AUTOMOTIVE EDGE
COMPUTING CONSORTIUM

AECC PROOF OF CONCEPT

Enabling Trusted HD Mapping Data Updates in a Multi-organizational Distributed Edge

By Toyota Motor Corporation, Intel

Version 1.0

Abstract

The AECC is developing an ecosystem of automotive OEMs, telecom network operators, service providers, and cloud and data analytics companies. We're in the process of unlocking the opportunities in big data delivery and processing for connected vehicles.

This opportunity comes with the challenge of securing the shared data and ensuring only authenticated accounts can access the systems shared by multiple organizations. This arises from the fact that the different entities accessing the system do not necessarily trust each other — nor should they. Cybersecurity is something that must be taken extremely seriously in any modern digital network.

One example of a valuable service for connected vehicle operators is HD maps. True HD maps aren't like the navigation services that many people use today; instead, they are extremely high-resolution and are updated in near-real time. They're often cited as one of the essential tools for self-driving cars, but they also have the potential to improve safety and route efficiency for any connected vehicle.

A previous proof of concept showed that the AECC's approach to mapping generation via distributed networks would work well at scale. Critically, it also showed that the maps could be updated just in time for the accuracy we need.

In the future, however, multiple companies will need to collaboratively collect and share geospatial data from various sources to create and maintain maps that are accurate and up-to-date.

The twofold goal of this proof of concept was to show that decentralized authentication for this will work, and so would the cross validation from various sources of the map data.

Why does the map update data need to be checked? In a crowdsourcing system like this, raw data for map updates are collected from various sources, such as vehicles, roadside cameras, and aerial imagery. But not all of the raw data sources can be correctly inferred as the same ground-truth event: one source may show the moment before a traffic accident, and another the moment it happens. Similarly, an image from one source may be crystal clear, and another blurry because the camera lens was obscured by snow.

The data, therefore, must be integrated and processed using algorithms and machine learning techniques to generate maps that can be used for vehicle navigation, logistics, urban planning, and other applications.

For this proof of concept, the engineering team used this procedure:

1. All the vehicles which accessed the map service were authenticated via blockchain.
2. Three vehicles uploaded raw data to the edge servers in different locations.
3. The generated map data was cross-validated via blockchain.
4. The new map update was downloaded by the last vehicle.

The study showed that map data can be securely shared amongst organizations for cross-validation, and that authentication can be controlled by many organizations using edge infrastructure. While the authentication experience isn't centrally controlled, it provides a better and more seamless user experience than traditional authentication.

Business Strategy

In the short term, the goal of our solution is to reduce the cost of operation. Blockchain technology can help eliminate discrepancies in the HD map update process, thus reducing map maintenance costs. It also provides traceability of these processes, ensuring trust between participants.

Blockchain is about data decentralization. It eliminates reliance on a single storage unit by leveraging the advantages of multiple nodes. The key attributes of blockchain that were used in our PoC to manage HD map updates are transparency, security, integrity, and efficiency.

To scale into the future, we could configure the business model to partner with various regional authorities, map companies, and data service providers to customize and commercialize our solution — not just for map data maintenance but also other road infrastructure information updates.

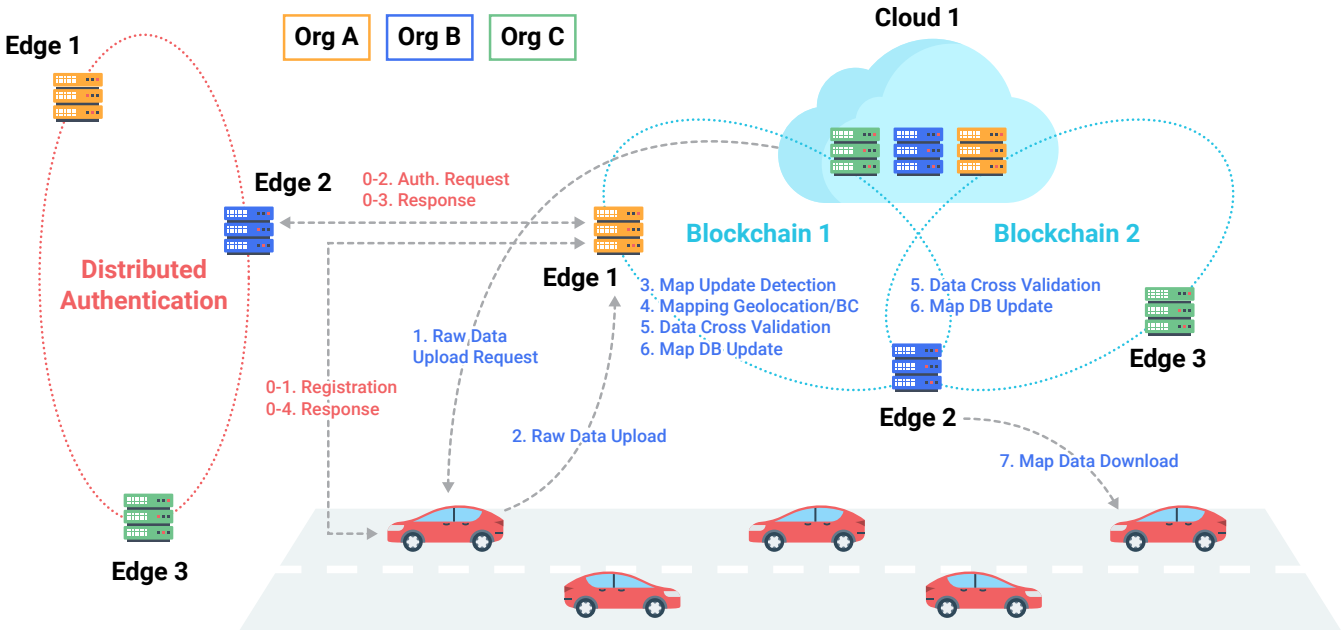
Proof of Concept Objective

The goal of this PoC was to verify the effectiveness of the new decentralized authentication and map update data validation processes in a multi-organizational distributed edge architecture.

HD maps and service login management using edge computing architecture are use cases that have been discussed before in AECC. In this scenario, achieving distributed map update management was an important challenge for fulfilling HD map service requirements. The engineering team proposed a PoC with distributed ledger technology to verify its effectiveness on distributed data management.

Proof of Concept Scenario

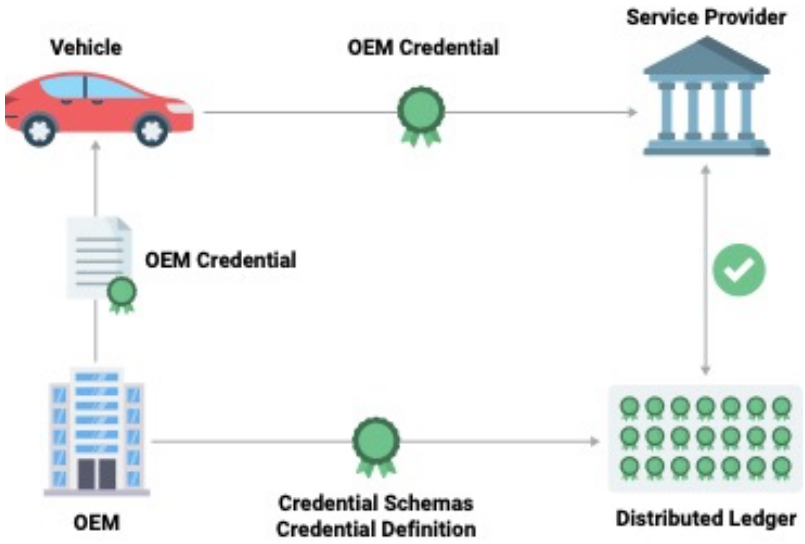
Essentially, three vehicles were uploading raw data associated with the same area and time period to the edge servers in different locations. Then the generated map update data was cross-validated via blockchain, and the new map update was downloaded by the last vehicle. All the vehicles were authenticated to access the map service via blockchain.



Process

As mentioned, there were two processes happening in this scenario: the authentication process and the map update generation process.

Vehicle Authentication



This was the step-by-step process for the authentication of the vehicles:

1. The OEM issued credentials to each vehicle. These credentials were complex strings of code that included unique identifiers for the vehicle.
2. The OEM shared the credentialing schema with the distributed ledger.
3. Each organization in the service ecosystem was able to use the unique identifiers from the OEM for each vehicle as part of its credentialing system. These were also verifiable via the distributed ledger.
4. Whenever a vehicle tried to access the map service (to either upload or download data) the distributed ledger provided the authentication.

From the perspective of the user on the vehicle side, the authentication process was the same as with traditional public key infrastructure (PKI) authentication, even though there wasn't one central authority. Each of the multiple nodes of the distributed ledger could confirm that the access request was legitimate.

The team set up the test to include valid credentials but also tested invalid information successfully.

Test Scenario for Map Data Cross-Validation

This was the step-by-step process for the map update and checking process:

1. Vehicle 1 (connected to edge server 1) uploaded raw data that showed a traffic accident.
2. Vehicle 2 (connected to edge server 1) uploaded raw data that showed traffic congestion.
3. Vehicle 3 (connected to edge server 2) uploaded raw data that showed a traffic accident.
4. The data was processed and cross-validated in the distributed edge network.
5. Vehicle 4 (connected to edge server 3) downloaded the newest map ahead that included the new traffic situations.

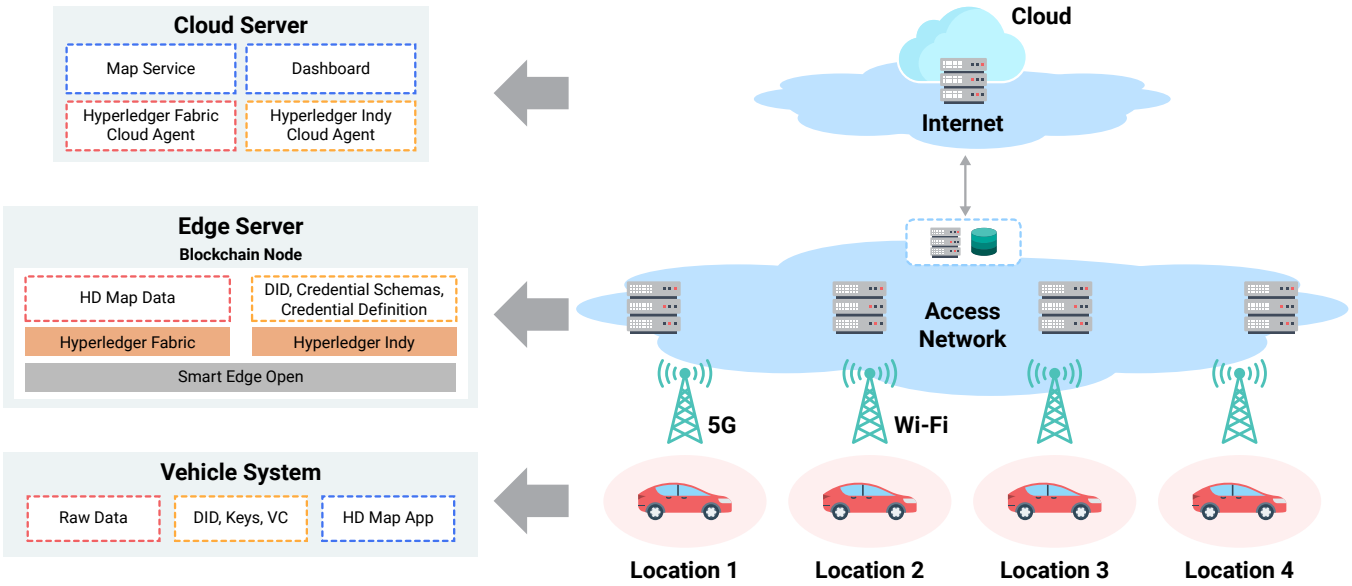
Challenges with Crowdsourced Map Generation

There are several challenges associated with a crowdsourced map generation system with multiple parties, including:

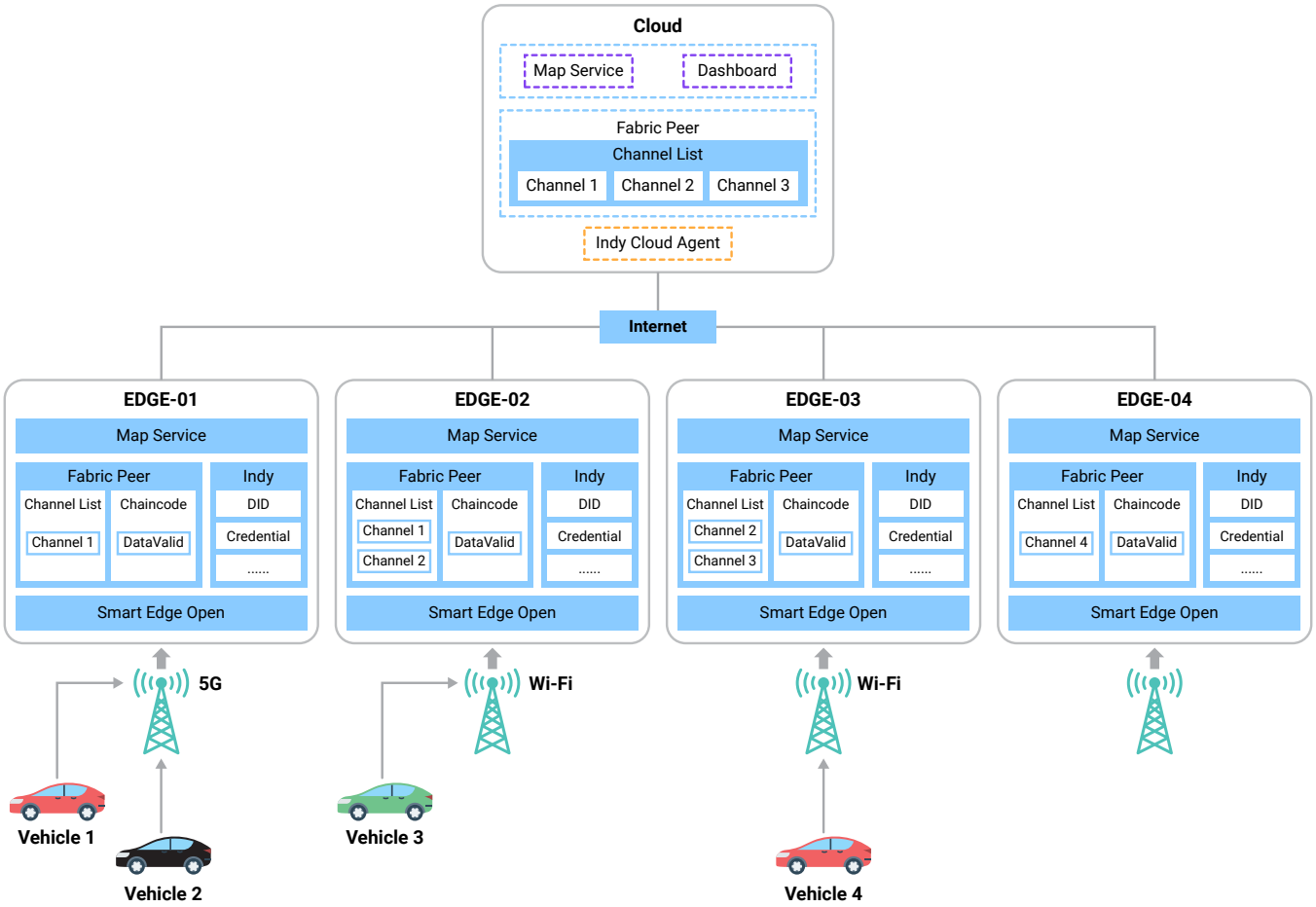
a. **Data quality:** One of the biggest challenges in a crowdsourced map generation system is ensuring the quality of the data. The data can come from various sources, including vehicles, sensors, and other data providers. Therefore, there may be differences in the accuracy, completeness, and consistency of the data, which can affect the overall quality of the map.
b. **Data privacy and security:** In a crowdsourced map generation system, data is typically shared among multiple parties. This raises concerns about data privacy and security, as the data may contain sensitive information about individuals or organizations. Therefore, it is important to ensure that appropriate security measures are in place to protect the data from unauthorized access or modification.
c. **Data ownership and control:** In a crowdsourced map generation system, multiple parties may contribute data to the map. This raises questions about data ownership and control, as each party may have different rights and responsibilities regarding the data.
d. **Coordination and governance:** In a crowdsourced map generation system with multiple parties, it is important to establish a coordinated and collaborative governance framework to ensure that all parties are working together effectively and efficiently. This requires trust and traceability among all parties involved in the map generation process.

In summary, new technology is needed to address the above challenges by providing a secure and transparent framework for data sharing and service authentication among multiple organizations for the AECC ecosystem.

Functional Architecture



PoC System Configuration



Advantages of Blockchain for This Scenario

In this PoC, all the raw data was uploaded to the edge server, which processed the raw data to generate a new map update. The distributed ledger was applied where the map data was generated, in this case, at the edge cloud servers. Blockchain helped with the following goals:

1. **Data quality:** Blockchain helped to cross-validate the data, which was generated from different sources and stored in different locations. It provided a transparent, consistent, and immutable record of the data.
2. **Data privacy and security:** Blockchain helped ensure the privacy and security of the data by providing a secure and decentralized framework for data sharing. The data was stored on the blockchain in an encrypted form, and access to the data was controlled by each organization.
3. **Data ownership and control:** Blockchain was used to establish clear rules and guidelines for data ownership and control via a permissioned chain and smart contracts. These tools defined the rights and responsibilities of each party involved in the map generation process, including data providers, validators, and users.

Blockchain Frameworks: Why Use Hyperledger?

Hyperledger is an enterprise-grade, open-source distributed ledger framework launched by the Linux Foundation in December 2016. It's one of the most mature and popular open-source projects in the community with a lot of active users. Hyperledger Fabric and Hyperledger Indy are highly modular, decentralized ledger technology (DLT)

platforms. Both can address our technical and business requirements while accelerating the PoC development and implementation.

Edge Computing

The edge computing environment was developed based on Intel® Smart Edge Open. As open-source software, it has the advantage of being highly interoperable and adaptable for future uses.

Proof of Concept Results

This PoC showed that:

1. Map data can be securely shared among multiple organizations for cross-validation.
2. Blockchain can be successfully used in a distributed network for processing map update data.
3. Distributed authentication works and preserves privacy for the vehicles involved.

Next Steps

The integration with the Intel® Smart Edge Open software toolkit for building edge platforms is ongoing. Once it has been fully integrated, it will enable our PoC implementations to be deployable in different edge environments. The team will also be able to manage the system in these edge environments using the Smart Edge Open components.

The team is also looking at enhancing the multi-edge orchestration to enable this system to be deployable with different operators in multi-access or connectivity environments.