Multimodal Trip Planning and Fare Payment System application is a distributed ledger-based multimodal trip planning application that allows users to plan, book, and pay for a multi-leg trip or journey from an origin to a destination. Data from multiple mobility service providers is integrated into a decentralized ledger based on data sharing agreements via smart contracts. This allows users to plan and book their multimodal trip from a variety of options integrated in the distributed ledger application, rather than booking multiple trips on different platforms. Users would only need to make a single payment to a distributed ledger-based application, which would use smart contracts to automatically handle revenue splitting among the participating mobility providers.

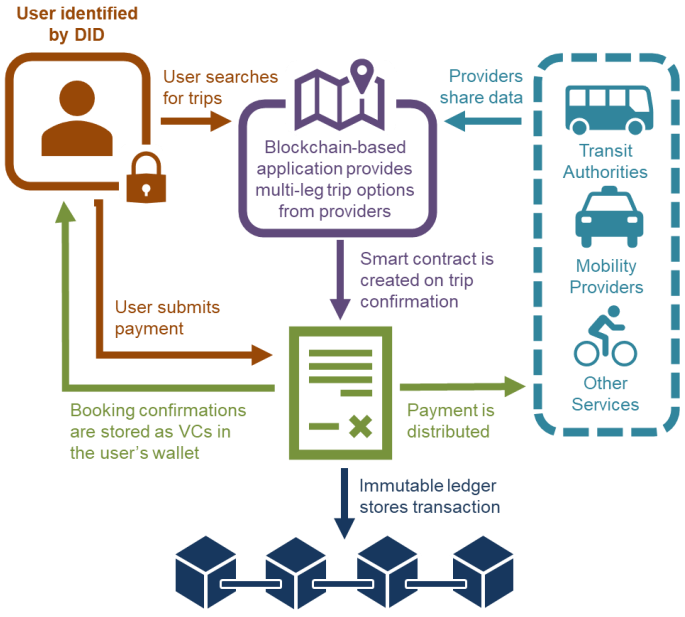

Figure 1: Distributed Ledger Application for Multimodal Trip Planning and Fare Payment

Additionally, the user's single payment method is interoperable between regions, so it can also be used when traveling to another marketplace's service area. Similar deployments that do not leverage DLT have already been realized in international markets; this distributed ledger-based application has been selected

due to the quantity of information readily available and the existing Mobility as a Service (MaaS) platforms and active pilot projects that show real-world benefits. In addition, this distributed ledger-based multimodal trip planning application was chosen due to the relevance it serves to four of the U.S. DOT's strategic goals: mobility, equity, climate and sustainability, and transformation.

2.2 Transportation-based Virtual Power Plant with Payment

The Transportation-based Virtual Power Plant with Payment application is a distributed ledger-based virtual power plant that would allow utility companies to authorize electric vehicle (EV) owners, property owners, and other energy consumers to use and pay for electricity as well as act as energy providers during periods of high demand. The application tracks when energy is being drawn or returned, creating a history of credits and debits that are recorded on a decentralized ledger. With this, users can monitor these transactions which enhances the transparency and traceability of the application. The overall data security, privacy, transparency, visibility, and immutability, ensures efficient, trusted, traceable, and auditable energy sourcing. There is currently an active pilot study to explore this application, and there is copious real-world information available. Due to this, and the relevance to four of the U.S. DOT's strategic goals: economic strength and global competitiveness, equity, climate and sustainability, and transformation, the distributed ledger-based virtual power plant application was selected for further analysis.

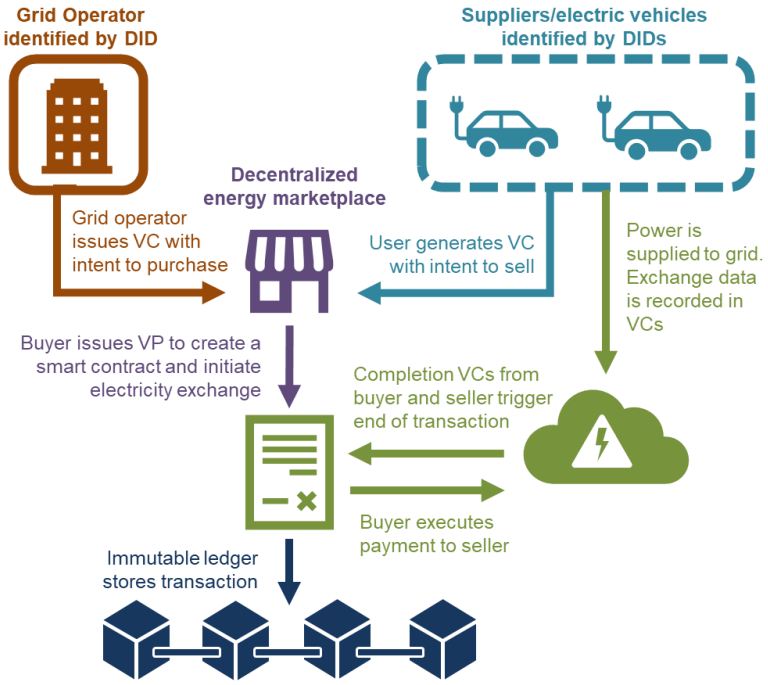

Figure 2: Distributed Ledger Application for Virtual Power Plant

2.3 Freight Management

The Freight Management application uses distributed ledgers to track packages and verify freight contracts. Entries within the distributed ledger can be used to record package status and relevant terms

and contracts to ensure accuracy, mutual agreement, and ease of reference for every stage of a freight trip. This application also enables interaction with Internet of Things (IoT) devices that can automatically monitor shipping conditions and calculate any relevant impact to final invoices. This application has been deployed and is already available for companies to use. While advanced capabilities are still under development, distributed ledger-based freight management system solutions have established the capability to scale effectively and have potential for both overland and oversea freight. Due to the prevalence of this application in the real-world, the abundance of information available, and the relevance of the application to the U.S. DOT's strategic goals, this application was selected for further analysis and potential next steps.

2.4 Usage-based Fees (UBF)

The Usage-based Fees (UBF) application would use a distributed ledger-based platform for assessing and collecting UBF for vehicle miles traveled (VMT). This would allow states and/or the Federal government to shift away from the present gasoline tax structure used to fund infrastructure projects. The DLT platform would enable automated collection through smart contracts and may be flexibly adapted to various activities, factors, and use cases. The distributed ledger platform can also be used to provide incentive to the users for using public transit and other shared mobility options and/or reduce the assessed UBF based on socio-economic indicators. All would be administered and verified on the distributed ledger, allowing for increased transparency and traceability into UBF collection, excise, and tax collection. In addition to this application encouraging and promoting more sustainable modes of transportation, it also allows for increased efficiency and reduced administrative costs associated with distributed ledger-based automatic payment processing and validation. There are currently pilot projects for this application in deployment and more to come. This application has been selected because of the quantity of information readily available and the relevance it serves to three of the U.S. DOT's strategic goals: mobility, economic strength and global competitiveness, and climate and sustainability.

2.5 Security and Credential Management (SCMS)

This application would be used to augment misbehavior detection among Security Credential Management Systems (SCMS) used to identify malfunctioning or malevolent connected vehicle (CV) on-board units (OBUs) or roadside units (RSUs). An SCMS provisions certificates to field and vehicle devices which allow other devices to know that device is trustworthy. If a vehicle OBU or RSU device is misbehaving, the device’s current and future certificates are added to a Certificate Revocation List (CRL) and blacklisted by the SCMS registration authority (RA). The loss of certificates lets other devices know that the OBU/RSU messages are not to be trusted and the devices receiving those messages will not act on them. The use of distributed ledger would allow for scalability of the CRL, permitting segmentation across states and allowing for flexibility as users travel within and between states. In turn, this ensures that devices only receive relevant information and the CRL is more manageable. Additionally, the use of smart contracts allows for automated removal and re-addition to the list based on compliance with performance criteria. This application is currently conceptual and has not been deployed yet, it has been selected for further analysis because of the relevance to the U.S. DOT’s strategic goals and research plans.

3 Identify Users and User Needs

This section identifies and classifies users for the proposed distributed ledger applications. Different users, which have already been identified based on work in the Task 2 Report, will generally have different use cases for distributed ledger applications, but they may be sorted into broader classifications based on their needs and capabilities.

3.1 Identification of Users

The flexibility of distributed ledger technologies and the diversity of proposed applications mean that there is a broad range of users and stakeholders. Most applications are relevant to multiple stakeholder groups. The users and stakeholders that have been identified as relevant in the Task 2 Report are listed below in Table 1.

Table 1: Users and Stakeholders Identified Across Proposed Applications

Stakeholder	Description
Building and Lot Owners	People or corporations that own or have construction rights to property
Charging Stations	Owners and operators of electric-vehicle charging stations
Departments of Motor Vehicles (DMVs)	State agencies responsible for administrating motor vehicle licensing and registration
Emergency Response Teams	Personnel involved in coordinating or executing emergency response services
Employers	Public or private organizations that employ workers; specifically, those that do or may offer subsidies or other benefits related to travel and commuting
End users	Private citizens who use the transportation network to travel to housing, employment, recreation, and other destinations

Stakeholder	Description
Federal Government	The United States government and its agencies, e.g., U.S. DOT
Financial institutions	Institutions such as banks and credit unions that are or may be involved in payment processing
Freeway and Arterial Managers	Organizations that coordinate travel along freeway and arterial corridors
Insurance Companies	Companies that offer insurance services to individuals and organizations
Independent Owner-Operators (IOOs)	Freight operators who own their own shipping equipment and contract with other companies to transport goods
Law Enforcement	Federal and local departments that engage in policing
Logistics Companies	Companies that manage or consult on freight operations
Manufacturers	Companies that manufacture vehicles and vehicle parts
Mobility Service Providers	Companies that provide or coordinate mobility services, such as micromobility or ridesharing
Non-Governmental Organizations (NGOs)	Private organizations that typically offer services independently of federal activity
Parking Authorities	Organizations in charge of enforcing parking regulations
Rental Companies	Companies that allow individuals to rent vehicles such as cars and bikes
Roadway Maintenance Crew	Individuals involved with maintaining road conditions and related infrastructure
Safety Focused Agencies	Public agencies that are partially or primarily focused on improving transportation-related safety outcomes in the United States
State and Local DOTs	Organizations responsible for managing transportation services and regulations in a state or municipality
Transportation Management Centers (TMCs)	Organizations that coordinate centralized monitoring and information distribution relating to transportation operations in an area

Stakeholder	Description
Transportation Network Companies (TNCs)	Companies that coordinate transportation services, such as ridesharing, using an app, a web platform, or other technology
Tolling Authorities	Organizations responsible for setting and enforcing tolls in an area
Transit Authorities	Agencies and other organizations responsible for operating and coordinating transit and transit policy in an area
Utility Companies	Companies that provide utilities such as water, gas, and electricity to an area
Weather Advisory Institutions	Institutions that provide weather forecasting and alert services, e.g., National Weather Service local stations

3.2 Categorization of Users

Because of the large number of users and stakeholders, it is helpful to group them in order to evaluate trends and high-level needs. This categorization allows for more general conclusions to be drawn. Moreover, as some stakeholders overlap or supersede one another—Safety-Focused Agencies are a subset of the Federal Government, for example—this sorting prevents double-counting stakeholders and helps to ensure that needs are balanced appropriately. The categorization of stakeholders is given in Table 2 below.

Table 2: Stakeholder and User Categorization

Category	Stakeholders Included
Public Institutions (PI)	DMVs, Federal Government, Freeway and Arterial Managers, Law Enforcement, Parking Authorities, Roadway Maintenance Crews, State and Local DOTs, TMCs, Tolling Authorities, Transit Authorities, Safety Focused Agencies
Logistics-Focused Organizations (LFO)	Logistics Companies, Rental Companies, TNCs

Category	Stakeholders Included
Vehicle-Focused Organizations (VFO)	Manufacturers, Mobility Service Providers
Vehicle Operators (VO)	End Users
Infrastructure-Focused Organizations (IFO)	Building Owners, Charging Stations, IOOs
Non-Transportation Institutions (NTI)	Emergency Response Teams, Employers, Financial Institutions, Insurance Companies, NGOs, Utility Companies, Weather Advisory Institutions

3.3 Identification of User Needs

User needs provide the foundation of subsequent systems engineering processes and are of critical importance to ensure that solutions effectively and completely target gaps in the existing system. User needs may be used to derive system requirements and key design elements.

A user need is an expression of a required capability of the system, stated in a way that is uniquely identifiable, describes a major desired capability, is solution-free, and captures its own rationale. The following table lists the User Needs identified in this project, organized by User Need ID. The table maps the user categories to relevant user needs; not all user needs are relevant to a user category in all circumstances, and needs are often shared by more than one user category. These needs were identified and developed in relation to the selected distributed ledger applications.

Table 3. Distributed Ledger User Needs

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-01	Mobility providers need to be able to provide up-to-date information on their vehicles and services so that they may communicate available services to customers.	X	X	X	X	-	-
BLCN-02	Users need to be able to pay for services available to them so that they may contract those services.	X	X	X	X	-	-
BLCN-03	Users need to be able to receive information on service options available to them so they can make an informed decision based on their personal needs and preferences.	X	X	X	X	-	-
BLCN-04	Users need to be able to verify terms of contracts they enter to understand what they are agreeing to.	X	X	X	X	X	X
BLCN-05	Users need to be able to verify that the services available to them are suitable to their needs and use case so that they may contract services as appropriate.	X	X	X	X	X	X
BLCN-06	Users need to ensure their personally identifying information (PII) is protected from public exposure so that they are not at risk of having personal data made improperly available.	X	X	X	X	X	X
BLCN-07	Entities selling goods or services need to ensure they receive appropriate payment so that they may engage with the marketplace in confidence.	X	X	X	-	X	X
BLCN-08	Users purchasing goods or services need to ensure they can verify their purchases so that they may engage with the marketplace in confidence.	X	X	X	X	X	X

[3] 'BLCN' refers to Blockchain

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-09	Entities splitting revenue need to ensure that it is divided appropriately based on previously agreed upon terms so that they may conduct business in compliance with contractual agreements.	X	X	X	X	X	X
BLCN-10	Entities conducting financial transactions need to ensure that private or proprietary information is not publicly exposed so that they may conduct business in compliance with security processes and financial regulations.	X	X	X	X	X	X
BLCN-11	Entities conducting financial transactions need to ensure that their transactions are conducted securely and in a timely manner so that they may conduct business in compliance with security processes and financial regulations.	X	X	X	X	X	X
BLCN-12	Operators receiving payments for services rendered need to ensure they are compensated according to pre-established rates so that they are in compliance with any relevant contractual agreements.	X	X	-	X	X	-
BLCN-13	Regulatory bodies need to be able to ensure that usage-based or mileage-based regulations are enforced accurately so that they may ensure compliance with their regulations.	X	-	X	X	X	-
BLCN-14	Governmental bodies need to ensure that taxes, fines, and fees are levied in accordance with the tax code and other relevant legal frameworks so that they are in compliance with financial regulations.	X	-	-	-	-	-
BLCN-15	Governmental bodies need to ensure that any taxes, fines, and fees are communicated to debtors in accordance with relevant legal frameworks so that they are in compliance with financial regulations.	X	-	-	-	-	-
BLCN-16	Governmental bodies need to ensure that any taxes, fines, and fees that are levied are paid in legal tender so that they are in compliance with financial regulations.	X	-	-	-	-	-
BLCN-17	Governmental bodies need to ensure that any disclosure of PII or other potentially sensitive information is conducted in compliance with relevant laws and regulations to ensure they are operating legally and responsibly.	X	-	-	-	-	-
BLCN-18	Governmental bodies conducting financial transactions need to ensure that such transactions are auditable so that they are in compliance with financial regulations.	X	-	-	-	-	-

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-19	Connected infrastructure needs to be able to send and receive signals in a format that it is capable of properly interpreting so that it may operate as intended.	-	-	X	-	X	-
BLCN-20	Data that is gathered for the purposes of analytics needs to be transmitted and stored accurately and securely to ensure it is only accessed by the appropriate parties.	-	X	X	-	X	-
BLCN-21	Transportation management organizations need to be able to gather and analyze data relevant to their operations so that they may understand the impact of their operations and adjust them accordingly.	X	X	X	-	X	-
BLCN-22	Organizations responsible for networks need to be able to enforce cybersecurity practices and regulations so that they may ensure the safety and integrity of their network.	X	X	X	-	X	-
BLCN-23	Organizations responsible for networks need to be able to identify and appropriately deal with malicious actors attempting to interfere with network activity so that they may respond to threats effectively.	X	X	X	-	X	-
BLCN-24	Organizations responsible for networks need to be able to identify and appropriately deal with glitches or technical errors impacting equipment within the network so that the network may operate as intended.	X	X	X	-	-	-
BLCN-25	Transportation management organizations need to be able to receive and respond to traveler feedback so that they are able to understand the impact of their operations and adjust them accordingly.	X	-	-	-	-	-
BLCN-26	Users of electric vehicles need to be able to find places to charge their vehicle so that they may operate their vehicle.	-	-	-	X	X	-
BLCN-27	Owners of electric vehicle charging stations need to be able to connect to the electric grid so that they may operate their business.	-	-	-	-	X	X
BLCN-28	Owners of electric vehicles need to be able to send power from and receive power to their vehicle's batteries so that they may charge and discharge it as needed.	-	-	-	X	X	X
BLCN-29	Organizations seeking to incentivize specific behaviors among travelers need to be able to track traveler behavior so that they may analyze it and design their incentives appropriately.	X	X	-	X	-	-

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-30	Organizations seeking to incentivize specific behaviors among travelers need to be able to distribute benefits to individual travelers based on their behavior so that they may influence traveler behavior..	X	X	X	X	-	-
BLCN-31	Travelers need to be able to apply received credit towards appropriate goods and services so that they may be able to utilize allotted benefits.	X	X	X	X	X	X
BLCN-32	Travelers need to be able to be informed about benefits and disbenefits that may be relevant to them so that they may make informed decisions about their travel.	-	-	-	X	-	-
BLCN-33	Organizations seeking to implement emissions-based benefits programs need to be able to receive data about specific vehicle and mode emissions so that they may perform accurate analyses.	X	-	X	-	X	-
BLCN-34	Transportation management organizations need to be able to share data on road conditions with travelers so that they may respond to current conditions and minimize risk exposure to travelers.	X	-	-	X	-	-
BLCN-35	Transportation management organizations need to be able to gather weather-related data on road conditions so that they may respond to current conditions and minimize risk exposure to travelers.	X	-	-	-	X	X
BLCN-36	Transportation management organizations need to be able to aggregate and analyze data from multiple sensors or instruments so that they may perform their coordination duties effectively.	X	-	-	-	X	-
BLCN-37	Connected vehicles need to be able to communicate with connected infrastructure devices so that they may operate as intended.	X	-	X	-	X	-
BLCN-38	Transportation management organizations need to be able to verify and validate data received from sensors and instruments so that they may ensure the integrity of the instruments.	X	-	X	-	X	-
BLCN-39	Transportation management organizations need to be able to coordinate road safety measures in response to information on road conditions so that they may reduce risk exposure to travelers.	X	-	-	-	X	X

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-40	Government and non-governmental organizations need to be able to coordinate transportation-related efforts so that they can provide appropriate services to the population.	X	-	-	-	-	X
BLCN-41	Government organizations need to communicate emergency information quickly, reliably, and effectively to those in affected areas so that they can improve safety outcomes.	X	-	-	X	-	X
BLCN-42	Individuals or organizations need to be able to ship goods reliably, efficiently, and cost-effectively so that they can conduct business.	-	X	-	X	-	X
BLCN-43	Logistics companies need to track goods in their system so that they may ensure the shipment's status and integrity.	-	X	-	X	-	X
BLCN-44	Logistics companies need to coordinate shipping across multiple modes and services so that they may deliver goods using optimal combinations of modes.	-	X	X	X	-	X
BLCN-45	Logistics companies need to compensate employees and contractors fairly and accurately so that they may conduct business according to relevant contracts.	-	X	-	X	-	-
BLCN-46	Logistics companies need to be able to verify the integrity of shipments so that they may conduct business according to relevant contracts.	-	X	-	X	-	-
BLCN-47	Individuals or organizations need to be able to compensate logistics companies according to pre-agreed contract terms so that they may conduct business according to relevant contracts.	-	X	-	X	-	-
BLCN-48	Logistics companies need to be able to settle shipping disputes so that they may conduct business according to relevant contracts.	-	X	-	X	-	-
BLCN-49	Drivers need to park their vehicles legally so that they comply with all relevant parking regulations.	-	-	-	X	X	-
BLCN-50	Drivers need to access safe, affordable, accessible parking facilities so that they may secure their vehicles.	-	-	-	X	X	-
BLCN-51	Owners of parking facilities need to communicate their availability status to potential customers so that customers may select appropriate facilities.	-	-	-	X	X	-

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-52	Owners of parking facilities need to receive payments from customers so that they may operate their businesses.	-	-	-	X	X	-
BLCN-53	Regulatory agencies need to ensure that commercial drivers comply with safety regulations so that the regulations are being followed.	X	-	X	X	-	-
BLCN-54	Parking authorities need to ensure that violations of curb-space usage regulations and policies may be tracked, recorded, and penalized appropriately so that they can enforce parking regulations as necessary and appropriate.	X	-	-	X	X	-
BLCN-55	Transportation service providers need to coordinate usage of limited public-space resources so that they are available where they are needed most.	X	X	X	X	-	-
BLCN-56	Transportation service providers need to record the condition of their assets so that they are able to manage them.	X	-	X	X	-	-
BLCN-57	Transportation service providers need to access information on the status of their assets so that they are able to manage them.	X	-	X	X	-	-
BLCN-58	Transportation service providers need to ensure that their assets are maintained regularly so that they are in good condition and will not break down unexpectedly.	X	-	X	X	-	-
BLCN-59	State governments need to be able to coordinate CRLs so that they are consistent across the country.	X	-	-	-	-	-
BLCN-60	Vehicle owners/operators need to ensure the safety and security of their connected vehicles so that they will not be stolen or compromised.	-	-	X	X	-	-
BLCN-61	Vehicle owners/operators need access to real-time notifications if their vehicle's certificates are revoked or if any misbehavior is detected so that they may be able to respond to and correct the intrusion or misbehavior.	-	-	X	X	-	-
BLCN-62	Governmental Organizations need a scalable and efficient system to manage and monitor the security of connected vehicles so that such systems will be capable of handling increasing numbers of vehicles.	X	-	-	-	-	-
BLCN-63	Governmental organizations need to segment and manage CRLs across states so that they are consistent across the country.	X	-	-	-	X	-

ID[3]	Need	PI	LFO	VFO	VO	IFO	NTI
BLCN-63	Governmental organizations need to access the performance data and compliance reports so that they are able to assess the effectiveness of the SCMS system.	X	-	-	-	-	-
BLCN-64	SCMS administrators need the capability to add, remove, or revoke certificates for OBUs and RSUs so that they are able to correct oversights or errors.	X	-	X	X	-	-
BLCN-65	Vehicle manufacturers need a standardized interface for registering and updating CRLs for their vehicles so that they are consistent and comprehensive.	-	-	X	-	-	-
BLCN-66	Drivers need confidence that connected vehicles on the road are secure and not prone to malicious activities so that they do not need to anticipate unexpected or dangerous behavior.	-	-	-	X	-	-

4 Gap Analysis

This section leverages the work done for the Task 2 report, in addition to further literature review and engaging industry experts to determine the current state and the desired state for the five selected distributed ledger applications. The current state was compared to the desired state to identify the gaps that are needed to fulfill the needs and design of the application's future state. From there, strategies can be developed to close those gaps. These gaps could potentially be bridged by distributed ledgers. This is explored further in Section 5 by expanding these potential solutions into individual use cases.

4.1 Current State of Distributed Ledger Applications

4.1.1 Multimodal Trip Planning and Fare Payment System

This distributed ledger-based application is a multimodal trip planning and fare payment system. This application has been deployed using other technologies, but a distributed ledger-based application has yet to be implemented. There is an existing use case in ITS for a distributed ledger-based platform, a Mobility as a Service (MaaS) marketplace, which integrates mobility data from multiple service providers and optimizes trip planning for travelers, while ensuring fair revenue allocation to providers and increased transparency for all parties. The concept of a mobility marketplace is not new. "Whim" and "UbiGo" are considered among the early deployers of the MaaS platform featuring a combination of public transit, taxi, car rental, car-share, and bike-share trip options. Whim operates in several cities around the globe such as Helsinki, Finland; Vienna, Austria; Tokyo, Japan; etc. In addition, a distributed ledger-based MaaS pilot project, Citopia MaaS, was completed where users could plan and book multimodal trips with Citopia's distributed ledger-based platform ("Citopia MaaS — Transit IDEA Award", n.d.).

4.1.2 Transportation-based Virtual Power Plant with Payment

This distributed ledger-based application is a transportation-based virtual power plant, with payment. This application is currently being piloted by IBI Group, SWTCH Energy Inc., and Slate Asset Management. The IBI Group-led Smart City Sandbox launched a distributed ledger-based, electric vehicle-to-building pilot. This pilot study, active in Toronto, utilizes distributed ledger technology to explore viability of vehicle-to-grid (V2G) charging for multi-tenant office buildings where EV owners can lend electricity to the building during peak hours. During the pilot, the parked Nissan Leaf will store energy during off-peak hours and redistribute that energy to the building and the EV chargers in use, creating an energy flow that is cost-effective and environmentally sustainable (Edwards 2021).

4.1.3 Freight Management

This distributed ledger-based application is a freight management system, which has been deployed. Distributed ledger-based freight management systems are offered as products by some logistics firms, and several high-profile partnerships have been successfully instituted, such as with Walmart Canada. However, such solutions are still somewhat novel and the capabilities and integration with distributed

ledger technologies are under development and expansion. There are many existing use cases of distributed ledger-based freight management within transportation. Maersk and IBM have started a venture to unlock efficiency in ocean freight by establishing a global distributed ledger-based system for digitizing trade workflows and end-to-end shipment tracking (Kückelhaus and Chung 2018). A similar effort by DLT Labs was adopted by Walmart Canada in 2020. The company's product, a system called DL Freight, acts as a ledger hosting all documents and data associated with freight shipments to allow for real-time shipping charge calculations and automated verification supported by Internet of Things (IoT) devices (Smith 2020).

4.1.4 Usage-based Fees

This application is a distributed ledger-based usage-based fee application. This application is currently being piloted; however, the pilot has been deployed without a distributed ledger. This mileage-based user fee pilot application is deployment ready with strong concerns about privacy, equity, and administrative costs. The Surface Transportation System Funding Alternatives (STSFA) Program has funded pilot projects in 13 individual states as well as two coalitions of states: the Western Road Usage Charge Consortium (RUC West) and the Eastern Transportation Coalition, which both aim to test the feasibility of regional mileage-based user fee systems (Minott 2022).

4.1.5 Security and Credential Management (SCMS)

The last selected distributed ledger application is a Security and Credential Management System (SCMS). This SCMS application is currently a conceptual use case as current SCMS systems do not utilize DLT. In this application, distributed ledger can be used to augment the misbehavior detection and certificate revocation process of SCMS potentially providing a more rapid regionally focused certificate trust mechanism while still supporting a larger nationwide certificate revocation mechanism.

4.2 Desired State of Distributed Ledger Applications

4.2.1 Multimodal Trip Planning and Fare Payment System

This application will connect users to various surface transportation modes and providers in a geographic area and allow them to make a single secure payment when booking their trip in advance. Users will receive optimized trip plans based on their needs which saves them time while helping to reduce their carbon footprint. Distributed ledger will automate the fare revenue allocation process amongst providers using smart contracts. The data will be connected through a cryptographic chain of trust to ensure that it is being transferred and shared securely.

4.2.2 Transportation-based Virtual Power Plant with Payment

This distributed ledger application will meet the growing demand for EV charging infrastructure without straining the electrical grid. Lower energy and operation costs encourage building and homeowners to adopt this technology and improve the accessibility of EV charging stations. The app will display nearby vehicle-to-grid charging locations and offer financial incentives to EV owners who utilize the two-way charging technology to share their electrical power. This will promote the use and purchase of climate friendly vehicles especially for rural residents who spend more money annually on motor vehicle fuel and maintenance and housing electricity costs (U.S. Bureau of Labor Statistics 2019). According to the final

rule published by the FHWA, all publicly accessible EV chargers will need to meet standards and regulations around topics such as payment methods, availability, physical security, and data privacy ("National Electric Vehicle Infrastructure Standards and Requirements" 2023).

4.2.3 Freight Management

A distributed ledger freight management application will alleviate some of the current friction that occurs in global trade logistics such as limited visibility in the supply chain, and time-consuming manual data entry for tracking (Kückelhaus and Chung 2018). It will provide a standardized digital process for tracking products which saves times and improves data accuracy. Real time measurements and calculations will be collected from internet of things (IoT) devices to verify that the product arrived in the agreed upon condition. Additionally, manufacturers will be able to upload proof of authenticity to the app to prevent fraud and identify counterfeit products/drugs.

4.2.4 Usage-based Fees

To address privacy concerns, this app will protect users' personal data and/or provide them the option to turn off location sharing. Data from various VMT tracking technologies such as smart phones apps, fueling stations, and on-board telemetric devices, will be consolidated to get an accurate VMT value. Users will be informed of accurate taxes and fees associated with the usage-based taxation system. Incentives will encourage greater use of public transportation which will help reduce some of the harmful greenhouse gas emissions in the atmosphere. Lastly, there will be lower administrative costs due to distributed ledger managing automated payments and VMT data collection and tracking.

4.2.5 Security and Credential Management (SCMS)

This application will provide a misbehavior detection and reporting capability that provides a mechanism for local devices to quickly identify devices that are no longer trustworthy while still supporting a nationwide certificate revocation. The current SCMS systems rely on a device detecting misbehavior, generating a misbehavior report and then sending that report to a Misbehavior Authority (MA). The MA then tracks these reports and works with other certificate authorities within the system to identify all current and future certificates for the misbehaving device and updating the CRL with those certificates. This process can take days, or even weeks, for all devices within the SCMS ecosystem to update their CRLs. The application detailed below would allow local devices to write and verify misbehavior into a distributed ledger which would be available for all local devices to use as a way to determine if a local device is no longer trustworthy. The MA can then track the distributed ledger and generate CRL updates like the existing system.

4.3 Current Gap(s) of Distributed Ledger Applications

4.3.1 Multimodal Trip Planning and Fare Payment System

To get from the current state to the desired state of a distributed ledger-based multimodal trip planning application, the preexisting work done for the active Citopia MaaS pilot project could be utilized. According to MOBI, the makers of Citpoia MaaS, the only aspect missing from this project is the lack of general transit feed specification (GTFS) and general bikeshare feed specification (GBFS) standards adoption by transit agencies and mobility service providers.

4.3.2 Transportation-based Virtual Power Plant with Payment

Currently, this distributed ledger application is being actively piloted by the IBI Group in one building. While this application is functioning as it should, to reach desired state, many more buildings and homeowners must be encouraged to adopt this technology and participate in an EV charging infrastructure. Additionally, the accessibility of the EV charging stations must meet the standards and regulations of the FHWA National Electric Vehicle Infrastructure Standards and Requirements. To achieve this, all public EV chargers must improve upon payment methods, availability, physical security, and data privacy.

4.3.3 Freight Management

This distributed ledger-based freight management system has been deployed successfully and is available to many companies. However, such solutions are still somewhat novel and the capabilities and integration with distributed ledger technologies are under development and expansion. Some areas still under development are the scaling of the system and the immutability of data.

4.3.4 Usage-based Fees

To reach the desired state of a distributed ledger-based usage-based fee application, the primary challenges learned from the STSFA pilots must be addressed. The challenges of the current system include concerns of privacy, equity, and administrative costs. To address these challenges, the system would need to have the ability to protect users' personal data, provide users the option to turn off location sharing, retrieve data from various VMT tracking devices, fund the incentives for users, and obtain acceptance from the public.

4.3.5 Security and Credential Management (SCMS)

The gaps addressed by the SCMS DLT misbehavior reporting application would be the need for a real time mechanism for CV devices to determine trustworthiness of other CV devices in real time. The current system relies on a central MA that can take days to update the CRL and then weeks to have all devices download and apply the CRL update, providing a large timeframe when a misbehaving device would be able to keep operating.

5 Use Cases for Real-World Distributed Ledger Applications

This section provides use case(s) for each of the identified distributed ledger applications to address some of the gaps identified.

5.1 Multimodal Trip Planning and Fare Payment System Use Cases

The use cases below rely on an approach, loosely called “Web3” — solutions use distributed ledgers to identify network participants and their digital agents at each and every point of interaction (i.e., Zero Trust), permitting participants to control the use and dissemination of their data. The use cases and solutions below use distributed ledgers solely for the purpose of registering identifiers. To improve data security and reduce centralization, all solutions below rely on two independent networks working together, neither of which contains the full information about users, trips, and transactions. DIDs are handled in a permissioned layer 2 blockchain with DIDs currently anchored to at least one public distributed ledger, such as the Integrated Trust Network (ITN). All other interactions are managed through a decentralized marketplace for parties to interact using VCs and SSDTs, relying on the permissioned distributed ledger identifiers for mutual identity recognition.

Transit agencies and enterprise participants alike can leverage the network to unlock circular business models, monetize untapped assets, streamline low-cost business automation, and develop shared solutions with other providers in the ecosystem while maintaining a competitive edge.

By enabling the integration of countless usage-based MaaS applications for seamless multimodal trip planning, booking, and payment, a Web3 approach makes it easier to build, manage, and access secure, flexible, sustainable, and lower-cost mobility solutions.

5.1.1 Universal Wallet for Interoperability, Identity and Payment Credentials

In the realm of transportation, the concept of a universal wallet signifies a major advance in the digital infrastructure, bringing a new level of interoperability among various mobility service providers. This groundbreaking concept is poised to create a cohesive and interconnected travel ecosystem by integrating distinct elements of multimodal travel into one unified platform.

Universal wallets solve two key obstacles to widespread adoption of multimodal transportation solutions:

- First, a key functionality of a universal wallet is its ability to facilitate users in searching, booking, and paying for a range of mobility services within a single digital platform. It eradicates the need for individual applications, logins, or payment systems, thereby giving users the seamless web experience, they demand, while mitigating the complications frequently encountered in today's multifaceted, multimodal travel scenarios. A critical hurdle in modern urban mobility is the

fragmented nature of services. Travelers often grapple with multiple platforms, each with its distinct application, login credentials, and payment mechanisms.

- Second, the interoperability enabled by a universal wallet eliminates the need for all providers to join a single platform, often run by a competitor, and the resulting tendency for "winner take all" outcomes. For example, Lyft does not offer rides on Uber's platform and Whim does not offer services or expose their customers on UbiGo's platform.

The universal wallet, by providing a common point of interaction for all these services, enables interoperability, significantly reducing this complexity, and enhancing the overall user experience. Moreover, it reduces costs associated with coordination between mobility service providers, as the alternative is a patchwork approach that requires the redundant engineering of one-to-one integrations.

The potential of universal wallets extends beyond the realm of basic convenience. They are specifically engineered to accommodate individual user preferences, providing route options based on chosen parameters such as the most environmentally friendly, fastest, least expensive, or the one with the fewest transfers. This personalization aspect underscores the capacity of these wallets to optimize travel experiences, considering various factors beyond just time and cost efficiency.

Table 4. Universal Wallet for Secure Identity and Payment Credentials

Use Case Component	Description
Use Case ID	5.1.3
Use Case Name	Universal Wallet for Interoperability, Identity and Payment Credentials
ARC-IT Categorization	Public Transportation, Traveler Information
Description	A universal wallet can provide interoperability for providers and seamless trips for travelers in an ecosystem that enables riders to search, book, and pay for multimodal trips from a single gateway. Wallet interoperability offers an efficient end-to-end experience; and eliminates the need for multiple logins, user cards, apps, and payment methods. Users can personalize their trips by specifying trip preferences and choosing from route options such as greenest, cheapest, fastest, and least number of transfers.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger(i.e., Hyperledger, Ethereum)
Actors	Primary Actor: Traveler Secondary Actors: Public transit agency, mobility service provider, public and private transportation infrastructure owner
Operational Objectives/Goals	• Single login for users • Seamless trip planning and payment using a single gateway for user-defined information • No exposure of traveler banking account or payment information beyond that needed to settle their contracted trip leg

Use Case Component	Description
Constraints/ Assumptions	It is assumed that there is a wide network of mobility service providers willing to participate and collaborate in this integrated system. The readiness of these providers to share information and adapt their payment and operating systems to work cohesively with the universal wallet is a key constraint. Secondly, it is assumed that the necessary digital infrastructure (permissioned network where DIDs can be anchored, ZKP integration, etc.) is in place, and users have access to internet-connected devices to use the wallet. Additionally, the success of the universal wallet also hinges on the assumption that users are willing to adopt this new method of transaction, preferring it over traditional payment methods. Users' trust in the platform's data security and privacy measures is a critical constraint in this regard. Moreover, the implementation assumes that regulatory bodies will allow for such an integrated payment system, and it's constrained by the need to meet all local and international data protection and financial transaction laws.
Pre-conditions	Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third-party developers of Web3-compliant B2C apps for multimodal trip planning and payment that don’t expose PPI, competitive business data, or payment details.
Workflow	User Registration/Onboarding: 1. The journey with a universal wallet begins when a new user signs up and verifies their Decentralized Identifier (DID), a unique identifier that forms the basis of their account. 2. With the DID, users bypass traditional usernames or passwords for simpler access. 3. Users then personalize their profile, specifying trip preferences and payment methods which are stored as Verifiable Credentials (VCs) in the universal wallet and tied to their DID. Trip Planning & Booking 1. When planning a journey, users input start and end points, and the system generates route options based on their location and saved preferences. 2. Users then select their desired route and payment method, with the booking confirmation recorded as another VC in their wallet. 3. During the journey, the booking and payment credentials can be quickly verified through their DID and corresponding VCs.
Alternative workflow	Alternatively, the entire trip can be bid on by a given mobility service provider, who then bears responsibility for coordinating with other mobility service providers for transit at each step in the multimodal trip. The same cryptographic tools and digital infrastructure can be used to ensure data privacy for every stakeholder; this approach is simply an alternative structuring to the process of executing a multimodal trip.

Use Case Component	Description
Information Requirements	• Traveler identifying information • Mobility Service Provider identifying information • Mobility Service Provider transit offerings information • Trip information • Payments information and pricing

5.1.1.1 Implementation Barriers

Collaboration Among Providers: Success hinges on widespread adoption by various mobility service providers. This requires a degree of cooperation and data sharing that may be difficult to achieve, given the competitive nature of these industries.

Regulation and Legislation: Regulatory bodies may have concerns about coordination between disparate governmental entities, especially any multiparty business process involving traveler PII. Additionally, ensuring compliance with regulations that differ between cities, states, and nationally can be challenging.

User Adoption: The success of a universal wallet system depends on convincing a critical mass of users to switch from their current methods of payment. Factors like ease of use, trust in the system, and perceived benefits will all impact the rate of adoption.

5.1.2 Data Privacy for Ecosystem Stakeholders (Riders and Service Providers)

In today's multimodal transportation ecosystem, travelers and mobility service providers often face challenges associated with privacy and data security. A typical journey for a traveler could involve multiple touchpoints—booking a ride-hailing service, purchasing a bus ticket, renting a bike, etc. Each of these touchpoints traditionally necessitates the sharing of PII, which presents a clear risk for the exposure of sensitive data.

Similarly, mobility service providers often need to expose sensitive business data in the process of verifying transactions or ensuring service authenticity. This creates potential vulnerabilities in providers' digital business perimeters and can foster a lack of trust among users. A privacy-preserving approach leveraging distributed ledger and integrating DIDs and VCs addresses these issues by creating an environment where sensitive data is protected and unnecessary exposure of information is minimized. This is facilitated through zero-knowledge proof (ZKP) techniques that allow the validation of necessary information without exposing the actual data. Within this framework, each traveler has a unique SSDT that is recognized across all services, thereby reducing the need to expose personal information at every interaction. Transactions are acknowledged with VCs, negating the need for each provider to directly handle or store sensitive customer data. Mobility service providers also benefit from the ability to leverage their SSDTs to verify transactions, authenticate services, and interact with other stakeholders without revealing sensitive business data.

In essence, a Web3 approach in a multimodal transportation ecosystem fosters an environment of enhanced data security, operational efficiency, and trust. It reduces the risk of data exposure for both travelers and mobility service providers, leading to a more secure and efficient transportation environment.

Table 5. Data Privacy for Ecosystem Stakeholders (Riders and Service Providers)

Use Case Component	Description
Use Case ID	5.1.1
Use Case Name	Data Privacy for Ecosystem Stakeholders (Riders and Service Providers)
ARC-IT Categorization	Public Transportation, Traveler Information
Description	Demonstration that decentralized apps with look and feel of existing centralized multimodal trip planning apps like Whim and UbiGo, can operate without undesirable and insecure sharing of personal and competitive information with secondary actors. Trip planning execution and payment occurs within a MaaS marketplace, which integrates mobility data from multiple service providers and optimizes trip planning for travelers while ensuring fair revenue allocation to providers and increased data security for all parties.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e., Hyperledger, Ethereum)
Actors	Primary Actor: Traveler Secondary Actors: Public transit agency, mobility service provider, public and private transportation infrastructure owners, TNCs.
Operational Objectives/Goals	• Seamless trip planning and payment using a single gateway for user-defined information • No transfer of a user's private information to secondary actors beyond that needed to fulfill their contracted trip leg (PII protection) • No transfer of secondary actor information to other secondary actors beyond that needed to fulfill their contracted trip legs (Proprietary Competitor Information protection) • No exposure of traveler location and location history to secondary actors beyond that needed to fulfill their contracted trip leg (location privacy) • No exposure of traveler banking account or payment information beyond that needed to settle their contracted trip leg (settlement privacy)

Use Case Component	Description
Constraints/ Assumptions	Assumes that all stakeholders, including travelers and mobility service providers, have access to the necessary technology and possess the digital literacy required to engage with the system. This includes being able to use DIDs and VCs, understanding how to handle digital credentials, and understanding how ZKPs can ensure data privacy. A major constraint could be the varying levels of data protection regulations across different jurisdictions. In order to operate regionally or nationally, it needs to comply with a multitude of differing regulations, which can significantly affect the design and operation of the system. Another critical assumption is that stakeholders are willing to adopt this new approach. For travelers, this means trusting the system to secure their data. For service providers, it assumes readiness to adjust current operations to integrate with the new system. A related constraint is the necessity for a secure, robust digital infrastructure that can support the complexity of these operations while maintaining high levels of performance and reliability.
Pre-conditions	Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third-party developers of Web3-compliant business to consumer (B2C) apps for multimodal trip planning and payment that don't expose PPI, competitive business data, or payment details.
Workflow	1. Traveler browses through the available services offered by mobility service providers, selecting the appropriate options to create their multimodal trip. 2. For each selected service, the application sends a request, including the traveler's DID and required transaction details (e.g., booking time, location), to the corresponding mobility service provider. 3. Upon receiving the request, each mobility service provider verifies the traveler's DID and checks the transaction details. 4. If the traveler's DID and transaction details are valid, each mobility service provider issues a VC to the traveler, which acts as a digital ticket for the specific service. 5. The traveler securely stores the issued VCs in their digital wallet. 6. When the time comes to utilize the booked service, the traveler generates a ZKP using their VC for that specific service. This proof confirms their valid booking without revealing any personal information or details of the VC. 7. The traveler presents the generated ZKP to the mobility service provider that issued the corresponding VC. 8. The mobility service provider verifies the authenticity of the ZKP without receiving any sensitive data. 9. Once the proof is verified, the mobility service provider grants access to the service, and the traveler proceeds with their journey. 10. The traveler repeats steps 1-9 for each subsequent service in their multimodal trip.
Alternative workflow	ZKPs are only one cryptographic method for achieving data privacy, and there are many situations where an alternative method may work better, either in tandem with or instead of ZKPs.

Use Case Component	Description
Information Requirements	• DIDs of entities transacting within the permissioned networks. 'Entities' are broadly defined to include people, organizations, IoT devices, SSDTs, etc. • Trip information (location, duration, etc.) • Mobility Service Provider information (schedules, offerings, etc.)

5.1.2.1 Implementation Barriers

Possible obstacles to implementing this approach in a multimodal transportation ecosystem can encompass factors such as regulatory compliance, user acceptance, and stakeholder buy-in. First, a multimodal transportation system would need to operate within the constraints of various regional and national regulations that pertain to data privacy and protection. Ensuring compliance can be challenging, given the complex and varying rules across jurisdictions.

Second, the acceptance and adoption of these systems by travelers are crucial. While the systems are designed with user privacy in mind, they represent a significant shift from traditional methods of transaction and identification. Travelers may be resistant to change or harbor concerns about the security of their data.

Finally, service provider buy-in can be a challenge. For these stakeholders, adopting new methods for validating transactions and identities could require adjustments to their current practices. They may also have concerns about the effectiveness and reliability of these new systems. Overcoming these barriers will require clear communication about the benefits of the new systems, alongside reassurances of their security and reliability.

5.1.3 Ability to Verify/Validate Identities and Transactions with a Zero Trust Architecture

As multimodal transportation systems evolve to provide a seamless and integrated travel experience, they are becoming more complex, interconnected, and hence, vulnerable to a range of digital threats. These threats can affect not only the transit authorities but also passengers and mobility service providers involved in executing a multimodal trip. From ticketing to scheduling, real-time tracking, and customer service, each stakeholder's digital footprint is expansive and complex. However, the current perimeter-based security approach is increasingly proving inadequate to address evolving cyber threats. A key point of vulnerability is the verification and validation of identities and transactions between the traveler and various mobility service providers.

Implementing Zero Trust Architecture (ZTA), underpinned by W3C DIDs, anchored on public distributed ledgers and leveraging VCs, offers a compelling solution. The ZTA paradigm operates under a 'never trust, always verify' approach, and the use of these novel technologies minimizes the risk of data breaches and internal threats. By granting least privilege access and continuously verifying identities and devices, a ZTA approach amplifies a multimodal transportation system's security posture. This will also be

key for compliance, as regulations, like those described in the Biden Administration's Executive Order 14028, "Improving the Nation's Cybersecurity"[4], begin to become common across jurisdictions.

Table 6. Ability to Verify/Validate Identities and Transactions with a Zero Trust Architecture

Use Case Component	Description
Use Case ID	5.1.2
Use Case Name	Multimodal Trip Planning and Fare Payment System — Ability to Verify/Validate Identities and Transactions with a Zero Trust Architecture
ARC-IT Categorization	Public Transportation, Traveler Information
Description	A technology-agnostic, vendor-agnostic, and cloud-agnostic ecosystem of interoperable applications that allows stakeholders to securely communicate, transact, and collaborate on multiparty business processes. Leverages W3C VCs and DIDs standards together with cryptographic ZKPs to ensure that the SSDTs of ecosystem stakeholders — including service providers, infrastructure owners, and end users — are compatible and can transact without multiple bespoke APIs
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e., Hyperledger, Ethereum)
Actors	Primary Actor: Traveler Secondary Actors: Public transit agency, private transportation provider, public and private transportation infrastructure owner, TNCs
Operational Objectives/Goals	Demonstration of • Seamless trip planning and payment using a single gateway for user-defined information • No bespoke APIs needed by providers to fulfill their contracted trip leg (interoperability) • No transfer of secondary actor information to other secondary actors beyond that needed to fulfill their contracted trip legs (Proprietary Competitor Information protection) • "Trusted Trip" standard - proof of location limited to what is needed to fulfill contracted trip leg (location interoperability) • No exposure of traveler banking account or payment information beyond that needed to settle their contracted trip leg (payments agnostic and interoperable)

[4] "Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity," *Code of Federal Regulations*, title 3 (2022): 556-572. https://www.govinfo.gov/content/pkg/CFR-2022-title3-vol1/pdf/CFR-2022-title3-vol1-eo14028.pdf

Use Case Component	Description
Constraints/ Assumptions	Assumptions include that all users have access to and can competently navigate digital devices or platforms, as the DID and VC systems are fundamentally digital. We also assume that the system and its users will readily accept a shift towards an alternative infrastructure for identity verification mechanisms. It's assumed that the technology, despite its complexity, will function as intended, ensuring consistent verification of DIDs and VCs without significant errors or delays. On the other hand, constraints may include technological limitations such as system downtime or connectivity issues, which could impact the verification process. Limited public awareness and understanding of DIDs and VCs could also constrain user adoption. Lastly, as this system would be handling sensitive personal and transactional data, it would be constrained by data protection laws and regulations, requiring stringent measures to ensure data privacy and security. While this is well addressed by the use of ZKPs, the constraint does still exist, as it will be key for the continued growth and scaling of an implementation.
Pre-conditions	Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third-party developers of Web3-compliant B2C apps for multimodal trip planning and payment that don't expose PPI, competitive business data, or payment details.
Workflow	2. Trip Initiation: The traveler uses the multimodal app or platform to initiate a trip. Each mobility service provider requests the traveler's DID and resolves it to its DID document for initial identity verification. 3. Credential Verification: Upon successful DID verification, the system requests the traveler's VCs to authenticate their privileges (like ticket validity or subscription status). The system checks the cryptographic proofs of the VCs to validate their authenticity and verify the traveler's permissions. 4. Mode Transition: Each time the traveler changes modes of transport, the system will re-initiate the verification process. On the initiation of a mode transition, the system prompts for the traveler's DIDs and VCs, repeating the process of identity verification and credential validation. This ensures security consistency throughout the journey. 5. Transaction Processing: For any transaction occurring during the trip (e.g., onboard purchases), the system prompts for DIDs and VCs to authenticate the traveler's identity and validate their payment credentials. On receiving the DID and VC, the system verifies them before authorizing the transaction. 6. Trip Completion: When the journey is complete, the traveler checks out through the system. As part of the checkout process, the system once again verifies the traveler's DIDs and VCs to finalize the session and any outstanding transactions.

Use Case Component	Description
Alternative workflow	Alternatively, the entire trip can be bid on by a given mobility service provider, who then bears responsibility for coordinating with other mobility service providers at each step in the multimodal trip. Here, the sequence would focus more on validations between the mobility service providers that are coordinating on the back-end to provide the mobility option for each mode of the multimodal trip.
Information Requirements	• Traveler identifying information • Mobility Service Provider identifying information

5.1.3.1 Implementation Barriers

On the user front, resistance to adopting new verification systems could pose a hurdle. Users may need education and reassurance about the safety and privacy of their data within this new system. Regulatory complexities may also arise. With the advancements in identity verification mechanisms, regulations are continuously evolving, and compliance with local and national laws will be critical to the successful implementation of this system.

5.2 Transportation-based Virtual Power Plant with Payment Use Cases

Batteries have become a ubiquitous part of modern life. Increasing demand for batteries in consumer electronics, electric vehicles, and supporting the grid has accelerated the global market. According to a 2022 study published by Global Industry Analysts Inc. (GIA), the market is projected to reach $173.7 billion by 2026, at a compound annual growth rate (CAGR) of 10.3% (Global Industry Analysts 2022). This estimate does not consider the market size created by the second life use cases. Manufacturers are continually looking to improve battery chemistries and materials to increase energy density, lengthen life, improve safety, lower cost, and enable sustainability through second life and recycling.

Global battery regulations such as the EU Battery Regulation and US Treasury CARB's Zero-Emission Vehicle Requirements increasingly recognize the importance of data privacy and ESG considerations in the battery value chain. Consortia such as MOBI and Global Battery Alliance (GBA) are working with ecosystem stakeholders to create an implementation framework, reference architecture, and data schemas for an industry-wide secure data management system that can be used to improve the visibility and sustainability of the global battery value chain. The aim is to facilitate seamless communication in production management, maintenance, safety, second and third life uses, and recycling while meeting consumer and regulatory demands.

In order to ensure the execution of secure, privacy-preserving, trusted IoT transactions and data sharing in a decentralized ecosystem, it is necessary to develop new ways to identify and verify the entities involved. In 2018, MOBI released MOBI VID to define a Vehicle SSDT, the first W3C DID-based vehicle identity that can be anchored on a distributed ledger. In mid-2020, MOBI began to focus its efforts on defining a Battery SSDT to support trusted battery tracking, evaluation, and management (Rajbhandari n.n.). The Battery SSDT stores a combination of static and real-time data to log a battery's journey throughout its lifetime. Battery SSDTs are onboarded and managed on Citopia, with trusted identity and assurance services provided by the ITN.

5.2.1 Grid Load Balancing Leveraging EV Batteries as an Electricity Store

Endowing EVs and their owners, as well as grid operators and their assets, with DIDs anchored on a public distributed ledger enables the integration of the EV's battery system and chargers with several layers of grid control systems for managing load through control of charging, both unidirectional and bi-directional. Bi-directional charging hardware has been introduced by numerous OEMs and suppliers (for example, a DC/AC inverter for EVs and chargers) and charging standards like ISO 15118 have been published. Now, many stakeholders are focusing on the decentralized identity and data management infrastructure required to bridge each stakeholder's legacy systems. With that level of interoperability, a rich array of vehicle-to-grid (V2G) business cases become possible – for example, EV owners could charge during off-peak hours and subsequently sell that energy back via V2G processes during peak hours in order to help stabilize the grid and earn a profit. In other words, the EV owners would be acting as transacting agents in a decentralized energy marketplace. This is key – the development required to enable this V2G load balancing would also support any application that fundamentally operates using a decentralized energy marketplace. Centralized energy marketplaces do exist, but usually have high barriers to entry that entirely prevent smaller actors (like an individual EV owner) from participating. Electricity can be bought and sold outside of these marketplaces, but this requires grid operators to negotiate individual Power Purchase Agreements with each buyer—an unscalable approach. A decentralized energy marketplace is necessary to include smaller actors like EV owners or individual producers/consumers, and the required infrastructure is precisely the infrastructure that enables V2G grid load balancing.

Table 7. Grid Load Balancing Leveraging EV Batteries as an Electricity Store

Use Case Component	Description
Use Case ID	5.2.1
Use Case Name	Grid Load Balancing Leveraging EV Batteries as an Electricity Store
ARC-IT Categorization	Sustainable Travel
Description	EV batteries can provide decentralized energy storage to improve grid robustness, smooth supply/demand mismatches, and back up renewable energy sources when hydroelectric, solar, or wind generation is not possible or sufficient. EV owners can be incentivized to make their EV's battery available for this purpose, enabling them to monetize their EV when it is not being driven, and giving the grid operators more resources.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e., Hyperledger, Ethereum)
Actors	Primary Actor: EV owners and fleet operators Secondary Actors: Utilities, grid operators, smart cities, green energy producers
Operational Objectives/Goals	Demonstrate use of EV and EV battery DIDs and SSDTs to: ● Connect to the grid ● Identify itself as an authorized decentralized energy storage device ● Communicate conditions for providing storage capacity to the grid ● Agree on contractual conditions ● Execute contract with obligations verified by counterparty ● Settle transaction on agreed contractual terms

Use Case Component	Description
Constraints/ Assumptions	The successful execution of the load-balancing use case faces a few significant constraints. Firstly, it requires the presence of robust technical infrastructure, such as internet connectivity and Internet of Things (IoT) devices for real-time data monitoring, as well as the capacity to integrate the innovative distributed ledger solutions into existing power grid systems. Secondly, the regulatory environment could pose limitations, as local, state, and federal laws around energy generation, distribution, and trading could restrict the ability to buy and sell energy on a peer-to-peer basis. Thirdly, due to the intermittent nature of renewable energy sources, efficient energy storage systems need to be readily available to bridge any gaps between electricity supply and demand. A few key assumptions underpin the success of the distributed ledger and microgrids use case. First, it is assumed that prosumers will be motivated to sell their excess energy through this decentralized marketplace for a variety of reasons, such as monetary benefits or a desire to support renewable energy. Second, the viability of peer-to-peer energy trading rests on the assumption that there will be enough participation from consumers in this market. Finally, it is assumed that the power grid can handle the increased complexity introduced by numerous microgrids and maintain stability amidst the variable nature of renewable energy sources.
Pre-conditions	Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third party developers of Web3-compliant B2C apps for multimodal trip planning and payment that don’t expose PPI, competitive business data, or payment details.

Use Case Component	Description
Workflow	1. Announcement of Seller's Interest: The user (seller), identified by their DID, issues a VC that indicates their interest in making their electricity available for sale. This credential includes relevant details like the maximum quantity of electricity available, price, and charger/meter-specific metadata. 2. Buyer's Interest Expression: A grid operator, identified by their own DID, reads the seller's VC. If they decide to buy electricity from the user, they issue a VC indicating their intent to purchase. 3. Transaction Initiation: The buyer uses their intent to purchase VC to generate a Verifiable Presentation (VP) for the seller, signaling the initiation of the electricity exchange. A smart contract, associated with both the buyer's and seller's DIDs, is created to outline the terms of the transaction. 4. Electricity Exchange and Real-Time Data Recording: As the electricity exchange occurs, VCs are generated by the metering infrastructure, associated with its own DID, recording data about the electricity flow. 5. Transaction Finalization: Once the electricity exchange is complete, two final VCs are issued by the buyer and the seller, each attesting to the end of the exchange and the total amount of electricity transferred. 6. Payment Submission or Settlement Trigger: The smart contract associated with the transaction recognizes the completion VC and generates a trigger to execute payment. The Buyer issues a transaction settlement VC when the payment settles and the Seller issues a confirmation VC in turn.
Alternative workflow	An alternative implementation may reject the approach of having the EV owners act as “sellers” of electricity and grid operators as “buyers”. Instead, the system could be implemented such that the grid operators hold a reverse auction, wherein the grid operator dictates the terms of the transaction, setting a price ceiling and letting EV owners compete to offer the lowest prices to the operator. This implementation approach may be more suitable in cases where transparency is highly valued, as an open reverse auction would prevent a grid operator from unfairly offering attractive terms to some buyers and not others.
Information Requirements	• Transaction data from the grid operators, either making an offer to purchase electricity or fixing a price and max quantity in a reverse auction • Transaction data from the EV owner, either making an offer to sell electricity or participating in a reverse auction. • Data from the EV and battery about its current charge level, State of Health (SOH), etc. • Data from the metering infrastructure about the electricity exchange

5.2.1.1 Implementation Barriers

Accessibility and user acceptance present the largest barriers to implementation. Many people may not wish to actively engage in a decentralized energy marketplace and may find the requirement to keep their vehicle plugged in during peak hours to be untenable. The best path around these barriers is to focus on usability and simplicity, perhaps by determining some “standard offer” that an EV owner can opt-in to that offers the least active management or movement restrictions.

This scenario also requires a robust public and private charging infrastructure where willing vehicles are plugged in during the peak hours (often midday). Currently, most EV owners charge their vehicles at home (up to 80% according to research conducted by the Department of Energy) and do not need to charge during the day and commuter-centric charging infrastructure is limited (Michael Blonksy 2021).

Battery Wear: Concerns on how bi-directional charging will impact long-term battery health and capacity will need to be addressed to garner additional participants.

5.2.2 Global Battery Passport

Global battery regulations such as the EU Battery Regulation and US Treasury CARB's Zero-Emission Vehicle Requirements increasingly recognize the importance of data privacy and environmental social governance (ESG) considerations in the battery value chain. The EU Battery Regulation also mandates the implementation of digital records to track the complete lifecycle of batteries and proposes a framework for a battery passport: a digital credential containing key information about the battery's composition, state of health, history, and more. This has the potential to unlock new circular business models by giving stakeholders new tools to ensure EV batteries are produced, distributed, maintained, and recycled in a safe and sustainable way, opening the door to an array of second and third-life battery uses.

The passport you carry to travel from one country to another not only serves to prove your identity but also allows international authorities to query and verify information about you from multiple databases. A physical passport is nothing but a presentation of data points that customs officers use to confirm your identity when deciding whether to permit you to cross a certain border. Similarly, a battery passport is nothing but a presentation of data points about a particular battery – i.e., who manufactured it, its physical and chemical composition, its current State of Health (SOH), whether it was refurbished or repurposed from another battery, etc. The battery passport has many uses. For example, regulators can reference a battery passport to verify whether that particular battery is composed of an adequate proportion of recycled material. Likewise, battery passports enable battery owners to query their battery's SOH.

A battery passport can be implemented as a barcode, a QR code, or in an RFID chip in the same way our travel passports are equipped with barcodes or long strings of alphanumeric characters, like the Battery Identification Number Standard released by MOBI in July 2022 ("First Open Battery Identity Standard Enables Web3 Supply Chain Efficiency" 2022). The barcode or QR code on a battery passport needs to retrieve information about the battery from some digital source. That digital source of information about the battery can be a centralized location and/or in the battery itself. This is where Battery SSDT comes in, which stores all pertinent data for the battery passport in its encrypted data vault, able to generate passport credentials or attestations to that data when needed.

Table 8. Global Battery Passports

Use Case Component	Description
Use Case ID	5.2.2
Use Case Name	Global Battery Passports
ARC-IT Categorization	Sustainable Travel

Use Case Component	Description
Description	Traceability of battery origin, production, usage, recycling/repurposing, and more is vital to ensuring compliance with various regulatory requirements (e.g., EU Battery Regulation, CARB), meeting ESG goals, improving warranty management, and many more. The battery SSDT provides information about the battery to a third party using the Battery Passport as a credential. In addition to holding the physical attributes of the battery, the battery SSDT also stores traceability-related data in its encrypted data vault. Because traceability data will come from multiple sources (entities), the battery SSDT will ensure the verifiability of such data by linking the identity of the entities to a trust anchor.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e., Hyperledger, Ethereum)
Actors	Primary Actor: Vehicle/Battery owner Secondary Actors: Battery manufacturer, transporter, regulator, insurer, charge point operator, recycler, etc.
Operational Objectives/Goals	Demonstrate ability of EV battery DIDs and SSDTs to: ● identify itself as an authorized and approved battery type ● communicate conditions of manufacture, including location, manufacturer, carbon content and other sustainability information, capabilities, SOH, etc.
Constraints/ Assumptions	Stakeholder Collaboration: The battery passport system assumes collaborative engagement and cooperation among battery manufacturers, vehicle manufacturers, service providers, and regulatory authorities. It assumes that these stakeholders will work together towards the common goal of implementing a standardized and effective passport system. Data Accuracy and Reliability: The system assumes that the battery-related data provided by manufacturers, service providers, and other sources is accurate, reliable, and verified. Trust in the data is essential for the effectiveness of the passport system. Technological Readiness: The assumption is made that the necessary technological infrastructure, such as IoT devices, communication networks, and data storage systems, are in place to support the collection, transmission, and storage of battery-related data. Regulatory Alignment: It is assumed that regulatory frameworks will evolve and adapt to support the implementation of battery passport systems. This includes defining standards, policies, and guidelines that promote the interoperability and secure exchange of battery data. Industry Adoption: The battery passport system assumes a willingness among industry participants to adopt and integrate the necessary hardware, software, and protocols to enable the creation and utilization of battery passports.

Use Case Component	Description
Pre-conditions	Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third-party developers of Web3-compliant B2C apps for multimodal trip planning and payment that don't expose PII, competitive business data, or payment details.
Workflow	1. Battery Information Storage: The battery manufacturer creates an SSDT for each battery, which generates and stores a DID for the battery, as well as physical attributes and traceability-related data. The data is stored in an encrypted data vault and associated with the battery manufacturer's DID. 2. Issuance of Battery Passport Credential: The battery SSDT, using its DID, issues a VC known as the Battery Passport. This passport represents the battery's physical attributes, traceability data, and the manufacturer's identity. 3. Battery Purchase and Ownership Transfer: A vehicle/battery owner buys the battery, and a VC representing the transfer of ownership from the manufacturer to the owner is issued. This credential is associated with both the manufacturer's and the owner's DIDs. The battery SSDT issues a new battery passport credential reflecting the change in ownership. 4. Battery Passport Credential Access: The vehicle/battery owner, or any third party given permission, can access the Battery Passport. 5. Traceability Data Verification: When new traceability data is added to the battery's SSDT by other entities (like service providers or recycling facilities), these entities issue VCs of their traceability data, ensuring that such data can be validated as coming from them in the future. 6. Continual Battery Passport Updating: As the battery's lifecycle progresses, the Battery Passport is updated, representing changes in its state, service history, ownership, and more. These updates are linked to the relevant DIDs for the relevant entities, ensuring transparent and verifiable traceability of the battery's life history.
Alternative workflow	The workflow above is general and applicable to a variety of implementation approaches. The flow leans towards complete transparency, with each update to the battery passport being associated with a VC, serving as an attestation of the update's data veracity from whatever entity produced that data. These VCs can be resolved back to the entity, which is good for transparency. However, an alternative approach would be for every update/change to the battery passport to be attested to by the current owner, who would then be responsible for storing the pertinent data behind each update. This would improve privacy (at the cost of transparency), as each change to the battery passport (and the business transaction/action behind it) would be private, only able to be disclosed by the battery owner.

Use Case Component	Description
Information Requirements	• Data from the battery management system (BMS) that is pertinent to the battery's fundamental characteristics or SOH • Data from the battery owner pertaining to the battery passport's data that does not come from the BMS, like the date of ownership transfer.

5.2.2.1 Implementation Barriers

The biggest barrier here is the difficulty of getting a critical mass of battery manufacturers to agree on the data that would comprise a battery passport – an issue that is currently being tackled by multiple consortiums. This is an issue that would mostly delay the implementation of a battery passport, rather than prevent it, due to existing EU regulatory requirements and potential regulation elsewhere mandating that a battery passport be made available.

5.2.3 Battery State of Health (SOH)

Vehicle owners can use the battery SOH data to determine when to replace a battery and assess their EV's value based on remaining capacity. Battery performance, especially the SOH, will be a key parameter that will influence consumers' vehicle buying choices. As rechargeable batteries become ubiquitous, discussions about their performance (as well as methods of estimation) will become more prominent. End consumers will want to know the initial SOH and how it will degrade over time for the vehicle of their choice before making purchasing decisions. Because batteries are a critical component of EVs, an EV's range — and, by extension, its value — will be tied to the battery's performance. Battery performance, especially the SOH, will be a key parameter that will influence consumers' vehicle buying choices. Insurance companies may want to know the residual value of batteries to correctly underwrite them. Lenders would want to know whether to extend the warranty of the vehicle or not. OEMs are also responsible for battery recalls, maintenance services, and management of battery warranties. Both OEMs and suppliers will have a responsibility to comply with future regulations regarding standardized reporting of SOH as well as battery recycling and repurposing. The SOH is used in determining the current maximum range of EVs. Current maximum range of an EV = current SOH x rated beginning of life range (e.g., 90% x 200 mi = 180 mi). Vehicle owners can use this information to determine time remaining before the battery has to be replaced and compare their EV's value based on remaining capacity. Battery SOH (current state and history) can be included in the distributed ledger so that the data becomes tamper evident against possible fraud in order to conflate the value of batteries and electric vehicles.

Table 9. Battery State of Health (SOH)

Use Case Component	Description
Use Case ID	5.2.3
Use Case Name	Battery State of Health (SOH)
ARC-IT Categorization	Sustainable Travel

Use Case Component	Description
Description	Vehicle owners, insurers, and recyclers can use SOH information to determine value, time remaining before the battery must be replaced, cost/benefit of using EV as decentralized storage device/virtual power plant, etc. Battery SOH data will be a powerful tool for stakeholders across the value chain to unlock more transparent and sustainable business models.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e. Hyperledger, Ethereum)
Actors	Primary Actor: EV/Battery owner Secondary Actors: Secondary market buyers; EV Manufacturers; Battery Manufacturers; Fleet Owners; Governments, Regulators, and Policymakers; Insurers of EV Owners; Lenders to EV Owners and Dealers; EV Dealers and Repair Shops; Battery Recycling and Repurposing Companies; Battery Swapping Companies; Battery Analytics Platforms; Battery Testing Companies.
Operational Objectives/Goals	Demonstrate ability of EV battery DIDS and SSDTs to: ● identify itself as an authorized and approved battery type ● communicate current condition (i.e. SOH) to buyer, service department, recycler, charge point, regulator, utility/grid operator, etc.
Constraints/ Assumptions	Data Collection and Integration: Implementing a comprehensive battery State of Health (SoH) monitoring system requires collecting data from various sources, such as battery sensors, diagnostic tools, and maintenance records. Integrating this data from different sources into a unified system can be challenging due to differences in data formats, compatibility issues, and limited access to proprietary systems. Data Accuracy and Reliability: Ensuring the accuracy and reliability of SoH data can be a constraint. Factors such as sensor calibration, data quality, and potential errors in measurement can impact the effectiveness of the monitoring system. Resource and Cost Limitations: Developing and deploying a battery SoH monitoring system may involve significant costs, including hardware, software, data storage, and ongoing maintenance. Limited resources or budget constraints could impede the implementation or scalability of the system. User Acceptance and Cooperation: The successful implementation of a battery SoH monitoring system assumes acceptance by EV value chain stakeholders as well as user acceptance and cooperation, such as vehicle owners or fleet operators providing access to battery data, granting necessary permissions, and actively participating in the monitoring process. Regulatory Support: It is assumed that regulatory frameworks support the collection and utilization of battery SoH data, ensuring compliance with data privacy and security regulations while allowing the necessary sharing of data for monitoring purposes.

Use Case Component	Description
Pre-conditions	Existence of a widely accepted battery SOH. Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third party developers of Web3-compliant B2C apps for multimodal trip planning and payment that don't expose PII, competitive business data, or payment details.
Workflow	1. Battery DID Registration and SSDT generation: The battery manufacturer registers a unique DID for the battery and generates the battery's SSDT. 2. Continuous Battery SOH Monitoring: The battery management system (BMS) constantly monitors the battery's SOH (i.e., charge cycles, temperature, capacity degradation, etc.) and stores the collected SOH data in the SSDT's encrypted data vault. The BMS reports the SOH to the end users, which is also a requirement in the EU Battery Regulation. 3. Issuance of SOH VC: The battery SSDT issues a VC representing the SOH of the battery at a specific point in time. 4. SOH Credential Access: The vehicle owner or authorized third-party service providers can access the issued SOH VC 5. Continuous Update of SOH VC: The SOH VC is updated on a regular basis (as determined by the BMS settings) to ensure it accurately represents the current SOH of the battery.
Alternative workflow	Here, the workflow assumes a static method for determining the battery SOH, such that the BMS itself can always determine its SOH. In practice, the algorithm used to determine SOH may be proprietary, or at least specific to (a) manufacturer(s) and may therefore be updated. By having the battery SSDT use the BMS to generate the SOH, changing the approach would require updating the BMS, which may be difficult at scale. Instead, having the data be sent from the BMS to the battery manufacturer, who then performs the SOH calculation and generates an attestation as to the SOH and their having calculated it privately.
Information Requirements	• Data from the BMS that would be used to determine the SOH • Data from the OEM and/or service providers as to any repairs/updates to the battery/BMS that are pertinent to the SOH determination

5.2.3.1 Implementation Barriers

Implementing a comprehensive battery State of Health monitoring system faces several challenges. One of the primary barriers is the complex nature of battery degradation, which involves various interrelated factors such as charge/discharge cycles, operating temperature, depth of discharge, and age. There is not yet a standardized approach to determining battery SOH and different approaches to determining SOH may produce similar looking SOH values that may not translate to similar outcomes.

5.3 Freight Management Use Cases

There are over 1 million trucking companies (or carriers) in the US, more than 95% of which are small firms with 10 or fewer trucks. Additionally, in 2022, trucking companies moved over 70% of all freight and generated more than $900 billion in annual revenue ("Truck Freight Tonnage and Revenues Rise in 2022, According to Report" 2023). The logistics industry is highly fragmented, with hundreds of enterprise systems used by these companies to manage their daily operations. These systems have little or no interoperability and there are no industry-wide standards to share information about shipments, drivers, performance, pricing, etc. This fragmentation has made it difficult for the industry to share at a national scale information needed to better plan and move shipments. Except for truck safety requirements, which are maintained by the Federal Motor Safety Administration (FMCSA) with support from state-level enforcement agencies, there are no national-level performance metrics such as on-time delivery or delinquency openly available. These metrics would be extremely important for carriers, shippers, insurance, and financial institutions to manage risks when hiring carriers as contractors, underwriting liability policies, lending, etc.

The use cases presented below may not pertain to intelligent freight operations on the nation's highways and roadways, but they are important in the sense that implementation of ITS service packages in ARC-IT provides data needed for the use cases.

5.3.1 Industry-Wide Service Performance Based Reputation System for Carriers

Shippers, third-party logistics providers (3PL), and fourth-party logistics providers (4PL) hire carriers to move their shipments. Before hiring the carriers, they must screen them for performance metrics such as reputation, safety history, financial performance, etc. Shippers use the FMCSA database to screen based on safety and out-of-service flags. They use various commercially available credit reports to understand the financial status of carriers. However, they do not have a system by which they can screen the carriers for their on-time delivery/pickup performance.

Table 10. Industry-Wide Service Performance Based Rating System for Carriers

Use Case Component	Description
Use Case ID	5.3.1
Use Case Name	Industry-Wide Service Performance Based Reputation Rating System for Carriers
ARC-IT Categorization	CVO01 Carrier Operations and Fleet Management CVO02 Freight Administration
Description	Currently, FMCSA provides safety based reputation system for carriers. Such a system is used by shippers/3PL/4PL to screen carriers before contracting them. There are also resources to discover the financial history of carriers. However, there is no system to discover a carrier's reputation-based performance such as on-time pickup/delivery. Most companies keep such records internal and do not share them with third-party aggregators due to confidentiality reasons. Such a reputation system can be applied to multimodal freight movement.
Type of Distributed Ledger	Permissioned ledger anchored onto public distributed ledger (e.g., Ethereum)

Use Case Component	Description
Actors	Primary Actor: For hire asset-based carriers; shippers/3PL/4PL that hire the carriers. Secondary Actors: Neutral third-party entities that develop and maintain such a rating system.
Operational Objectives/Goals	Objectives/goals for this distributed ledger use case deployment would be to ensure that the carriers have access to the traceability and auditability of performance records that were utilized in determining their reputation rating. This allows the carriers to raise disputes if a shipper has falsely provided the report of on-time delivery or pick up.
Constraints/ Assumptions	Assumes the solution uses global identity standards such as W3C to create unique DIDs of shipments/entities which are anchored in a federated certificate authority (e.g., Integrated Trust Network) and that entities have access to a permissioned network and employ agreed data schemas for exchanging of data. Potential constraints or assumptions to create such a system include economic incentives for the entities to share data about the shipments and the system's ability to uniquely identify such shipments, trust the pickup/drop off dates/times provided by the shipper/carrier's applications, and aggregate the performance to create a robust reputation system.
Pre-conditions	The successful use case depends on the ability of the shipper's and carrier's systems to provide accurate information about individual shipments' on-time arrival and departure. One of the biggest constraints is that there are no globally unique identifiers of shipments since each system assigns its own unique identity. The use case also depends on economic incentives for the actors to share individual shipment performance data with a third-party entity. Also, the algorithms used to determine ratings must be robust.
Post-conditions	The expected outcome of the application will be a simple reputation rating system to screen carriers based on types of shipments, origin-destination corridors, etc.
Workflow	1. On-time performance of shipments is typically recorded in the carrier or shipper's enterprise systems. 2. The carrier and shipper will share such data with a third-party entity, which ensures a one-to-one match of shipment identity. The entity provides economic incentives to the carriers/shippers for providing the data. 3. The entity will then assign a dynamic rating based on the data it receives. The entity will anchor the final rating and hash of unaggregated data used to calculate the rating in a public distributed ledger. This provides traceability and auditability for carriers and shippers if they want to raise disputes with the entity.
Alternative workflow	The third-party entity can build crypto incentives to streamline and automate the "data purchase" from shippers/carriers.

Use Case Component	Description
Information Requirements	A list of information that is required for the scenario/application to work are the following: ● Shipper and carrier provided information on individual shipment's on-time performance. ● Economic incentives for shippers and carriers to share data with a third party. ● Robust algorithms to determine the reputation rating of carriers. Shippers and carriers should have access to transactions anchored on the distributed ledger for traceability and auditability.

5.3.1.1 Implementation Barriers

The biggest hurdle of creating such a system is the need to collect shipment performance data from hundreds of vendors and systems, which will require many one-off integrations. On top of that, there are no industry standards that these systems follow in terms of describing the shipment attributes. That means the third-party entity has a tremendous challenge ahead to translate the incoming data into a standardized format to feed into its reputation rating algorithms.

5.3.2 Multijurisdictional Automated Cargo Clearance at Ports

At marine ports, multiple government and non-government entities operate to facilitate inflow, storage, cargo loading/unloading, outflow, safety screening/inspections of cargo, payments, and customs clearance. Entities may include federal customs agencies, agricultural inspection agencies, port authorities, terminal operators, customs brokers, carriers, 3PL/4PL, stevedoring companies, banks, etc. In most ports, these entities operate in silos and share data on a limited basis although they all have a common mission to process cargo in the minimum amount of time without compromising the security and illegal movement of goods. Clearance of cargo prior to pickup is done at several levels by different agencies. For example, terminal operators want to ensure that they're paid by the cargo owners, port authorities must ensure that trucks/drivers have the proper authority to enter the port, and customs agencies must ensure that trucks do not contain illegal goods and that proper tariffs are paid on time. An automated one-stop clearance system will allow all these entities to collaboratively share data with each other or with the system such that 1) all the entities are accountable to perform their duties in a timely fashion, 2) it provides traceability and visibility to the cargo owners, and 3) entities can share risk related information with each other to screen potential bad actors in the marine port value chain.

Table 11. Multijurisdictional Automated Cargo Clearance at Ports

Use Case Component	Description
Use Case ID	5.3.2
Use Case Name	Multijurisdictional Automated Cargo Clearance at Ports
ARC-IT Categorization	CVO03 Electronic Clearance CVO11 Freight Drayage Optimization

Use Case Component	Description
Description	This use case will develop a single-window system at a marine port to provide traceability of cargo movement inside the ports. The system will be integrated with individual systems maintained/operated by various agencies operating at the port and be able to record events/milestones/decisions administered by the agencies on cargo. Such events will be recorded in a permissioned ledger that is available to all agencies.
Type of Distributed Ledger	Permissioned ledger with anchoring of events/milestones/actions in public distributed ledger via smart contracts.
Actors	Primary Actor: Federal customs agencies, agricultural inspection agencies, port authorities, terminal operators, customs brokers, carriers, 3PL/4PL, stevedoring companies, and banks. Secondary Actors: Port-based trade organizations, insurance companies
Operational Objectives/Goals	The objectives/goals for this distributed ledger use case deployment are as follows: ● Events, milestones, and actions performed by the agencies are recorded on to distributed ledger via smart contracts. ● Cargo owners can present to third-party (such as insurance) information about such events via verifiable credentials and transactions in smart contracts.
Constraints/ Assumptions	Potential constraints or assumptions to create such a system include: ● Willingness of agencies to provide data about actions taken by them to the system without prejudice to any actors in the value chain. ● Willingness of agencies to cooperate and abide by the system's protocols ● Willingness of the agencies to allow the system to integrate with their legacy systems. Assumes the solution uses W3C standards for DIDs and VCs and that all participants have access to a permissioned network and employ agreed data schemas for exchanging data and payments. Assumes all shared private data is protected using ZKPs.
Pre-conditions	The successful use case depends on the ability of the agencies to provide information about events/actions performed on cargo in a timely manner. Individual agency systems must also use a common identifier for trucks and cargo. Scalability and long-term sustainability of the use case depend on economic incentives for the actors to financially sustain the system.
Post-conditions	The expected outcome of the application will be a single window system that allows all actors to view cargo events/milestones/actions and provides an audit trail of such events.
Workflow	1. Depending on cargo import or export, agencies utilizing their internal systems will send a data payload about the cargo's events/actions to the system with digital fingerprints. 2. Cargo owners will view the events/actions taken on their cargo. Companies must be able to view such information for cargo for which they are the beneficial owners. 3. Cargo owners will share VCs about the cargo event with other shippers, insurance carriers, etc.

Use Case Component	Description
Alternative workflow	N/A
Information Requirements	• Agreement between terminal operators, customs agencies, and other entities to assign a common identity to cargo/trucks/appointments. • Smart contracts with business logic agreed by the entities. • Data pertaining to events/milestones/actions performed on individual cargos

5.3.2.1 Implementation Barriers

One of the most significant challenges in establishing a comprehensive single-window system lies not in its technical implementation, but in overcoming the obstacles related to agency cooperation and data sharing. While the technical aspects of creating such a system can be addressed through appropriate expertise and resources, the critical factor for success lies in building consensus and fostering collaboration among the various agencies involved.

5.3.3 Actual Weight-Based Road Usage Charging of Trucks

Road Usage Charging (RUC) based on actual traveled distance using odometer data or telematics is a widely known concept and has been piloted in several states in the US. In the freight industry, it is prudent to track the amount of weight a given truck carries over a reported distance. Installing weight sensors inside trucks is expensive and unreliable. However, truck drivers are required to carry a bill of lading which includes the weight of the freight they are transporting. Hence, the shipper who prepares the bill of lading and provides it to the truck driver has access to weight information. In order to implement weight-based RUC, the shipper must provide information about the weight, shipment info, truck identity, etc., to the state agency, which must then reconcile the truck's mileage with the weight information. The use of a distributed ledger can enhance efficiency in this process and allow trucking companies to view details about their charges by querying smart contracts or similar on-chain logic execution mechanisms.

Table 12. Actual Weight-Based Road Usage Charging of Trucks

Use Case Component	Description
Use Case ID	5.3.3
Use Case Name	Actual Weight-Based Road Usage Charging of Trucks
ARC-IT Categorization	CVO01 Carrier Operation and Fleet Management CV016 Electronic Driver Logs TM11 Road Usage Charging

Use Case Component	Description
Description	Using distributed ledger technologies, particularly smart contracts or similar on-chain execution logic, can be leveraged to reconcile weight information provided by shippers with mileage information provided by trucking companies. This enables an efficient determination of road usage charges. Since these two processes are independent, the shipper needs to input weight information from the bill of lading, while the carrier must input mileage information using a globally unique identity for the truck and the shipment. By connecting these two pieces of information through a smart contract, the carrier can authenticate and validate the road usage charges invoiced by the RUC program administrator.
Type of Distributed Ledger	Permissioned identity registration layer and smart contract type on-chain execution environment such as Ethereum.
Actors	Primary Actor: Shippers, trucking companies, RUC program administrator. Secondary Actors: ELD service providers.
Operational Objectives/Goals	The objectives/goals for this distributed ledger use case deployment are as follows: ● Ability to correctly gather information from the shippers about the weight of the freight being transported. ● Ability to correctly gather mileage information from the trucking companies. ● Ability to reconcile weight and mileage data using a tamper-evident ledger via an on-chain execution program such as smart contracts.
Constraints/ Assumptions	There are several constraints to consider, such as the existence of numerous ELD service providers and enterprise systems utilized by shippers for generating bills of lading, none of which adhere to a standardized format. Consequently, the system must establish connections with a multitude of diverse and non-interoperable systems, which can result in significant implementation costs.
Pre-conditions	In addition to the privacy concerns raised by trucking companies when reporting mileage data to RUC program administrators, a notable challenge lies in developing standardized payload data for submitting both bill of lading information and mileage data to smart contracts.
Post-conditions	The expected outcome of the application will be a system that connects to shipper and carrier systems to receive information about weights and mileage and encode the information in a tamper-evident ledger. The actual charge to the trucking company doesn't need to be on-chain. The ELD is also not required to provide the telematics breadcrumbs on-chain. A ZKP execution would verify whether a given truck is actually located in the origin and destination zip codes as defined in the bill of lading.
Workflow	1. Shippers will upload the information from the bill of lading (not all data points in the bill of lading are essential to this use case) to a system. 2. The trucking company provides the ELD information. 3. The system then associates the information about the trucking company, origin/destination, and pickup/drop off dates with the trucking company-provided mileage using ZKP execution. 4. Once reconciled, the system generates the appropriate charges and transaction identity provided to the trucking company.

Use Case Component	Description
Alternative workflow	An alternative workflow could leverage Weigh-in-Motion (WIM) systems and Automatic Number Plate Recognition (ANPR) systems. As a truck passes over the WIM system, it detects the vehicle and measures its weight, while the ANPR system identifies the vehicle by its license plate. Both sets of data are associated with the weight data with the vehicle identification data and records the time of the measurement. The system then calculates road usage charges based on the recorded weight, specific charges for different weights, and estimated distance traveled (based on the locations of the WIM systems the vehicle was detected at). After charges are calculated, an invoice is generated and sent to the trucking company associated with the vehicle's license plate, using an automated system such as email or direct integration into their accounting software.
Information Requirements	● Selected information from the bill of lading (e.g., trucking company information, origin/destination, pickup/drop off dates/times, weight of the freight being transported). ● ELD data of truck's positions. ● ZKP execution to ensure the truck actually traversed the origin-destination mentioned in the bill of lading.

5.3.3.1 Implementation Barriers

The primary obstacle in developing such a system is scalability, as it necessitates integrating with a vast number of enterprise systems and ELD service providers. However, there are many aggregators in the market that already provide one-stop access to multiple of these systems.

5.4 Usage-based Fees Use Cases

As the mobility paradigm continues to evolve, federal, state, and local governments in the United States have begun showing increasing interest in implementing usage-based mobility payment systems. For example, with increased fuel efficiency and the growing adoption of hybrid and electric vehicles, states like Oregon, Utah, and California are looking to adopt RUC as an alternative to the traditional gas tax. Cities that struggle with traffic congestion and clogged roadways are evaluating congestion pricing systems, which incentivize drivers to take alternative routes to reduce traffic congestion. Another key example of usage-based mobility (UBM) is the carbon credit system, in which drivers are rewarded for using vehicles that contribute a lower proportion of carbon emissions. This offers the basis for a vehicle carbon accounting system and incentivizes sustainable behaviors.

Usage-based mobility payment systems provide an enterprising opportunity for more sustainable, equitable infrastructure funding. However, current usage-based systems require expensive hardware, lack the ability to capture relevant contextual factors such as location, and rely heavily on centralized third parties for continual service. Altogether, these factors make the cost of collection unacceptably high. Moreover, successfully executing these systems requires many stakeholders to expose private data. For these reasons, UBM payment systems have remained unfeasible at scale. However, the emergence of new technologies (distributed ledger, ZKPs, DIDs, and VCs) has enabled a decentralized, privacy-preserving approach that has brought the implementation of such usage-based systems within reach.

5.4.1 Dynamic and Decentralized Curb Management

In an era where urban spaces are increasingly constrained and in high demand, there exists a need for smart, efficient, and secure solutions to optimize the use and monetization of a city's most precious and underutilized asset — the curb. Comprising roadside loading and parking zones, the shoulder, and the adjacent sidewalk, this space presents a significant opportunity for innovative technologies to drive optimal utilization, efficiency, and revenue generation. This use case explores a dynamic and decentralized approach to curb management, leveraging modern technologies such as DIDs and VCs, ZKPs, and distributed ledger networks.

This proposed solution envisions a system where zones can be dynamically altered from parking lanes to loading lanes to traffic lanes based on real-time conditions or the time of day. Furthermore, it introduces an efficient method for monitoring usage, reserving space, and enabling online payments without sharing user PII or the need for a mega platform provider. This approach promises not only to enhance the efficiency and flexibility of urban space usage but also to provide robust security and privacy for users and a new revenue stream for cities.

Table 13.Dynamic and Decentralized Curb Management

Use Case Component	Description
Use Case ID	5.4.1
Use Case Name	Dynamic and Decentralized Curb Management
ARC-IT Categorization	Traffic Management, Commercial Vehicle Operation, Parking Management
Description	The curb — including roadside loading and parking zones, shoulder, and the adjacent sidewalk — comprises some of the most valuable and in demand space in a city, but it is not efficiently used or monetized. Modern geolocation technologies, combined with vehicle identifiers and distributed ledger networks, enable efficient methods for optimizing and monetizing these assets in real time. Dynamically changing zones from parking lanes to loading lanes to traffic lanes in response to conditions or time of day, monitoring use, reserving space, and online payment is possible without sharing user PII or empowering a mega platform provider.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e. Hyperledger, Ethereum)
Actors	Primary Actor: Personal and commercial vehicle operators Secondary Actors: Smart cities, infrastructure owners, delivery companies, TNCs
Operational Objectives/Goals	The objectives/goals for this distributed ledger use case deployment are as follows: ● Vehicle and infrastructure identifiers are recorded on distributed ledger ● Reservations are booked and authorized via VCs ● Vehicle owners can present to third-party infrastructure owners information about the vehicle, infrastructure use, reservation, etc. via additional VCs ● Settlement of transactions in smart contracts.

Use Case Component	Description
Constraints/ Assumptions	For the curb management use case using distributed ledger technologies, several constraints and assumptions are key to its implementation. One constraint is the availability and accuracy of real-time curb data, including curb usage, restrictions, and occupancy. The system assumes the availability of reliable and precise geolocation technologies to track vehicle movement and parking behaviors. Another constraint is the need for robust, secure, and scalable distributed ledger infrastructure capable of handling high transaction volumes and maintaining data privacy. The system assumes that all involved stakeholders, such as local authorities, delivery services, and drivers, will participate and comply with the system's rules. Furthermore, there is an assumption that the necessary legal and regulatory frameworks are in place.
Pre-conditions	Existence of public sector pricing algorithms for curbs and adjacent infrastructure. Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third-party developers of Web3-compliant B2C apps for curb, parking, zone use management, and payment that do not expose PII, competitive business data, or payment details.
Workflow	1. Announcement of User's Interest: A user, identified by their DID, issues a VC indicating their interest in reserving curb space. This credential includes relevant details like the required amount of space, the intended use (parking, loading), duration of use, and specific location preferences. 2. City's Interest Expression: A city traffic manager, identified by their own DID, reviews the user's VC. If the requested curb space is available and the conditions are acceptable, they issue a VC indicating their approval. 3. Reservation Initiation: The user uses their approval VC to generate a Verifiable Presentation (VP) for the city, signaling the initiation of the curb space reservation. A smart contract associated with both the user's and city's DIDs is created to outline the terms of the reservation. 4. Curb Space Use and Real-Time Data Recording: As the user utilizes the reserved curb space, VCs are generated by the geolocation infrastructure, associated with its own DID, recording data about the space usage. 5. Reservation Finalization: Once the curb space usage is complete, two final VCs are issued by the user and the city, each attesting to the end of the usage period and the total duration of curb space used. 6. Payment Submission or Settlement Trigger: The smart contract associated with the reservation recognizes the completion VC and generates a trigger to execute payment. The user issues a transaction settlement VC when the payment settles, and the city issues a confirmation VC in turn.

Use Case Component	Description
Alternative workflow	As an alternative approach, Internet of Things (IoT) technologies and Machine Learning (ML) algorithms could be incorporated into the Dynamic and Decentralized Curb Management system. IoT devices can provide real-time data regarding curb usage and environmental conditions, allowing for more precise and dynamic allocation of curb space. ML algorithms can process this data and learn from patterns, effectively predicting peak usage times, traffic patterns, and optimal curb space allocation strategies. In this way, the system can proactively manage the curb space rather than merely reacting to user requests and immediate conditions. User DIDs and VCs would still be used for reserving curb space and making payments while maintaining privacy and security. However, instead of a manual process initiated by the user's request, the ML algorithm would recommend optimal curb usage based on learned patterns and predictive models. This approach could potentially lead to more efficient utilization of curb space and enhanced user satisfaction, as it would take into account broader usage patterns and predictive data. The integration of IoT and ML would require additional initial development and resources but could offer significant benefits in terms of efficiency, user experience, and overall curb management.
Information Requirements	• City mapping data • Curb and parking availability data • Identifying data for the drivers and for the state entity

5.4.1.1 Implementation Barriers

One key barrier to implementation could be user acceptance and adoption. Changing habitual behaviors and convincing users to trust and utilize a new system, especially one based on technologies that they may not fully understand, like distributed ledger, can be a significant challenge. Additionally, there are potential regulatory hurdles related to data privacy and security, particularly concerning the handling of PII. While the system protects PII through the use of DIDs and ZKPs, achieving and maintaining compliance across multiple jurisdictions that are regularly evolving can still be complex. Lastly, accurately predicting and dynamically managing curb usage can be difficult due to the unpredictable nature of urban traffic and user behavior, even with the help of advanced technologies like Machine Learning.

5.4.2 Dynamic and Decentralized Tolling and Road Usage Charging (RUC)

In the United States, state and federal governments currently fund road maintenance largely through the gas tax. When vehicles drive on a street, the damage to the road is influenced by the weight of the vehicle — a small sedan will cause much less damage than a large truck or SUV would. While a small 15-year-old sedan may have identical fuel efficiency to a modern truck, they may cause significantly different amounts of damage per mile to the roadway they're driving on. With the gas tax, or even a basic RUC system with a flat fee per mile, the vast difference in the marginal cost of the 15-year-old sedan's trip versus the brand-new truck's trip is not captured at all. A dynamic, decentralized tolling and RUC system, integrated with vehicle telematics, can capture all pertinent data required to accurately determine the marginal cost of a given vehicle's trip and, by proxy, determine the optimal fee. Moreover, it could automate the onerous identity/transaction authentication/validation costs that drive a high cost of collection in today's operating RUC systems.

Table 14. Dynamic and Decentralized Tolling and Road Usage Charging (RUC)

Use Case Component	Description
Use Case ID	5.4.2
Use Case Name	Dynamic and Decentralized Tolling and Road Usage Charging (RUC)
ARC-IT Categorization	Traffic Management
Description	Modern geolocation technologies, combined with vehicle identifiers and distributed ledger networks, enable efficient methods for optimizing and monetizing road assets in real time. Vehicles can be charged true marginal cost, based on algorithms for pricing road damage, congestion, etc. EVs can be charged their fair share, or alternatively subsidized to promote adoption.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e. Hyperledger, Ethereum)
Actors	Primary Actor: Road infrastructure owners and operators Secondary Actors: Vehicle owners, smart cities, toll operators, etc.
Operational Objectives/Goals	The objectives/goals for this distributed ledger use case deployment are as follows: ● Vehicle and infrastructure identifiers are recorded on distributed ledger ● Vehicle route monitored and marginal cost debited to the ledger in real time based on algorithms which account for vehicle weight, congestion, carbon footprint, etc. ● Periodic presentation and settlement of transactions in smart contracts.
Constraints/ Assumptions	RUC systems rely heavily on the availability and accuracy of vehicle-related data such as real-time location, distance traveled, and vehicle identity. Lastly, the success of this initiative presumes active participation and compliance from all relevant stakeholders, including drivers, vehicle manufacturers, transportation authorities, and potentially even third-party service providers, and access to such data is a key assumption for this use case. Digital literacy and adoption stand as key constraints; the system's success is reliant on users' (drivers, road authorities, etc.) understanding of digital tools and their willingness to adopt this new technology. Legal and regulatory frameworks are another notable constraint; the system needs to operate within the confines of rules and regulations concerning data privacy, the use of distributed ledger technology, and inter-state road usage charging.
Pre-conditions	Existence of public sector pricing algorithms for road infrastructure, congestion, pollution, etc. Existence of at least one permissioned network, ultimately anchored to public distributed ledgers, with sufficient node operators offering network access to travelers, secondary actors, and their SSDTs, providing key GAIA services of Governance, Authority, Identity, and Authentication.
Post-conditions	Creation by third-party developers of Web3-compliant B2C apps for road use charging and payment that don’t expose PPI, competitive business data, or payment details.

Use Case Component	Description
Workflow	1. Vehicle Registration: The vehicle owner (driver), identified by their DID, issues a VC including information about their vehicle and their interest in participating in the RUC program. 2. Authority's Interest Expression: The transportation authority, identified by its own DID, reads the driver's VC. If the authority approves the driver's participation, it issues a VC indicating its acceptance. 3. Program Initiation: The driver uses their acceptance VC to generate a Verifiable Presentation (VP) for the authority, signaling the initiation of the RUC program. A smart contract associated with both the driver's and authority's DIDs is created to outline the terms of the program. 4. Road Usage and Real-Time Data Recording: As the vehicle is used, VCs are generated by the vehicle's digital identity and/or phone-based geolocation system, recording data about the mileage, location, and other pertinent data. 5. Charge Calculation: Once a certain threshold of road usage is reached, or at the end of a specific period (e.g., monthly), a VC is issued by the smart contract on the distributed ledger, which calculates the road usage charge based on the data collected. The charge is transparently computed using the terms outlined in the smart contract. 6. Payment Submission or Settlement Trigger: The smart contract associated with the RUC program recognizes the charge calculation VC and generates a trigger to execute payment from the driver to the appropriate transportation authority. The driver issues a transaction settlement VC when the payment settles, and the authority issues a confirmation VC in turn. 7. Interstate Trips Handling: For interstate trips, the system recognizes the different geolocations and distributes payments to the corresponding authorities in each state, preserving the privacy of the driver's exact route using ZKPs.
Alternative workflow	The way DIDs are assigned and managed could vary in an alternative implementation. One approach could be to assign a separate DID for each vehicle, another could be to assign a DID per user (covering all vehicles they may drive), and another could even include assigning a temporary DID for each trip. Each of these approaches would offer different balances between privacy, ease of use, and granularity of data. Similarly, the implementation of VCs could be based on different standards or protocols, such as JSON Web Tokens (JWT) or Linked Data Proofs (LDP), each with its own advantages and trade-offs in terms of compatibility, complexity, and data size.
Information Requirements	• Fee table for all roadways covered by the RUC program • Identifying information for the driver, vehicle, and state authority • In-vehicle telematics data, including location, speed, weight, and driver behavior (fast stops and starts, etc.)

5.4.2.1 Implementation Barriers

User acceptance and adoption may present a barrier to realizing this use case. Users could be wary of a system that monitors their driving habits, even with the promise of privacy-preserving technologies like ZKPs. Similarly, there might be concerns about the security and reliability of a decentralized system,

given that distributed ledger is still largely associated in the public mind with cryptocurrencies and their associated volatility.

Additionally, there are regulatory considerations. The implementation of such a system would require alignment with a multitude of rules and regulations, from data privacy laws to road traffic regulations. Changes to existing legislation or the creation of new laws might be required to enable this new model of RUC.

5.4.3 Usage-Based Insurance (UBI)

Distributed ledger technology is decentralized, meaning that it is not controlled by a single entity with built-in resistance to vendor lock-in. The most anticipated feature of this technology, smart contracts, are digital agreements that run on the distributed ledger. Because smart contract transactions are carried out without human intervention, they are faster and more secure than traditional contracts. This feature of smart contracts has the potential to transform the insurance industry by simplifying processes, improving transparency, and increasing operational efficiency.

Table 15. Usage-Based Insurance (UBI)

Use Case Component	Description
Use Case ID	5.4,3
Use Case Name	Usage-Based Insurance (UBI)
ARC-IT Categorization	Traffic Management, Public Safety
Description	Traditional auto insurance relies on factors such as driver age, location, miles driven, vehicle value, etc. to price risk. These factors have only a loose connection with true risk and are often misrepresented. Recently, insurers have persuaded some customers to install OBD dongles that transmit data such as fast driving, sudden acceleration and deceleration, aggressive lane changes, etc., which are more closely linked to true risk. However, this requires sharing PPI that could be misused, hacked, or sold to third parties. Modern geolocation technologies, combined with vehicle identifiers, ZKPs, and distributed ledger networks, enable new and better ways of underwriting auto collision and liability risk without sharing PPI. With a better understanding of risk, better underwriting will improve insurance product pricing for consumers and align incentives to improve driver behavior, saving lives and reducing injuries.
Type of Distributed Ledger	Permissioned identity recognition layer anchored in public distributed ledger (i.e. Hyperledger, Ethereum)
Actors	Primary Actor: Drivers Secondary Actors: Insurers, reinsurers, insurance regulators

Use Case Component	Description
Operational Objectives/Goals	The objectives/goals for this distributed ledger use case deployment are as follows: ● Vehicle and infrastructure identifiers are recorded on distributed ledger ● Vehicle route and driver behavior monitored and risk cost debited to ledger in real time based on algorithms which account for driver, location, and condition-specific factors ● Periodic presentation and settlement of transactions in smart contracts. ● Periodic, actionable feedback to drivers about behaviors that could be improved to lower their premiums ● Improved driver behavior and improved road safety as drivers respond to feedback and aligned incentives
Constraints/ Assumptions	Assumptions: This use case hinges on the reliable availability of diverse vehicle and driver data. It assumes that all stakeholders, including drivers, insurers, vehicle manufacturers, and regulators, willingly participate. Moreover, it presumes that users will accept this insurance model, and insurers will adjust their business models. Constraints: This model faces regulatory compliance constraints in the heavily regulated insurance industry. Its success also depends on consumer adoption, with the willingness of drivers to participate being a potential barrier. The variability in vehicle technology might limit initial applicability, necessitating reliance on third-party OBD-II dongles, thereby adding to cost and complexity.
Pre-conditions	Driving Behavior Data: To assess risk and calculate premiums, data about the user's driving behavior and the vehicle's usage needs to be continuously collected and sometimes stored. This data could include GPS coordinates, mileage, speed, braking patterns, and more. Real-Time Data Processing Capability: The system must be capable of processing the collected data in real time to calculate risk and adjust insurance premiums dynamically. This requires a robust infrastructure that can handle large volumes of data and perform computations efficiently. Regulatory Compliance: The system should also comply with data protection and insurance regulations, which vary between jurisdictions. Distributed Ledger Infrastructure: A trusted identity layer, leveraging public distributed ledgers, is necessary to provide a decentralized, transparent, and tamper-resistant system for anchoring This distributed ledger should support the implementation of smart contracts to automate many of the system's functions.

Use Case Component	Description
Post-conditions	The implementation of this use case is expected to transform the auto insurance industry, leading to more accurate risk assessment and fairer pricing of insurance premiums. By harnessing distributed ledger, DIDs, VCs, and ZKPs to create a dynamic, usage-based insurance model, insurers can more accurately price policies based on real-time risk factors. This could lead to safer driving behaviors as drivers become more aware that their actions directly influence their insurance costs. Furthermore, this approach is expected to enhance customer trust and satisfaction, as it offers increased transparency and control over personal data. As a significant additional outcome, the privacy-preserving aspect of this approach addresses major concerns related to data security and misuse in the current usage-based insurance models.
Workflow	1. User Identification and Vehicle Registration: The user signs up for the service and registers their vehicle's DID in the system. 2. Driving Behavior Data Collection: As the user drives, data about their behavior and the vehicle's usage, such as GPS coordinates, mileage, speed, hard braking events, sharp turns, and fast accelerations, are collected. Each data entry is associated with a VC, ensuring the integrity and authenticity of the data. 3. Real-Time Risk Assessment: A real-time risk assessment system runs computations to determine the real-time risk of a given trip. Smart contracts can be used to implement the insurance company's risk assessment algorithms. 4. Premium Calculation and Adjustment: The risk assessment results are then used to calculate the insurance premium for the user. This premium is dynamic and can adjust in real-time as new data comes in and the risk profile changes. 5. Payment and Claim Management: The user pays their insurance premiums, with transaction confirmation attestations optionally anchored on-chain. In the case of an accident or claim, the user issues a VC indicating the event. The insurance company, upon verification of the claim, initiates a VC representing the payout.
Alternative workflow	Smartphone Data Collection: In this alternative approach, GPS data could be captured through a mobile application installed on the driver's phone, rather than using vehicle-based sensors. This would alleviate the need for significant hardware upgrades on vehicles but could lead to less precise data. Alternative Structuring: This program flow optimizes for maximum privacy and minimized disruption to existing business processes. Leveraging methods like secure multiparty computation in zero knowledge can enable multiple insurers to service one policy without requiring any expose sensitive business model data.
Information Requirements	• Insurer, driver, and vehicle identifying data • Policy data • In-vehicle telematics data (or data from an alternative data reporting method), particularly location, speed, weight, and driver behavior (fast stops and starts, etc.)

5.4.3.1 Implementation Barriers

Implementing a distributed ledger-based UBI model can encounter several potential barriers. Data privacy and security concerns can arise, especially considering the vast amount of sensitive data involved, such as driver behavior and vehicle location. While ZKPs and other cryptographic measures address these concerns technically, user trust will still be a significant factor. Additionally, regulatory compliance could pose a challenge. The insurance industry is heavily regulated, and creating new pricing models based on such real-time data may require approval from regulators who might not be familiar with distributed ledger technology or novel approaches to insurance like UBI more generally. Additionally, there might be legal constraints concerning data management across different jurisdictions.

5.5 Security and Credential Management (SCMS) Use Cases

5.5.1 Distributed Ledger Approach to Misbehavior Detection (MBD) Reporting

The current approach for detecting and reporting misbehavior within a connected vehicle environment is very early in development. It primarily relies on devices that are detecting misbehavior generating a report that is sent to a central misbehavior authority that processes these reports and when the misbehavior authorities misbehavior threshold is reached it will work with the multiple internal systems to identify all of the certificates, both current and future, associated with the misbehaving device and then adds those certificates to a certificate revocation list (CRL). That CRL would then be distributed to devices within the CV ecosystem. One of the downsides of this approach is the high amount of latency (likely days) between when a device detects misbehavior and when a CRL can be generated and distributed throughout the ecosystem.

The approach detailed in the use case below could provide benefits over this traditional approach by identifying misbehaving devices to other devices in a local region close to immediately while still providing a mechanism for the longer-term revocation mechanisms.

Table 16. Distributed Ledger Approach to Misbehavior Detection Reporting

Use Case Component	Description
Use Case ID	5.5.1
Use Case Name	Distributed Ledger Approach to Misbehavior Detection Reporting
ARC-IT Categorization	This application falls under Support ARC-IT Area Categorization per Task 2 report.

Use Case Component	Description
Description	This use case identifies an approach for reporting misbehavior within a connected vehicle system by having misbehavior detection devices writing observed misbehavior to the distributed ledger where other devices within range would verify that misbehavior report and write it to the distributed ledger. Local devices could then utilize the distributed ledger to determine trust in local devices based on their certificates. A misbehavior authority would monitor this distributed ledger and generate a certificate revocation list (CRL) or separate untrusted device distributed ledger (which would utilize the linkage authorities to remove trust for all certificates associated with a misbehaving device.
Type of Distributed Ledger	Permissioned
Actors	**Primary Actor:** Devices that can detect misbehavior, which in this case would include on-board units (OBU) usually installed on vehicles, roadside units (RSU) or potential a CV device that is focused on only misbehavior detection. **Secondary Actors:** Misbehavior Authority that can identify all credentials associated with an untrusted device.

Operational Objectives/Goals	The Operational Objectives/Goals for this Use Case are:
	• Demonstrate the feasibility of documenting observed misbehavior to a distributed ledger
	• Measure performance of distributed ledger based misbehavior reporting including:
	  ○ Processing Load
	  ○ Time to write, verify and publish misbehavior to distributed ledger
	• Demonstrate feasibility of misbehavior authority based CRL generation of distributed ledger based reporting

Constraints/ Assumptions	• Devices have sufficient processing capability to handle the processes involved in identifying misbehavior, generating the ledger entry and verifying other devices misbehavior entries • The misbehavior authority is able to process the distributed ledger entries if they contain similar information as a misbehavior report

Use Case Component	Description

Pre-conditions	• Defined and agreed to definitions of misbehavior. Current definitions include:
	  ○ ETSI Misbehavior Reporting Services (https://www.etsi.org/deliver/etsi_ts/103700_103799/103759/02.01.01_60/ts_103759v020101p.pdf)
	  ○ SCMS Manager Misbehavior Report and Application Specification for Connected Vehicle Pilot Deployment (https://scmsmanager.org/wp-content/uploads/2020/01/Misbehavior-Report-and-Application-Specification-v1.0.pdf)
	  ○ Potentially additional misbehavior definitions from SAE and SCMS Manager
	• Defined format for documenting misbehavior within the distributed ledger.
	  ○ The documents listed above include misbehavior report formats that can be used as a starting point
	• Application software for CV devices that can detect some/all of the defined misbehaviors, write to the distributed ledger and then verify the misbehavior detected by others
	• Misbehavior Authority that can process entries on the misbehavior reporting ledger and generate a CRL

Post-conditions	• Distributed ledger with verified misbehavior on the ledger • CRL with future certificates from devices identified as misbehaving • Logs from devices that can be analyzed for performance metrics
Workflow	The following use case workflow describes the sequence of events for conducting distributed ledger based misbehavior reporting. 1. 3 or more CV devices are operating within the CV range (~300m) of each other 2. CV Device 1 starts exhibiting one of the defined misbehaviors 3. CV Device 2 and CV Device 3 independently identify CV Device 1 exhibiting misbehavior 4. CV Device 2 generates a misbehavior entry on the distributed ledger. 5. CV Device 3 having independently observed the same misbehavior, verifies that misbehavior entry. 6. With the misbehavior entry verified the misbehavior is written to the misbehavior reporting distributed ledger 7. CV Device 4 reads the distributed ledger update and decides to cease processing messages from CV Device 1. 8. The Misbehavior Authority monitors the misbehavior reporting distributed ledger. 9. CV Device 1 has enough misbehavior on the misbehavior reporting distributed ledger to trigger the revocation of their credentials. 10. The Misbehavior Authority works with its internal systems to identify future certificates associated with CV Device 1 and adds them to the CRL. 11. The Misbehavior Authority distributes the updated CRL to the CV device ecosystem. 12. CV devices download and apply the updated CRL.

Use Case Component	Description
Alternative workflow	10. A. The Misbehavior Authority generates a new entry on the Untrusted Device Distributed Ledger for CV Device 1, which includes future certificate information for CV Device 1. 11. A. Other internal elements of the Misbehavior Authority verify the new CV Device 1 entry on the Untrusted Device Distributed Ledger and the new entry is written to the Ledger. 12. A. Other CV devices utilize the updated Untrusted Device Distributed Ledger to determine trust in other devices. The other alternate flow would be increasing the number of devices needed for ledger entry verification.
Information Requirements	• Misbehavior definitions • Misbehavior reporting ledger entry format • CV messages (used to detect the misbehavior) • Misbehavior reporting distributed ledger • Untrusted Device Distributed Ledger

5.5.1.1 Implementation Barriers

Current connected vehicle (CV) devices are usually resource constrained from a processing standpoint. The addition of a potentially computation intensive task such as writing to and reading from a distributed ledger may be too resource intensive for current CV devices to perform. This could be addressed through the use of new roadside infrastructure that connects to a Traffic Management Center or Mobile Edge Computing and process the reads/writes to the DLT in bulk, but that would necessitate upfront capital investment. Additionally, the current SCMS system and misbehavior authority are not configured to use DLT and it may take extensive work to integrate a DLT based aspect of the system into the current architecture.

5.5.2 Use of Federated Certificate Authority to Register Object Identifiers

A Federated Certificate Authority (FCA) is an innovative approach to digital identity and security in decentralized systems. It's a collective of member organizations that jointly provide trust services in a decentralized manner. Unlike traditional Certificate Authorities (CAs), which are centralized entities that issue and manage digital certificates, a FCA operates on a distributed basis, with multiple independent entities participating in the issuance and validation of certificates.

In a typical FCA setup, each participating entity operates one or more nodes that are part of the overall network. These nodes have the ability to issue, validate, and revoke certificates within their domain of authority. The federated nature of the system allows for a higher degree of resilience and security compared to a centralized CA. If one node is compromised, it doesn't necessarily impact the integrity of the entire system.

An important feature of a FCA is that it can support self-sovereign identities. This means that entities can control their own digital identities, reducing reliance on third parties. For example, in the context of the Internet of Things (IoT), an FCA can enable devices to have trusted, verifiable identities that are used in secure transactions. In this scenario, the FCA could help facilitate trusted interactions between devices in a scalable and decentralized manner.

A FCA can serve as the backbone for a wide range of applications, from secure API access management in microservices architectures to registering object identities in an IoT ecosystem. By leveraging the benefits of decentralization and self-sovereign identity, a FCA offers a compelling alternative to traditional trust models in the digital world.

An FCA can be instrumental in registering object identities, especially in the context of IoT. In the world of connected devices, establishing a trusted identity for each object is of paramount importance. An FCA offers a scalable solution to create and manage these identities in a decentralized manner, reducing reliance on centralized authorities. This is achieved through the creation and management of Decentralized Identifiers (DIDs), which are unique, cryptographically protected identifiers that are self-sovereign, meaning they are created and managed by the entities to whom they belong. When anchored in a tamper-evident decentralized trust network, DIDs allow these entities (objects) to authenticate themselves, which is foundational to their participating in secure, private transactions. This approach empowers connected entities to own and control their data while shielding sensitive data from aggregators and bots, thereby enabling more secure IoT transactions.

Table 17. Use of Federated Certificate Authority to Register Object Identifiers

Use Case Component	Description
Use Case ID	5.5.2
Use Case Name	Use of Federated Certificate Authority to Register Object Identifiers
ARC-IT Categorization	SU06 Object Registry and Discover SU08 Security and Credentials Management
Description	Vehicle-to-Everything (V2X) communication relies on wireless objects exchanging information in real time. The objects exchanging information must trust each other to do so. It would be computationally infeasible for the objects to verify messages from other objects every time messages are exchanged. Hence, such objects must be properly registered with an “authority” which takes on the responsibility of guaranteeing such trust to objects. An FCA can be used to register object identities, leveraging distributed ledger to enable traceability and visibility of which objects were provided identity, when an object’s identity has been revoked or delegated, etc.
Type of Distributed Ledger	Permissioned and public.
Actors	**Primary Actor**: A consortium of entities that form the certificate authority. **Secondary Actors**: Device manufacturers, state/local agencies, USDOT.
Operational Objectives/Goals	Create one or more federated certificate authorities (if more than one, they must be compatible) for device makers to register their device identities before being used in V2X deployments.
Constraints/ Assumptions	The device makers have to agree on the infrastructure/architecture/standards of the certificate authority, otherwise it would not be adopted by the industry.
Pre-conditions	The industry must agree on implementation standards for registering devices on distributed ledger and perform pilots to solve practical issues for object registration and revocation.
Post-conditions	The use case should encourage various entities to collaboratively form such authorities in a compatible and financially sustainable way.

Use Case Component	Description
Workflow	1. Identity Request: The owner of the object requests the FCA to generate a DID for that object. This DID can issue an identity credential, which would include necessary information about the object, such as its type, model, manufacturer, etc. 2. Identity Creation: Once verified, the FCA creates a unique digital identity for the object. This involves generating a digital certificate for the object, which includes the object's unique identifier and other relevant information. 3. Identity Assignment: The FCA assigns the created identity to the object. This could involve sending the digital certificate to the object or storing the certificate in a location where the object can retrieve it. 4. Identity Usage: The object uses its assigned identity for various activities in the system, such as authenticating to services, establishing secure connections, or engaging in transactions. 5. Identity Validation: Whenever the object interacts with other entities or services in the system, those entities/services validate the object's identity by checking its digital certificate with the FCA. If the identity is valid, the interaction proceeds; otherwise, it is denied.
Alternative workflow	An alternative workflow could have object owners do the DID generation themselves, simply anchoring the generated DID in the FCA. Similarly, there are a variety of ways to implement a federated certificate authority and a DID resolver, each of which implies different tradeoffs.
Information Requirements	The device manufacturers and the developer of the authority must agree to the implementation standards for issuing and revoking device identities.

5.5.2.1 Implementation Barriers

A key barrier to implementation even at the pilot stages is funding. Without well-funded pilots, the efficacy of the authority for real-world transportation use cases and the ability to deter security attacks will be infeasible.

5.5.3 Federated Certificate Authority for Secure API Access Management

In the rapidly progressing world of automotive and transportation technology, APIs (Application Programming Interfaces) have become essential tools. They act as bridges connecting various components of modern transportation systems, be it vehicle-to-infrastructure communication, telematics data sharing, or fleet management solutions. As the automotive landscape moves towards more integrated and distributed networks, especially with the rise of connected vehicles and smart infrastructure, the challenge to securely manage API access amplifies. FCAs are poised to play an indispensable role in ensuring secure API access management tailored for the automotive and transportation sector.

In this context, every component, whether it's an application within a car's onboard system or a microservice in a traffic management solution, is granted a distinct identity by the FCA. This authority, functioning as a decentralized network of certificate-issuing nodes, each managed by diverse entities,

distributes digital certificates. These certificates act as digital identities, authenticating each component when it tries to access or communicate via an API.

The beauty of the federated model lies in its trustworthiness. Each participating entity retains control over its dedicated node and the certificates it generates. By decentralizing the process, we eliminate the dangers associated with a single point of failure and bolster the system's overall security. This becomes especially crucial in the transportation arena, where the integrity of communications can have direct safety implications. By leveraging the unique identities assigned by the FCA, not only can we ensure that only approved components access specific APIs, but we can also closely monitor and regulate these accesses.

Therefore, when integrating sophisticated transportation systems, the adoption of the FCA model is paramount. It doesn't just enhance the security fabric but also provides precise, effective, and adaptable API access management suitable for the dynamic needs of the automotive and transportation ecosystem.

Table 18. Federated Certificate Authority for Secure API Access Management

Use Case Component	Description
Use Case ID	5.5.3
Use Case Name	Federated Certificate Authority for Secure API Access Management
ARC-IT Categorization	SU08 Security and Credentials Management
Description	In the world of distributed systems where numerous applications and microservices interact, managing secure API access is a significant challenge. An FCA, operating as a decentralized network of certificate-issuing nodes, can provide a unique digital identity to each application or microservice in the system. These identities authenticate each entity during API calls, ensuring only authorized services access specific APIs. This decentralized approach enhances security by avoiding a single point of failure and allowing for effective, granular API access control. This way, the FCA can significantly improve the security posture of distributed systems while enabling efficient API access management.
Type of Distributed Ledger	Public and/or permissioned
Actors	**Primary Actor**: Application/Microservice owner **Secondary Actors**: FCA
Operational Objectives/Goals	The objectives/goals for the Federated Certificate Authority for Secure API Access Management use case are: • Establish a global, scalable, and resilient API security infrastructure. • Enable secure, private, and non-reputable API access management for members/users of the FCA. • Deliver API security as a service to members/users of the FCA.

Use Case Component	Description
Constraints/ Assumptions	Constraints: • Scalability: The FCA needs to be able to scale to handle a large number of API calls. This is particularly important in microservices architectures where there could be numerous internal API calls. • Performance: The FCA should not significantly degrade the performance of the API calls. Extra security should not come at the cost of usability. • Regulatory Compliance: The FCA must comply with various data protection and privacy regulations. This can vary depending on the jurisdiction and industry of the participating organizations. Assumptions: • Secure Communication: It's assumed that the communication between the nodes of the FCA and the services making API calls is secure. This could be through secure network protocols like HTTPS or through the use of Virtual Private Networks (VPNs). • Accurate Time Synchronization: Accurate timekeeping is essential for many security protocols. It's assumed that all nodes in the FCA network have accurate and synchronized clocks. These constraints and assumptions would need to be validated and addressed during the design and implementation of the FCA for Secure API Access Management.
Pre-conditions	Data Encryption: All data, especially sensitive data such as identifiers and API call data, must be encrypted during transmission and at rest. Secure Key Management: The keys used for encrypting and decrypting the data must be securely managed. They should be stored securely and should never be exposed. Auditability: All actions related to the FCA and API access management should be logged and auditable. This is important for accountability and for investigating any security incidents. Secure Communication: Communication between the FCA nodes and the services making API calls should be secure. This could be achieved through secure network protocols like HTTPS or the use of VPNs. It's important to note that these requirements can vary depending on the specific context and implementation of the FCA.

Use Case Component	Description
Post-conditions	The expected outcome of the Federated Certificate Authority for Secure API Access Management use case is an enhanced level of security in the communication between microservices in a distributed system. With each application or microservice possessing a unique identity granted by a Federated Certificate Authority, there is an assurance of authenticated and secure API calls. This implies that only authorized services will be able to access certain APIs, thereby preventing unauthorized access and potentially malicious activities. Consequently, this use case promotes a robust distributed system where data privacy is prioritized and security is upheld, which in turn leads to more reliable applications and services and fosters trust among system users and administrators.
Workflow	1. Identity Creation: When a new application or microservice is created within the distributed system, its owner generates a DID for that application or microservice and anchors it in the FCA. 2. API Access Request: The application or microservice then makes a request to access a specific API within the system. This request includes the entity's DID and a digital signature created using the entity's private key. 3. API Access Validation: The API, before granting access, verifies the request. This verification involves checking the entity's certificate, validating the digital signature using the entity's public key (found in the certificate), and confirming that the certificate was indeed issued by the FCA. 4. API Access Granting or Denial: If the request is validated successfully, the API grants access to the requesting entity. If not, the API denies the request. 5. API Usage: Once access is granted, the application or microservice uses the API to perform the necessary operations. 6. This flow repeats every time an application or microservice in the distributed system needs to access an API, ensuring secure and authenticated API calls at all times.
Alternative workflow	An alternative approach to implementing the "Federated Certificate Authority for Secure API Access Management" use case could utilize a dynamic and context-based access control mechanism, introducing an additional layer of security. In this scenario, rather than the API granting or denying access solely based on the validated request, the system could consider additional contextual information such as the current load on the API, the time of the request, and the nature of the requested operation. For example, an entity requesting access during peak usage times or frequently within a short time span might be subject to additional verification steps or temporary throttling.
Information Requirements	Identity Data: The FCA needs data to identify and authenticate the entities involved in the API calls. This may include DIDs, public/private keys, etc. API Call Data: The FCA needs to know the details of the API call such as the API endpoint, the parameters, and the payload. This data is necessary to validate the API call.

5.5.3.1 Implementation Barriers

Adoption Resistance: Convincing stakeholders of the benefits and necessity of implementing a Federated Certificate Authority could be challenging. This could stem from a lack of understanding of the technology, concerns about the cost and ROI, or hesitation to change established processes.

Network and System Security: Implementing a Federated Certificate Authority involves rigorous security measures. Any vulnerability in the system could expose the organization to risks such as data breaches or cyberattacks, leading to financial and reputational damage.

Regulatory Hurdles: Certain sectors have stringent regulations governing data security and privacy. Navigating these regulations to ensure the Federated Certificate Authority complies with all legal requirements could be a complex process.

Data Management Challenges: Ensuring the privacy and security of data when issuing, revoking, and managing certificates can be a complex task. This is particularly true when dealing with large volumes of data or sensitive information.

5.5.4 Federated Certificate Authority for Secure Multi-Party Computation

Intersection safety is of paramount importance in the domain of contemporary transportation. The integration of technology to enhance this safety has been under rigorous scrutiny, and Secure Multi-Party Computation (SMPC) presents a robust solution. SMPC allows for a collaborative computation among various vehicles and infrastructure components based on shared data, without the revelation of individual inputs. This collaborative approach is especially beneficial for complex scenarios such as traffic flow optimization at intersections, where discrete data sharing is necessary without compromising on individual data privacy. The efficacy of SMPC, however, hinges on the trustworthiness of the participants, which is addressed by the Federated Certificate Authority (FCA).

The FCA assigns authenticated identities to units within a transportation framework, be it vehicles or integral infrastructure elements. These authenticated identities ensure the legitimacy of each participant, establishing an environment where neither malicious entities nor unauthenticated ones can compromise the SMPC process. Specifically for intersection safety, the FCA is instrumental in allocating these identities to vehicles and infrastructure elements, such as traffic signals or pedestrian monitoring systems. This rigorous authentication ensures that only vetted participants partake in the computation process, thereby maintaining the integrity and authenticity of the resultant decisions.

Adopting a federated model for the FCA implies a decentralization of the verification responsibility across multiple nodes or entities. This distributed architecture is critically salient for intersection safety as it mitigates the risks associated with a centralized point of failure.

Upon authentication by the FCA, vehicles are equipped to engage in SMPC with a heightened degree of confidence. For example, in strategizing the optimal timing sequence for traffic lights rooted in real-time vehicular data, individual vehicle inputs can be integrated without disclosing granular details, such as exact velocities or intended routes. Consequently, intersection operations can be refined with an emphasis on efficiency, all while upholding the privacy prerogatives of individual drivers.

In summary, the amalgamation of a Federated Certificate Authority with Secure Multi-Party Computation represents a sophisticated advancement in the pursuit of intersection safety. By instilling trust and ensuring vetted participation, it heralds a more secure and efficient trajectory for intersection

management, underscoring the potential for safer transportation ecosystems for all stakeholders involved. As urban environments and their corresponding transportation networks continue to mature, the synergistic relationship between FCA and SMPC will be indispensable for achieving optimal traffic management outcomes.

Table 19. Federated Certificate Authority for Secure Multi-Party Computation

Use Case Component	Description
Use Case ID	5.5.4
Use Case Name	Federated Certificate Authority for Secure Multi-Party Computation
ARC-IT Categorization	SU08 Security and Credentials Management
Description	The Federated Certificate Authority for Secure Multi-Party Computation use case pertains to scenarios where multiple entities need to perform computations on shared data, without revealing their individual inputs to each other. This could apply in situations such as sharing automated vehicle training data, where confidentiality of individual input is crucial. The FCA would provide a secure identity layer for participants to authenticate themselves and secure the computation process. This ensures a secure, private, and non-reputable multi-party computation environment.
Type of Distributed Ledger	Public and/or permissioned
Actors	Primary Actor: Entities performing computation on shared data Secondary Actors: FCA
Operational Objectives/Goals	• Provide a secure and reliable mechanism for granting identities to participants involved in multi-party computations, enhancing the overall security of the computation process. • Ensure privacy by allowing participants to compute shared data without revealing their individual inputs. • Offer a level of assurance to all participants that their input will remain confidential and secure during the computation process. • Facilitate trust among participants, allowing them to engage in computations with confidence in the system's integrity. • Contribute to the democratization of the IoT commerce ecosystem by reducing reliance on centralized authorities, thereby empowering entities to control their data and transactions.

Use Case Component	Description
Constraints/ Assumptions	The Federated Certificate Authority for Secure Multi-Party Computation use case has several constraints that need to be considered. Firstly, computational limitations are a significant constraint because SMPC requires substantial computational resources. The ability to scale these computations while maintaining privacy and security is crucial. The use case also makes several assumptions. It presumes that the FCA can reliably verify and issue identities for the entities involved, which implies an efficient and secure identity verification process. The system also assumes that participants will follow the protocol and rules defined for SMPC. Non-compliance could compromise the privacy and security of the computation. Another assumption is that there is sufficient infrastructure (both hardware and software) available to support the high computational and data storage demands of SMPC. Finally, the system presupposes that participants adhere to the DIDs standard and other relevant technical standards. This adherence ensures interoperability and security within the system.
Pre-conditions	The Federated Certificate Authority for Secure Multi-Party Computation use case requires specific conditions and data needs to be effectively implemented. The conditions include: Standards Adoption: Entities involved in the use case should adopt the DID and VC standards. This adoption is crucial for the identification and verification of entities participating in SMPC. Security of Computation: The computation process itself must be secure. This means that it should be resilient against attacks that aim to disrupt the computation or reveal the private data involved. Regulatory Compliance: The system must comply with all relevant data privacy and cybersecurity regulations. This compliance includes ensuring that identity data is stored and used in a manner that respects the privacy rights of the entities involved. In sum, a balance of reliable infrastructure, protocol adherence, and strict privacy and security measures are critical conditions for the successful implementation of the Federated Certificate Authority for Secure Multi-Party Computation use case.

Use Case Component	Description
Post-conditions	An expected outcome of the Federated Certificate Authority for Secure Multi-Party Computation use case is the establishment of a secure and trusted system for computation among multiple parties where sensitive data is involved. This system enables participants to compute a function over their inputs while keeping those inputs private. Moreover, an additional benefit of this use case is the enhancement of data security in the context of growing IoT and digital commerce activities. With the FCA's federated approach and by using best practices for data security, the vulnerabilities associated with decentralized digital businesses can be mitigated. This leads to a reduction in the cost of trust, including security and regulatory compliance costs, thus fostering a more robust and democratic IoT commerce ecosystem.
Workflow	1. Each participating party generates a CSR containing their public key and relevant information. 2. Each participating party uses a secure MPC protocol to jointly compute the certificate signing process. 3. After completing the secure computation, the federated network generates the certificate using the joint results. 4. The signed certificate is distributed to the requesting party via a secure channel.
Alternative workflow	An alternative implementation approach for the Federated Certificate Authority for Secure Multi-Party Computation use case could involve the use of additional/alternative decentralized and privacy-preserving approaches to ensuring security and privacy such as secure enclaves or homomorphic encryption. In this approach, each participating party would maintain their private enclave or encrypted data, ensuring that their sensitive information remains protected. The secure enclaves could be used to securely compute the certificate signing process without revealing individual inputs to other parties. Alternatively, homomorphic encryption techniques could enable the parties to perform computations on encrypted data without decrypting it, preserving privacy.

Use Case Component	Description
Information Requirements	Shared Computation Inputs: The federated network will require inputs from the participating parties for performing computations securely. These inputs may include the CSRs, cryptographic keys, threshold values, or other relevant information required for the certificate signing process. Certificate Data: The federated network will generate certificates as an output of the MPC process. These certificates contain information about the party, such as their identity, public key, validity period, and any relevant attributes associated with the certificate. Network Communication Data: During the MPC process, data related to network communication is required. This includes messages exchanged between the participating parties, encrypted data transmission, and secure communication protocols used to protect the confidentiality and integrity of the data being shared. It is important to note that the specific data requirements may vary depending on the chosen implementation approach, the MPC protocols employed, and the security and privacy needs of the federated network.

5.5.4.1 Implementation Barriers

Technical Complexity: Secure MPC protocols and cryptographic techniques can be technically complex to implement and integrate into existing systems. The design and implementation of robust and efficient MPC algorithms require specialized knowledge and expertise in cryptography and distributed systems.

Performance Overhead: Secure MPC protocols often introduce additional computational and communication overhead compared to traditional centralized systems. The computation and communication costs associated with securely aggregating inputs, ensuring privacy, and reaching consensus among multiple parties can impact the system's performance and responsiveness.

Legal and Regulatory Compliance: Implementing an FCA may involve compliance with legal and regulatory requirements, such as data protection, privacy, and industry-specific regulations. Navigating these compliance frameworks, ensuring data sovereignty, and addressing cross-border data transfer challenges can be time-consuming and resource-intensive.

6 Conclusions and Next Steps

This report further explores the work from the Task 2 report: *Potential Categories for the Application of Blockchain in Intelligent Transportation Systems (ITS)* by conducting a gap analysis on five selected distributed ledger applications from this report. The gap analysis was conducted by first determining the current state of these applications, (1) Multimodal Trip Planning and Fare Payment System, (2) Transportation-based Virtual Power Plant with Payment, (3) Freight Management, (4) Use-based Fees, and (5) Security and Credential Management (SCMS), and then determining the desired/future state of these applications based on stakeholder feedback and literature reviews. Gaps were then identified by determining what steps, if any, could be taken to get from the current state to the future state for a given application. Sixteen use cases were developed, providing real-world scenarios to illustrate how a distributed ledger could potentially or is currently being used to advance the current state of the five applications to their desired/future state.

The use cases and gap analysis presented in this report have been validated with internal USDOT stakeholders prior to publication. These materials will be used to develop a comprehensive research plan structured to further explore the application of distributed ledger to ITS solutions and provide inputs to ITS JPO Program Areas. This research plan is expected to be completed in late 2023 and remain an internal USDOT document. ITS JPO will collaborate with modal partners, where appropriate, to conduct the necessary research activities.

In 2024, the materials in this report will also be presented to other industry stakeholders to help prioritize the greatest research needs and adapt to real-world conditions. Feedback from the industry is considered a critical input to ensure that ITS JPO funding would produce materials with the largest potential impact and utility for the research and deployment communities.

Appendix A. References

Abrol, Ayushi. 2022. “Blockchain Vs. Distributed Ledger Technology.” *Blockchain Council*. March 11, 2022. https://www.blockchain-council.org/blockchain/blockchain-vs-distributed-ledger-technology/.

Baseline Technical Steering Committee. 2022. “Digital Business at a Crossroads.” *Baseline Protocol*. December 7, 2022. https://www.baseline-protocol.org/blog/digital-business-at-a-crossroads/.

Blonsky, Michael, Prateek Munankarmi, and Sivasathya Balamurugan. 2021. “Incorporating Residential Smart Electric Vehicle Charging in Home Energy Management Systems: Preprint.” National Renewable Energy Laboratory. https://doi.org/NREL/CP-5D00-78540.

Burdova, Carla. 2022. “What Is Web 3.0 (Web3 Definition)?” Avast. December 8, 2022. https://www.avast.com/c-web-3-0.

“Citopia MaaS — Transit IDEA Award.” 2022. MOBI | The New Economy of Movement. February 8, 2022. https://dlt.mobi/maas/.

Edwards, Shannon. 2021. “IBI Group, SWTCH Energy Inc., and Slate Asset Management Launch First Blockchain-Based, Electric Vehicle-to-Building Pilot in Canada.” *Arcadis | IBI Group*. October 7, 2021. https://www.ibigroup.com/2021/10/07/ibi-group-swtch-energy-inc-and-slate-asset-management-launch-first-blockchain-based-electric-vehicle-to-building-pilot-in-canada/.

“First Open Battery Identity Standard Enables Web3 Supply Chain Efficiency.” 2022. *MOBI | The New Economy of Movement*. July 19, 2022. https://dlt.mobi/bin-release/.

Global Industry Analysts. 2022. “With Market Size Valued at $173.7 Billion by 2026, It’s a Healthy Outlook for the Global Battery Market.” *PR Newswire*. January 18, 2022. https://www.prnewswire.com/news-releases/with-market-size-valued-at-173-7-billion-by-2026--its-a-healthy-outlook-for-the-global-battery-market-301461864.html.

Kückelhaus, Dr. Markus, and Gina Chung. 2018. “Blockchain in Logistics.” DHL Customer Solutions & Innovation. https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf.

Minott, Owen. 2022. “Mileage-Based User Fee Pilot Programs and the IIJA.” Bipartisan Policy Center. February 11, 2022. https://bipartisanpolicy.org/blog/mileage-based-user-fee-pilot-programs-and-the-iija/.

“National Electric Vehicle Infrastructure Standards and Requirements.” 2023. Federal Highway Administration. https://www.federalregister.gov/documents/2023/02/28/2023-03500/national-electric-vehicle-infrastructure-standards-and-requirements.

Rajbhandari, Rajat. n.d. “MOBI Battery Initiative: Now and Future.” *MOBI | The New Economy of Movement*. https://dlt.mobi/mobi-battery-initiative/.

Smith, John G. 2020. “Walmart Canada Leverages Blockchain to Solve a Billing Nightmare.” *Truck News* (blog). September 11, 2020. https://www.trucknews.com/features/walmart-canada-leverages-blockchain-to-solve-a-billing-nightmare/.

“Truck Freight Tonnage and Revenues Rise in 2022, According to Report.” 2023. *American Trucking Associations*. July 19, 2023. https://www.trucking.org/news-insights/truck-freight-tonnage-and-revenues-rise-2022-according-report.

U.S. Bureau of Labor Statistics. 2019. “Table 1720. Type of Area: Annual Expenditure Means, Shares, Standard Errors, and Coefficients of Variation, Consumer Expenditure Survey, 2019.” U.S. Bureau of Labor Statistics. https://www.bls.gov/cex/tables/calendar-year/mean-item-share-average-standard-error/cu-area-type-2019.pdf.

“What Is Blockchain Technology?” n.d. IBM. https://www.ibm.com/topics/blockchain.

Whitacre, Brian, and Lara Brooks. 2017. “Web 2.0: What Is It and What Can It Do For My Business?” OSU Extension. April 2017. https://extension.okstate.edu/fact-sheets/what-is-it-and-what-can-it-do-for-my-business-2.html.

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO--23-119

U.S. Department of Transportation