Secure and Tamper-Resilient Data Aggregation for Autonomous Vehicles and Smart Mobility[*]

Sananda Mitra Sumanta Bose Sourav Sen Gupta
Anupam Chattopadhyay Kwok-Yan Lam

School of Computer Science and Engineering,
Nanyang Technological University, Singapore

{sananda.mitra,sumanta001,sg.sourav,anupam,kwokyan.lam}@ntu.edu.sg

Abstract

The future of transportation is going to change forever with the advent of Autonomous Vehicles (AVs) and the Smart Mobility framework. With the industry leaders investing billions of dollars in research and development, the reality of having driverless cars seem to be nearer each day. Autonomy of a vehicle is currently recognized in a scale of zero (no autonomy) to five (full autonomy), as per SAE taxonomy. Progressively advancing driver assistance support is provided over the levels, and as of 2019, level 4 autonomous cars are already in the prototyping stage by the automotive giants. To achieve full autonomy, vehicles need to be manufactured as complex Internet-of-Things (IoT) enabled cyber-physical systems. However, the security and safety vulnerabilities of self-driving cars are quite unlike that of the conventional cyber-physical systems. In order for the security considerations of AVs to be modelled based on the complex IoT systems, this area of research must be advanced so that we understand how to address the specific security threats. Data aggregation plays a crucial role in the safety of an autonomous vehicle embedded within the smart mobility architecture, and supplies real-time information to the network. In this chapter, we focus on the security and tamper-resilience of data aggregation in AVs as a part of the smart mobility infrastructure, based on the backbone of a distributed ledger. A distributed ledger structure is an ideal candidate due to its intrinsic features of consensus-driven synchronization and maintenance of transactional information without any central authority or storage. A consortium blockchain network is observed to be the most suited distributed ledger instantiation as it can be mapped to the internal network of an AV with consensus entrusted on the pre-decided AV internal units. The core data aggregation platform is therefore designed and instantiated as a consortium blockchain following a detailed cyber-physical security analysis with reference to standard adversary models.

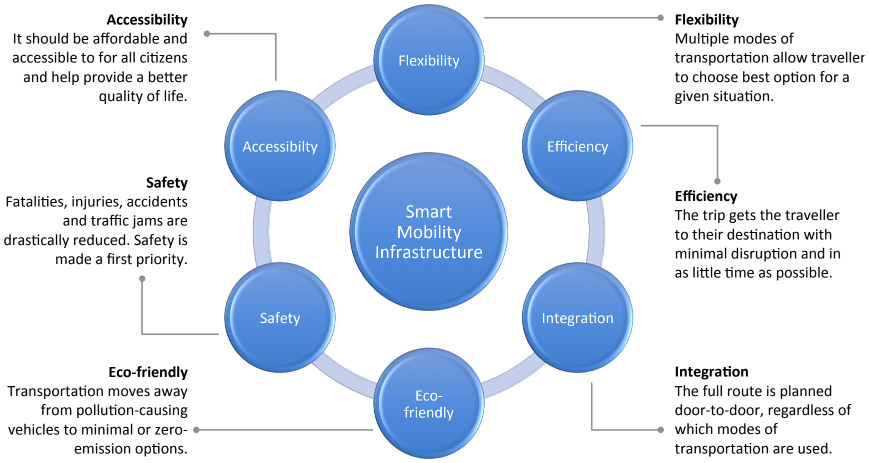
[*] The authors would like to acknowledge the support from SPIRIT, the centre for Smart Platform Infrastructure Research on Integrative Technology, Nanyang Technological University, and ERI@N, the Energy Research Institute, Nanyang Technological University.

1 Introduction

The concept of a *Smart City* goes above and beyond its technological backbone, as it needs to integrate social and political aspects as well. The six key pillars of Smart City, as identified by a 2015 Siemens AG report,[1] are Smart Living, Smart Mobility, Smart Society, Smart Economy, Smart Government and Smart Environment. Within these, Smart Mobility is a key component to achieve sustainable development of any city. In this connection, one may envision a Smart City as a complex system which employs a mesh of Internet-of-Things (IoT) enabled sensors and cyber-physical devices to acquire, aggregate and utilise information for efficient management of the city's assets and resources.

1.1 Smart Mobility

One of the key pillars of smart city, *Smart Mobility Infrastructure*, focusses on information acquisition from fixed assets, portable devices, and autonomous vehicles (AVs) to monitor and manage smart traffic and transportation systems. The idea of smart mobility goes beyond just alternative forms of transportation.[2] Smart mobility is built on the core principles of flexibility, efficiency, integration, eco-friendliness, safety and accessibility,[3] as illustrated in Figure 1.



Accessibility
It should be affordable and accessible to for all citizens and help provide a better quality of life.

Flexibility
Multiple modes of transportation allow traveller to choose best option for a given situation.

Safety
Fatalities, injuries, accidents and traffic jams are drastically reduced. Safety is made a first priority.

Efficiency
The trip gets the traveller to their destination with minimal disruption and in as little time as possible.

Eco-friendly
Transportation moves away from pollution-causing vehicles to minimal or zero-emission options.

Integration
The full route is planned door-to-door, regardless of which modes of transportation are used.

Figure 1: Key Principles of Smart Mobility Infrastructure.

[1] Seimens AG, *Smart Mobility – A tool to achieve sustainable cities*, `http://www.vt.bgu.tum.de/fileadmin/w00bnf/www/VKA/2014_15/150212_Smart_Mobility_v5_TUM.pdf`, 2015.

[2] Land Transport Authority, Government of Singapore, *Smart Mobility 2030*, `https://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion/intelligent-transport-systems/SmartMobility2030.html`, 2014.

[3] Frost and Sullivan, *Future of Mobility*, `https://ww2.frost.com/research/visionary-innovation/future-mobility`.

Globally, smart mobility infrastructure is being adopted in several leading cities that are paving the way for others to follow. Columbus (Ohio, USA), for example, is collecting traffic data to identify and address safety issues such as identifying collision hotspots and detecting potential signal issues. It is soon to become the first smart city in the United States of America. Another classic example is Singapore, where growing number of residents (over 5.6 million people) and vehicles (almost 1 million motor vehicles) in an island limited by land area has been the catalyst in the creation of an intelligent transport system to help the commuters enjoy a hassle-free travel.

The strategic planning of Singapore's Smart Mobility 2030 goal revolves around the next generation of transportation with focus on information, interaction, assistance and green mobility. The key strategies to achieve these goals, as outlined in the plan,[4] are: (*i*) to implement innovative and sustainable smart mobility solutions; (*ii*) to develop and adopt intelligent transport system standards; and (*iii*) to establish close partnerships and co-creation. Authors of this chapter are closely associated with the centre for Smart Platform Infrastructure Research on Integrative Technology (SPIRIT), NTU Singapore, and are first hand witnesses to the aforementioned smart mobility revolution and the pivotal role played by the evolution of autonomous vehicles.

1.2 Autonomous Vehicles

AVs can be considered as one of the most crucial elements in the smart mobility infrastructure. Introduction of driverless cars for private and public transport in smart cities shall require a secure, efficient, robust and scalable design for the transportation framework. Intelligent transportation system will necessitate AVs to interact and integrate information from a range of entities like intra-vehicular control units (vehicle-to-vehicle *aka* V2V), smart roadside units (vehicle-to-infrastructure *aka* V2I) and even smart devices with mobile roadside citizens (vehicle-to-pedestrian *aka* V2P).

Autonomy of vehicles in the context of a smart city is not realised in isolation. With the advent of cloud, fog and mist computing,[5] it is appropriate to consider an AV as a Cyber-Physical System (CPS) embedded within an *intelligent* grid of infrastructured and infrastructureless information agents. The autonomy of the AV unit may be considered as a three-phase learning mechanism:

Perception — The first phase is perception, which denotes the interaction of the AV with information agents for data accumulation. The agents may be within the vehicular system or in the overall Smart Mobility environment.

Decision — The second phase is decision, which the the process of drawing inference from the accumulated data, through artificial intelligence algorithms, often executed in real-time for control and cognitive resolution.

[4] Land Transport Authority, Government of Singapore, *Smart Mobility 2030*.

[5] Angelo Corsaro, "Cloudy, Foggy and Misty Internet of Things," in *7th ACM/SPEC on Intl. Conf. on Performance Engg.* (Delft, The Netherlands, 2016), 261–261.

Actuation — The third phase is actuation, whereby the implementation of cumulative cognitive decisions are undertaken, with adequate feedback and response, to ensure autonomous navigation and operation of the vehicle.

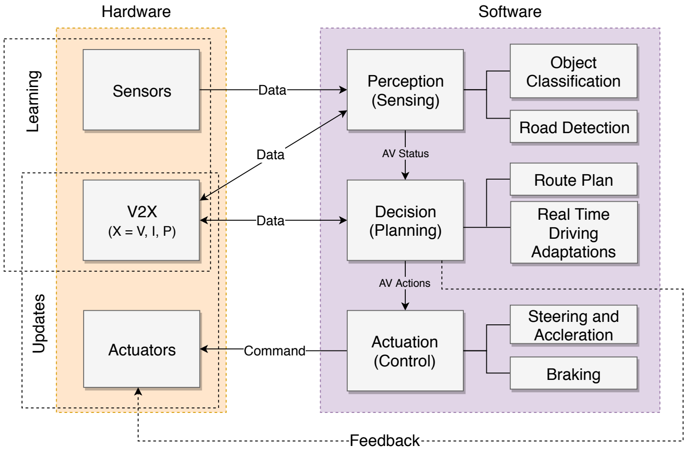


Figure 2: Data Flow Diagram of Autonomous Vehicles.

1.3 Security Concerns

In prevalent smart mobility platforms, real time data is integrated through the information and communication substructure. Ensuring security and privacy of the data flow is pivotal for safe and reliable transport. In a recent work[6] at University of Michigan, researchers have proposed a threat identification model to analyze the likelihood and severity of potential threats by accounting for the attacker's skill level and motivation, the vulnerable vehicle system components, the ways in which an attack could be achieved, and the repercussions, including for privacy, safety and financial loss. In another relevant work,[7] researchers have extensively studied the potential threats, the vulnerable components and eventual consequences. Similar studies[8] reveal that the threats posed to an AV not only compromises road safety,[9] but may also be detrimental to the entire

[6] Derrick Dominic et al., "Risk Assessment for Cooperative Automated Driving," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, Austria* (2016), 47–58.

[7] Jonathan Petit and Steven E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Trans. Intelligent Transportation Systems* 16, no. 2 (2015): 546–556.

[8] Marko Wolf, André Weimerskirch, and Christof Paar, "Security in automotive bus systems," in *Workshop on Embedded Security in Cars* (2004).

[9] Mario Gerla et al., "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on* (IEEE, 2014), 241–246.

smart mobility infrastructure.[10] Cybersecurity is still an overlooked area of research in AV technology, even though many threats and vulnerabilities exist, and more are likely to emerge as the technology progresses to higher levels of automated mobility. It is therefore important to analyse the likelihood and severity of potential cyberthreats to intra-AV and inter-AV networks.

Realisation of the security issues arising from data flow network within an AV is critical to the eventual understanding of higher-level security concerns in the smart mobility ecosystem. To that effect, we start by examining the data flow in autonomous vehicles as a part of the smart urban mobility architecture. In our previous work[11] we have explored a secure and tamper resilient framework based on Distributed Ledger Technology (DLT) for data aggregation in AVs for fixing the existing safety loopholes. In this chapter we show that a secure and tamper-resilient ledger can be a dependable source of information beyond the AV, for manufacturers, service providers and insurance companies. The smart mobility infrastructure can also monitor and harvest immutable and validated data from the ledger. Secure remote monitoring, over-the-air updates or diagnostics, dynamic evaluation of insurance value, etc., will be of major relevance to complete the overall picture of smart urban mobility.

Organisation. Section 2 lays the background of autonomous vehicles, in terms of operation, data flow and system architecture, followed by the current data aggregation mechanisms in the smart mobility infrastructure. Section 3 considers the overall data aggregation architecture, and explains the design considerations necessary to ensure the security requirements in a smart mobility infrastructure. Section 4 presents a reference instantiation to illustrate the end-to-end distributed ledger design for autonomous navigation in an AV, in the context of the IoT infrastructure of smart mobility. Section 5 concludes the chapter.

2 AVs and Smart Mobility

Over the past decade, the average commute time of urban citizens have increased considerably. Connected in-vehicle services like onboard infotainment and diagnostics are now major contributing factors for buying choices of vehicles, along with the ever-existing demand for seamless and hassle free commute. A promising solution for smart transportation are autonomous vehicles as they provide improved efficiency in traffic flow and road safety. As discussed earlier, the full potential of AVs can only be realised through a complete understanding of its various components, comprehensive knowledge of the internal data management network, interpretation of its dependency on the smart mobility framework, and a thorough risk assessment of the entire cyber-physical architecture.

[10] Mevlut Turker Garip et al., "Congestion attacks to autonomous cars using vehicular botnets," in *NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA* (2015).

[11] Sananda Mitra et al., "Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles," in *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)* (IEEE, 2018), 548–551.

2.1 Information Units

The data flow and aggregation in an AV, depends on the harmony of several *information units*, such as vehicular perception sensors,intra-vehicular control units and communication modules as shown in Figure 3.

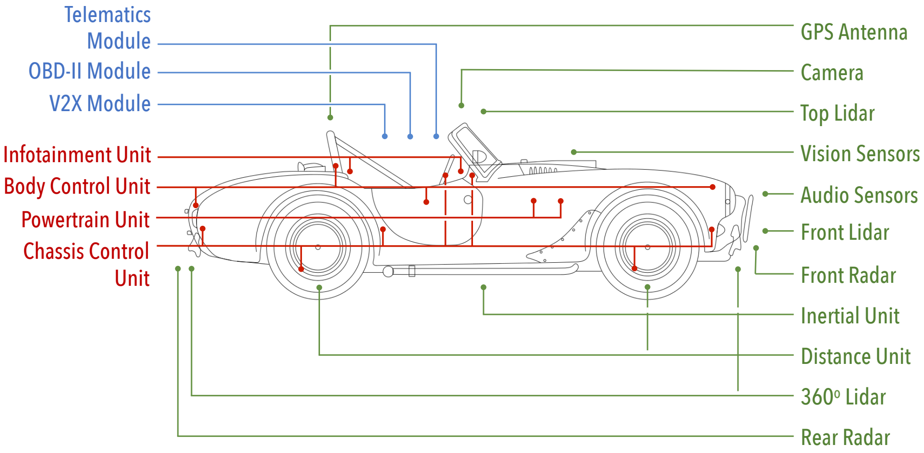


Figure 3: Information Units in typical AVs: ●— Intra-vehicular Control Units, ●— Perception Sensors, and ●— Peripheral Communication Modules.

The *Powertrain Unit* and the *Chassis Unit* are the two major control units overseeing engine and gears control, steering control, breaks, airbag opening etc. The *Body Unit* monitors central locking, lights, air conditioning, while the *Infotainment Unit* allows in-vehicle entertainment (radio, HDTV etc.) and information systems like GPS navigation. Communication via radio, and telecommunication services is supervised by telematics and V2X module.[12]The analysis of the collective information by the Advanced Driver Assistance Systems (ADAS) help in charting a safe and optimal route for the AV. ADAS also issues intermittent diagnostic warnings.

As discussed earlier the successful operation of AVs depend largely on the the ability to communicate and co-ordinate with the Vehicle-to-everything (V2X) framework.Vehicle to everything (V2X) data communication is a synergy of different IoT technologies like Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Vehicle to Pedestrian (V2P). V2V communication provide 360 degree awareness of speed change, range, direction of travel, braking, and potential hazards of other automobiles via wireless communication. Information generated from different vehicles can be aggregated before it is delivered to other vehicles. But V2V communication is not enough for taking adaptive cruise control decisions, as the range of V2V communication is up to 300 meters or about 10

[12] Gang-Neng Sung, Chun-Ying Juan, and Chua-Chin Wang, “Bus Guardian Design for automobile networking ECU nodes compliant with FlexRay standards,” in *IEEE Intl. Symposium on Consumer Electronics* (2008), 1–4.

seconds at highway speeds. To have information like road conditions and traffic flow outside the visual range of the car, the AVs are also expected to communicate with static roadside units. Reliable and low latency data communication is also required to ensure safety and issue security alerts to pedestrians or cyclists.

2.2 Stages of Data Flow

The complex data flow network in an AV is modelled in three functional stages — data generation (telematics and diagnostics), data acquisition (perception and communication), and data processing (decision and actuation), as follows.

Data Generation — Data generation in AVs is aided by a range of perception sensors such as LiDAR, RADAR, surround view front/rear cameras, inertial sensors etc. To enable complex driving assistance AVs requires multiple and redundant information sources which is a combination of information from perception sensors supported by V2X communication. Sensors collect surrounding data and provide them to the on-board Electronic Control Units (ECUs). Navigation of an AV require the connected ECUs inside the vehicle to generate a substantial amount of data, typically in the order of terabytes per hour.[13] The variety of data generated inside the components of an AV include diagnostic data, behavioural data for autonomous driving, reports on failures and crashes, and data for in-vehicle entertainment. On-board flash storage are no longer a viable option for storing such volume of data generated inside and communicated to it. The industry is actively looking into sustainable hybrid models for data storage, with full-stack integration of in-vehicle storage units to the cloud.

Data Acquisition — Acquisition is the process of fusing the data collected by the sensors with the help of standard in vehicle communication protocols. Communication between the control units is of paramount importance to navigation fidelity of an AV. The standard communication protocols for safety critical (powertrain and chassis) and non-critical operations are Controller Area Network (CAN), CAN Flexible Data-Rate (CAN FD), FlexRay, Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST) and Ethernet.[14] CAN is a multi-master message broadcast bus system that supports serial communication between different ECUs. While CAN is mostly used for low speed in-vehicle communication (1 Mbps), CAN FD and FlexRay are suitable for real time safety critical operations as they are capable of high speed communication, robust error detection and fault tolerance. LIN is a low-cost sub-bus for CAN and is mostly used for non-mainstream body electronics, where speed, error handling and fault tolerance are not of utmost importance. MOST and Ethernet are high bandwidth protocols used for infotainment

[13] Accenture, *Autonomous Vehicles: The Race is On*, `https://www.accenture.com/us-en/insights/communications-media/autonomous-vehicles-data-challenges`, 2018.

[14] Wolf, Weimerskirch, and Paar, "Security in automotive bus systems."

and telematics. In addition, there are five OBD-II signalling protocols, including classical CAN, in any AV. Data fusion in the conventional sense requires interconnection between the internal communication protocols as well as external V2X ecosystem like IEEE 802.11p, Wi-Fi, Bluetooth, 3G/LTE, etc. for data exchange.[15]

Data Processing — The AI-driven computing module is responsible for processing the intra-AV data, and analysing the information accumulated from the smart mobility framework to model the environment around the vehicle. It takes informed decisions regarding navigation, maintenance, route determination, parking etc., and is the crux of automation that creates a safe and secure perception-decision-actuation loop based on data.

3 Data Aggregation Architecture

In order to design a robust data aggregation framework for smart mobility infrastructure, we need to consider the practical security challenges. The security and privacy concerns regarding the smart mobility data will eventually guide us to formulate the design principles for data aggregation and analysis.

3.1 Security Challenges

In a smart mobility infrastructure, V2X technology allows vehicles to communicate via wireless exchange to have a co-ordinated sense of the environment and to take preemptive actions for seamless navigation. Use of wireless channels for communication exposes the V2X system to various threats and attacks. To understand the complete security scenario, we must identify the actors involved in V2X communication. The main actors of such a network are as follows,[16] as depicted in Figures 4 and 5, the real-life V2V, V2I and V2P network models.

Traffic Centres (TC) — Responsible for identity verification, certificate management, remote monitoring and control of entities and conditions.

Road Side Units (RSU) — Placed within infrastructural components or standalone; responsible for managing V2X communication with vehicles.

On Board Units (OBU) — Sensors, cyber-physical devices, ECUs or onboard computing platforms present within an autonomous vehicle.

Smart Devices — Devices with pedestrians or other AVs, able to communicate with the vehicles to ensure pedestrian safety or for diagnostics.

[15] Paulo H. L. Rettore et al., “Towards intra-vehicular sensor data fusion,” in *19th IEEE Intl. Conf. on Intelligent Transportation Systems, Brazil* (2016), 126.

[16] Sheng Zhong et al., “Connecting Things to Things in Physical-World: Security and Privacy Issues in Vehicular Ad-hoc Networks,” in *Security and Privacy for Next-Generation Wireless Networks* (Springer International Publishing, 2019), 101–134.

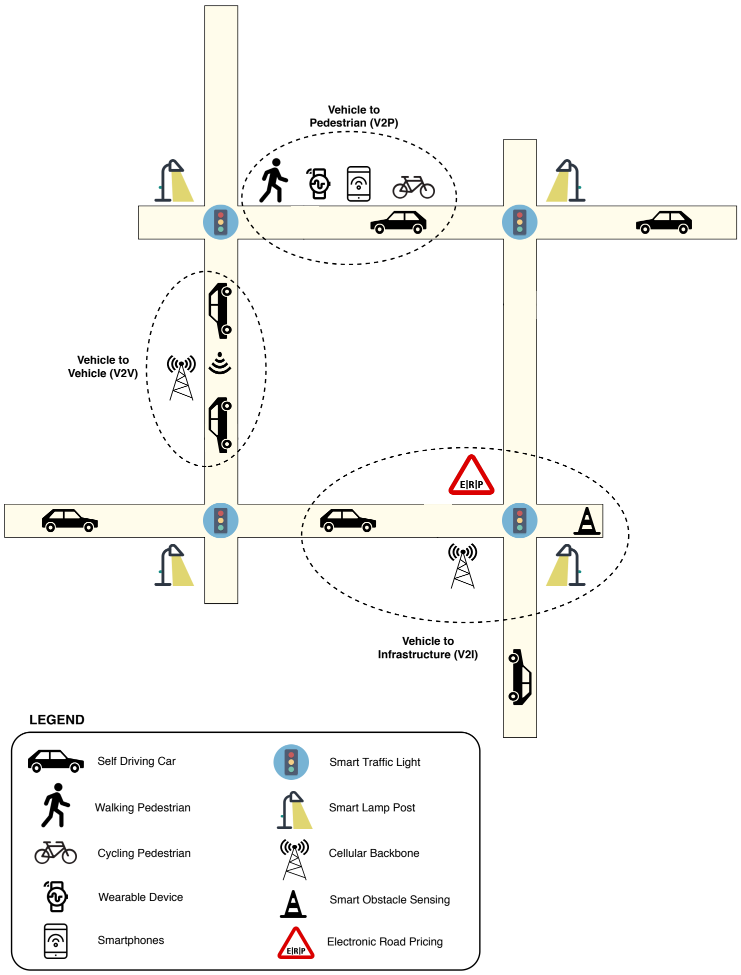
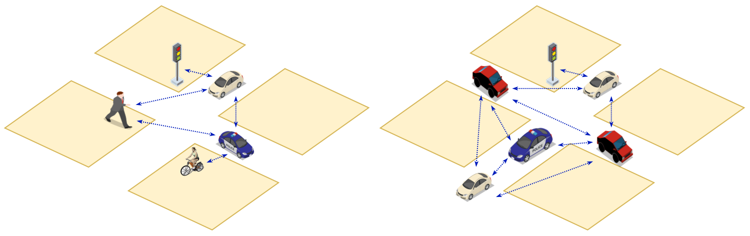


Figure 4: The V2X communication infrastructure — Vehicle-to-vehicle (V2V), Vehicle-to-infrastructure (V2I), and Vehicle-to-pedestrian (V2P) networks.



(a) Hybrid V2X communication. (b) High-speed V2X communication.

Figure 5: Real-time communication substructure for autonomous navigation.

The desired security principles for V2X communication between the above actors are — (i) proper identification and authentication of the actors before communication, (ii) verification of data integrity generally by redundancy, (iii) confidentiality of communicated and stored data, (iv) authorised provisioning of services, (v) availability of information or over-the-air updates, (vi) privacy preserved user data communication, and (vii) accountability of information source.

Even though the security requirements for V2X communication is of primary importance in smart mobility, we need to consider three reference domains in the smart mobility architecture — (a) the V2X communication network, (b) the AV in-vehicle data network, and (c) the service information platform, like diagnostic services, insurance, certification authority, etc. These three domains should be considered separately as each one presents unique characteristics in terms of overall security of the smart mobility infrastructure.[17]

Security threats based on the reference domains (V2X network, in-vehicle network, and service network) include, but are not always limited to — malicious use of a vehicle providing misleading information to other vehicles, malicious entity posing as a Roadside Unit providing fake information to passing vehicles, generating high volume of fake messages or replay messages for denial of service within the V2X domain, posting malicious information to the in vehicle data aggregation system using smart devices, attacking adjacent road side units and vehicles in a specific area so that they cannot communicate with the V2X framework, and privacy violation by analysis of network traffic and obtaining vehicle specific data. Most of the research work in this area till date has been focused on simply encrypting the data, on both the vehicular system and the wireless channels, without evaluating the complete space of solutions.

3.2 Attack Surfaces

Ironically, the capabilities provided to an AV by the V2X platform can make the system fall prey to more vulnerabilities. Increased complexity of ADAS systems exposes more attack surfaces in the smart mobility architecture. *Autonomous Cruise Control* presents quite a challenging scenario for security management with increasing levels of autonomy. To ensure performance efficiency and safety, secure communication between vehicle control units is extremely important. Miller and Valasek[18] showed the possibility of malicious attacks on AVs via mobile telephone network. They hacked a Chrysler Jeep by injecting messages into the CAN bus through the V850 controller designed to be able to communicate with it and took control over its engine unit and disabled its brakes entirely. Similar attacks furthermore showed that even though an adversary can attack an AV remotely there is no remote means to fix the attacks.[19]

[17] Samuel Woo, Hyo Jin Jo, and Dong Hoon Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems* 16, no. 2 (2015): 993–1006.

[18] Charlie Miller and Chris Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA* 2015 (2015): 91.

[19] Maurice Schellekens, "Car hacking: Navigating the regulatory landscape," *Computer Law & Security Review* 32, no. 2 (2016): 307–315.

The security threats creep into the smart mobility framework more so because real time safety is the essence in these systems. For example if the Chassis Control Unit issues a braking signal there is no double guessing. In subsequent efforts made by automotive companies like Tesla and Chrysler, security updates were send to manufacturers via remote patching or using USB sticks carrying the updates. Both these methods have severe cybersecurity flaws. If the manufacturers can communicate with the vehicle processor and post remote updates, so can a hacker, provided a proper entry point is exploited. Plugging USB keys for updates can have dire consequences as it would very hard to verify whether the device can be trusted or if it is malware free. Researchers have shown that spoofing of GPS systems and sensor manipulation are significant threats.[20] Table 1 shows the potential attacks, targeted assets security issues and possible countermeasures of the mobility domains.

Safety of passengers in an AV heavily depend on the security solutions conceived for the ubiquitous network encompassing the vehicles as well as intra-vehicular network. There is not enough evidence in the literature to provide us with definitive prerequisites and guidelines for developing an appropriate data management framework for autonomous navigation that can rule out all cybersecurity threats. In certain scenarios, a distributed ledger based data aggregation seems to resolve a number of existing issues pertaining to security and privacy, and brings forth the inherent benefits of consensus-driven decentralisation.[21]

3.3 Design Considerations

In light of the security challenges faced by AVs, as discussed above, the current need of the hour is a secure and tamper-resilient data aggregation mechanism within a set of participating entities with a shared state. This is the forte of Distributed Ledger Technology (DLT), such as blockchain. There are manyfold advantages of DLT, particularly with respect to state-of-the-art data privacy and real-time automation through smart-contracts.[22]

Distributed Ledger Technology facilitates a networked database that is consensually shared and synchronised across multiple parties that may be hosted in diverse logical or physical geographies. It allows transactions to have publicly verifiable 'witnesses', thereby making the proof-of-data tamper-resilient. The participant hosting each node of the network can access and own identical copies of the shared records. Modifications or appends made to the ledger are reflected and copied to all participants through a consensus mechanism.[23] Blockchain is a specific kind of distributed ledger technology that guarantees data provenance, data validity and immutability across the network.

[20] Saeed Asadi Bagloee et al., "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies," *Journal of Modern Transportation* 24, no. 4 (2016): 284–303.

[21] Mitra et al., "Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles."

[22] Vitalik Buterin, *On Public and Private Blockchains*, Ethereum Blog, 2015.

[23] Christian Cachin and Marko Vukolic, *Blockchain Consensus Protocols in the Wild*, 2017, eprint: `arXiv:1707.01873v2`.

Table 1: Security Issues and Countermeasures in Smart Mobility Infrastructure.

Attack	**Access**	**Target**	**Issue**	**Countermeasure**
Packet Injection (in CAN Bus)	Remote	AV ECUs, ADAS, OBD II	Integrity	Identification, Authentication, Blockchain
Eavesdropping	Remote, Proximity	AV Sensors, V2X Platform	Confidentiality, Privacy	In-vehicle Data Encryption
Firmware Tampering	Remote, Physical	OBD II Port, AV Processor	Integrity, Availability	Authentication, In-vehicle Data Encryption, Root-of-Trust, Blockchain
Side-Channel Attack	Remote	AV Processor, ADAS, OBD II	Confidentiality, Privacy	Authentication, Access Control
Identity Spoofing	Remote, Proximity	AV Sensors, GPS System	Integrity	Packet Filtering, Authentication
Packet Sniffing	Remote	AV Telematics, V2X Platform	Confidentiality, Privacy	Authentication, Intrusion Detection, Encrypted Comm.
Routing and Map Poisoning	Remote	AV Telematics, V2X Platform	Integrity, Availability	Authentication, Intrusion Detection
Distributed DoS and Blackhole	Remote, Proximity	AV Actuators, ADAS, Network	Availability	Identification, Authentication, Intrusion Detection
Data Remanence	Remote, Physical	Flash Storage in AV, OBD II	Confidentiality, Privacy	Deep Formatting, Access Control
Data Tampering	Remote, Proximity, Physical	Flash Storage, ECUs, OBD II, V2X Platform	Integrity	Authentication, Encrypted Data Storage, Blockchain
Fault Injection (in CAN bus and FlexRay)	Remote, Proximity, Physical	ADAS and Computing Devices	Integrity	Authentication, Access Control, Blockchain
BotNet	Proximity	V2X Platform	Integrity, Availability	Trust, Reputation, Segregated Computing

Design Principle — We observe that the internal network of an AV can be envisioned as a consortium blockchain with consensus depending on the predecided peers, as explored in our previous work.[24] Distributed ledgers offer a shared state of transaction or contract records that have been approved through a consensus mechanism executed in a consortium of participating entities. It eliminates the need of a central authority to keep a check on manipulation, and the secure tamper-resilient distributed ledger becomes a dependable source of information for manufacturers, service providers and insurance companies.

The smart mobility infrastructure can also monitor and harvest immutable and validated data from the ledger. Remote monitoring of AVs for safety, over-the-air updates or diagnostics, and dynamic evaluation of insurance value, will be of major relevance to complete the overall picture of smart urban mobility. Parties monitoring and retrieving data from AVs can also be the peers in a consortium blockchain to share the data. Channel design of such consortium structures must ensure selective involvement of peers in the sharing of data and remote administration, as well as guarantee privacy of sensitive data.

Safety-critical operations in an AV require real time decision making, while data aggregation through blockchain can be a robust but computationally heavy operation. If it is required to incorporate the data aggregation framework in real time decision control loops in an AV, the solution must use extremely high throughput DLT design, supported by a low-latency consensus mechanism.

Smart Contracts — Computer programs executed in a blockchain network, containing a set of rules under which the participating entities agree to interact with each other, are called smart contracts. They enforce automated agreement triggered under certain circumstances. In the context of an AV, smart contracts can formalise the relationships between its core components, data modules and data flow channels. The transaction rules (agreement) of the smart contract define the conditions – rights and obligations – to which the multiple participating entities of the protocol consent. This can be predefined, and the agreement may be attained by simple opt-in actions. In case of autonomous navigation, as illustrated in Figure 7, the smart contract ruleset can be formalised with the rights and obligations pre-established. The contract may then be automatically executed by the network of the concerned data modules – infotainment module, chassis control module, telematics module and V2X module.

The smart contracts executed in an AV can bring tremendous cost savings, as they are capable of tracking performance in real time. Controlling and compliance can happen on the fly. Smart contracts need information oracles, which feed the contract with external information for its functionality. Key virtues of a well deployed smart contract are being *self-verifying*, *self-executing* and *tamper-resilient*. The deployed AV network smart contracts can turn deterministic legal obligations into automated processes, guarantee a greater degree of data security and privacy, reduce reliance on trusted intermediaries, lower data aggregation costs, and automate real-time processes.

[24] Mitra et al., "Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles."

4 Reference Instantiation

In this section, we design and instantiate the internal network of an AV, as well as the smart mobility infrastructure, as a consortium blockchain with consensus amongst the major actors (peers and modules) of the cyber-physical network.

4.1 Design of Blockchain

Based on network structure, identity and trust among the peers blockchain network have been classified into three categories, namely public, private and consortium.[25] While Ethereum[26] promoted blockchain from a ledger of records to a decentralized trusted operating system equipped with smart contracts, Hyperledger[27] and Corda[28] propelled it into the arena of consensus-driven enterprise networks. This is where an automated blockchain framework interfaces with the AV ecosystem in the context of data aggregation and automation.

The information on the blockchain is securely and accurately stored using cryptographic primitives and can be accessed using cryptographic keys and digital signatures. Once the information is logged (stored) in the network, it acts as an immutable database, governed by the network protocols. While centralised ledgers could be prone to cyber-attack, it is inherently harder to attack distributed ledgers owing to the presence of distributed copies among network participants that needs to be attacked individually and simultaneously for an attack to be successful. Further, these records are made resistant to malicious changes by a single party not meeting the consensus criteria. The distributed ledger contains a verifiable and tamper-resilient proof of every transaction in the network, and ensures three key data properties.

> *Provenance of Data* — Ensures a verifiable source of origin for all records and transactions in the network, thus eliminating any conflict by design.
>
> *Validity of Data* — Facilitates a distributed verification mechanism of all records and transactions in the network, adhering to some pre-defined robust multi-party consensus mechanism across a decentralised network.
>
> *Immutability of Data* — Guarantees the secure storage of all records or transactions in the network, with tamper-proof cryptographic primitives (hash functions) that are resistant to malicious changes by a single party.

We observe that data aggregation network in an AV resembles a consortium blockchain network, which operates under the federation of multiple groups of entities, with the consensus dependent on a pre-decided subset of participants, as in Figure 6, the IoT landscape of autonomous vehicles and smart mobility.

[25] Buterin, *On Public and Private Blockchains.*

[26] Fabian Vogelsteller, Vitalik Buterin, et al., *Ethereum Whitepaper*, `https://github.com/ethereum/wiki/wiki/White-Paper`, 2017.

[27] The Linux Foundation, *Hyperledger*, `https://www.hyperledger.org/projects/fabric`, 2016.

[28] Mike Hearn, *Corda: A distributed ledger*, `https://docs.corda.net/head/_static/corda-technical-whitepaper.pdf`, 2015.

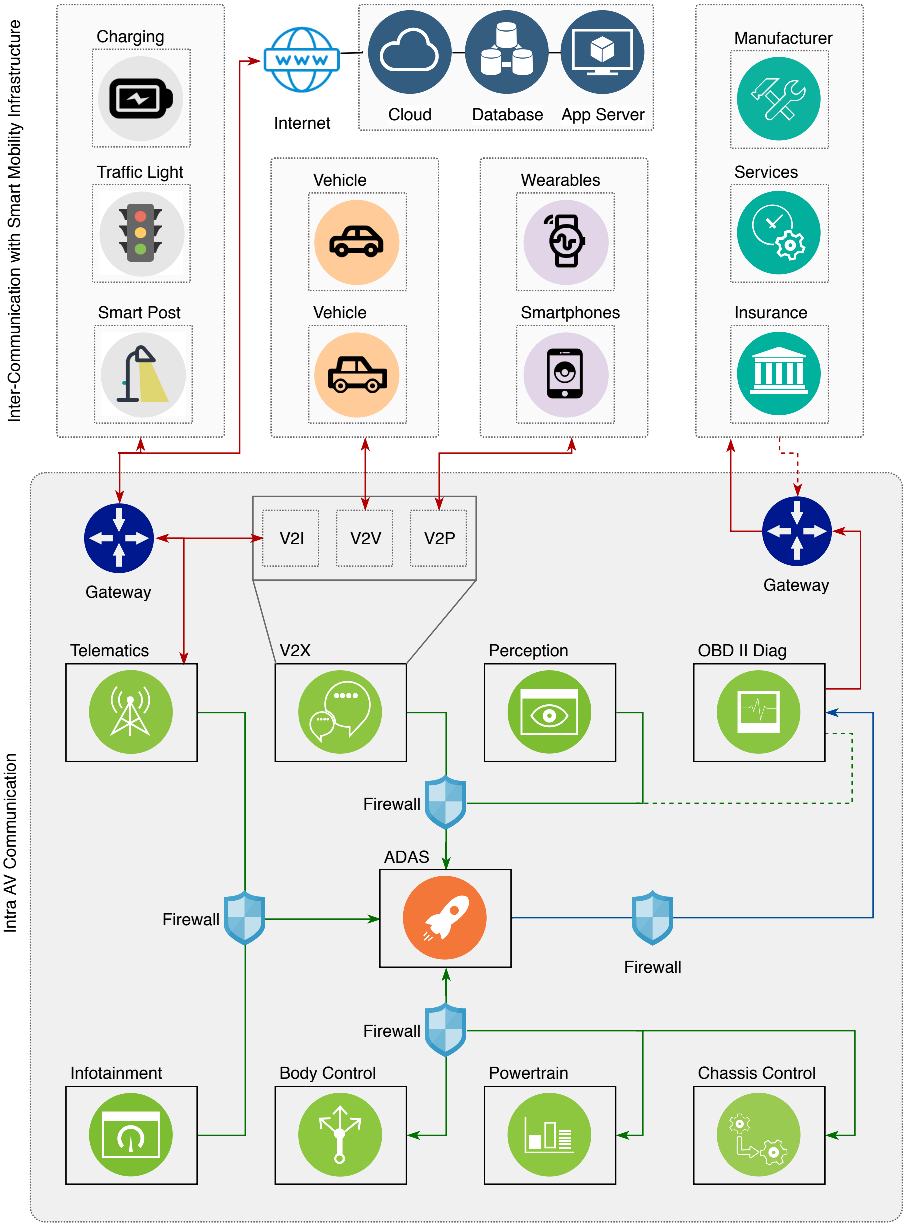


Figure 6: The IoT Landscape of Autonomous Vehicles and Smart Mobility.

4.2 Data Aggregation Framework

In Figure 6, we present a conceptual model of the complex IoT interconnection and data flow network within and around an AV, with its core components. The intra-AV data communication consists of the three step data aggregation, and communication to the smart mobility infrastructure. The smart mobility data from different V2X IoT platforms are aggregated using vehicle as a resource.[29] The information from each mobility substructure is communicated to the cloud for storage, analysis and remote monitoring. In this chapter, we design our smart mobility blockchain framework based on this reference architecture.

Autonomous Navigation — We first discuss the operational layout of the autonomous navigation data flow, based on a consortium blockchain proposed in our previous work.[30] Figure 7 shows Components, Modules and Channels for the model, where the *Autonomous Cruise Control* is divided into two logical units — the *Perception–Decision* unit and the *Decision–Actuation* unit.

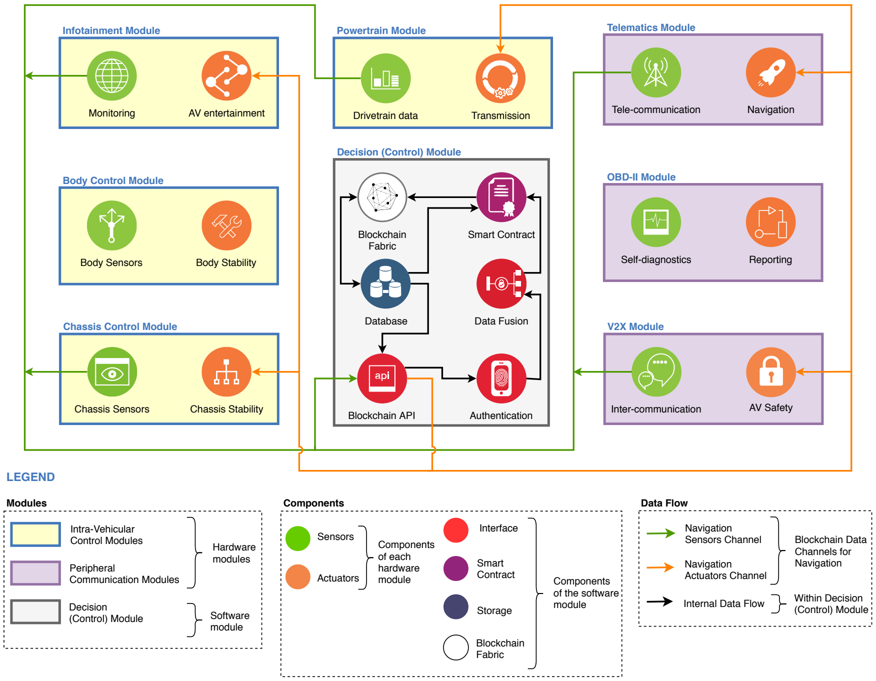


Figure 7: Components, Modules and Data Flow Channels for *Autonomous Navigation* with an underlying Blockchain framework for Data Aggregation.

[29] Sherin Abdelhamid, Hossam Hassanein, and Glen Takahara, "Vehicle as a resource (VaaR)," *IEEE Network* 29, no. 1 (2015): 12–17.

[30] Mitra et al., "Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles."

The in-vehicle modules namely powertrain, chassis, telematics, infotainment, V2X form a consortium, and contribute peers to create the data-flow channels. Two data flow channels, *navigation sensor channel* and *navigation actuation channel*, control the navigation events and record them in a shared ledger. The navigation sensor channel comprises of sensors and peripheral communication ports of each module, and the actuation units and ECUs are contributed to the navigation actuation channel. Authenticated sensor data are recorded in the form of smart contracts through the central Decision (Control) module. The mutually authenticated data from the peers will be used by ADAS to take a consensus-backed decision. The actuation units and ECUs receive the decision via navigation actuation channel. Overall security and privacy of the system is ensured by source attestation and recipient attribution using smart contracts.

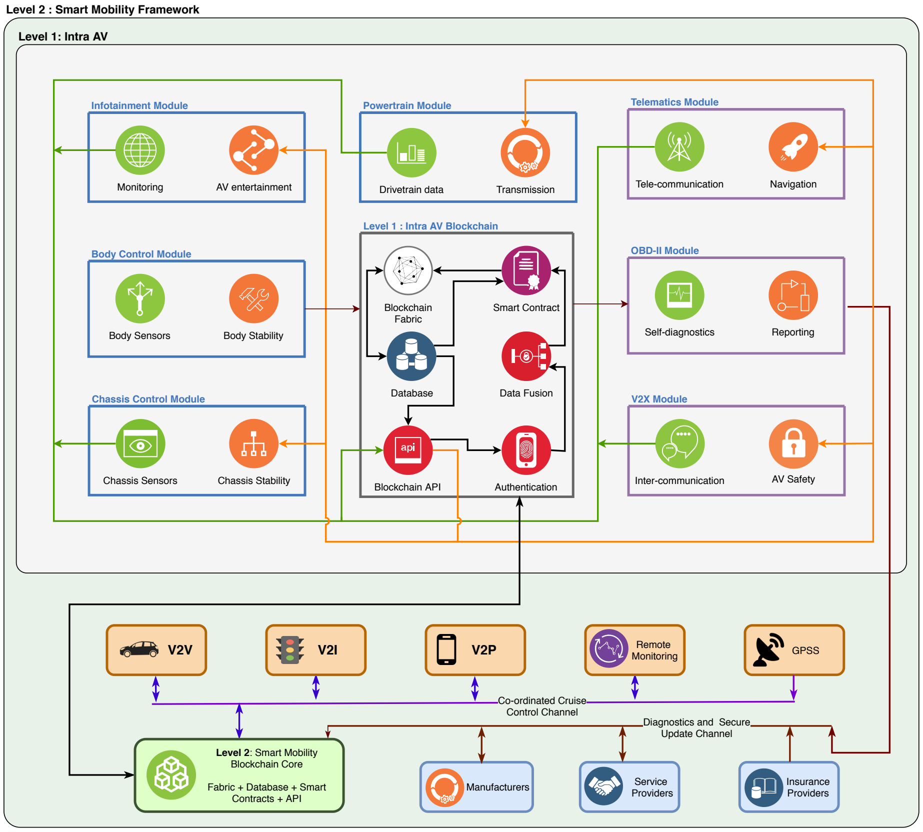


Figure 8: Consortium Blockchain Architecture for Smart Mobility.

Smart Mobility — Beyond the scope of our previous work, we extend this framework in this chapter to assimilate the complete smart mobility landscape, with peers and data channels pertinent to the smart mobility IoT landscape.

Figure 8 refers to the consortium blockchain architecture for smart mobility. The consortium blockchain will allow participants to access the distributed ledger and smart contract services only as a part of segregated channels. Other than the parties participating in the consortium network authorized Government agencies may have access to the root hash and prerogative to probe and verify the blockchain status. Similar to the previous work the consensus within the smart mobility blockchain will depend on the subgroup of entities forming the individual channels. The mobility framework is at first logically sub-divided into two functional segments pertaining to real time navigation control and diagnostics or other services which may not be essentially real time. For real time navigation control V2V, V2I, V2P, authorized remote monitoring agencies and geolocation satellite will contribute peers and will have private communications within the scope of co-ordinated cruise control channel. All transactions relating to cruise control will be performed within the cruise control channel. Similarly manufacturers, diagnostic service providers and insurance agencies will contribute peers to the diagnostics and secure update channel. The level 1 blockchain can incorporate copies of ledger updated and maintained by the level 2 blockchain. The hierarchical structure instead of a monolithic one is suggested to counter storage inefficiency and on chain slowness.

4.3 Security and Scalability

In certain scenarios, a blockchain based data aggregation resolves a number of existing issues[31] pertaining to security and privacy in an AV.[32] As additional security measure, a trusted execution environment based on modern Intel[33] or ARM[34] processors may also be provided at the Decision (Control) Module for secure execution of the core data fusion. With the trusted execution environment, the authenticated data fusion will provide consistency and accountability guarantees during secure processing of data for training of the on-board AI core.

However, safety critical operations in an AV demands real-time response which makes the response time a crucial factor. Blockchain based data aggregation being inherently computationally heavy operation may increase the waiting time for responses. Using blockchain data aggregation within a real-time decision control loop in an AV will require an extremely high throughput DLT design, supported by a low-latency consensus mechanism like pBFT.[35] One may also consider a modular design of the consortium network to allow for a highly efficient consensus based on sharding.[36]

[31] Wolf, Weimerskirch, and Paar, "Security in automotive bus systems."

[32] Simon Parkinson et al., "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. on Intelligent Transportation Systems* 18, no. 11 (2017): 2898.

[33] Intel Corporation, *Intel Trusted Execution Technology*, https://www.intel.com/content/www/us/en/architecture-and-technology/trusted-infrastructure-overview.html.

[34] ARM Limited, *ARM Security Technology – Building a Secure System using TrustZone Technology*, https://www.arm.com/products/security-on-arm/trustzone.

[35] Miguel Castro and Barbara Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.* 20, no. 4 (2002): 398–461.

[36] Eleftherios Kokoris-Kogias et al., "OmniLedger: A Secure, Scale-Out, Decentralized

The solution to scalability in a traditional database system is to increase computational power (i.e. add more servers) to handle the added transactions. In our example of a decentralised AV blockchain network, however, every data aggregation instance needs to be processed and validated by every node. Thus to get faster, we need to add more computational power to every node in the network. In permission-less (public) blockchains, we have little or no control over the public nodes in the network. Therefore, there is a trade-off between low transaction throughput and high degree of centralisation in most permission-less blockchain with decentralised consensus protocols. However, for permissioned (private) blockchain networks like our AV blockchain, we have more control over the network nodes, and hence over the scalability. With the growing size of a network, the computational power, storage and bandwidth requirements of the participating nodes increases. This may lead to the risk of centralisation.

In order to scale the AV blockchain protocol, we must have a mechanism to limit the number of participating nodes necessary to validate each transaction, while still ensuring the AV network's trust on the validity of each transaction. In this context, the following three requirements are imperative.

(a) Since every node doesn't have the responsibility to validate every transaction, they must have a game-theoretic trust mechanism to ensure that transactions not validated by them have been securely validated by others.

(b) There must be some way to guarantee the availability of transaction data. In other words, even for a transaction valid from the perspective of a node that has not directly validated it, unavailability of that transaction data (due to malicious attack, node power loss, etc.) would lead to a deadlock, and no other node can validate or create new transactions.

(c) In order to achieve scalability, different nodes must have the capability of processing transactions in parallel. As blockchain state transitioning also has several non-parallelizable components, there are certain restrictions on transitioning blockchain state, balancing scalability and parallelizability.

Some possible approaches of scaling the AV blockchain protocol are as follows.

Off-chain state channels — State channels allow interactions that were normally meant to occur within the blockchain to instead occur off the main chain. This is done in a cryptographically secure way without increasing the risk of any participant, while providing significant improvements in cost and speed. In future, state channels could be a critical part of scaling the AV blockchain to support higher levels of use, as recent reports have shown.[37] One option to create a state channel solution for AV data aggregation is as follows.

1. Part of the AV blockchain would be locked using multi-sig (or a smart-contract), which can only be updated if a specific set of participants agree.

Ledger via Sharding," in *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA* (2018), 583–598.

[37] Andrew Miller et al., "Sprites: Payment Channels that Go Faster than Lightning," *CoRR* abs/1702.05812 (2017), arXiv: 1702.05812.

2. The participants would make updates amongst themselves by constructing and signing transactions privately, without posting them on main chain.
3. At some later point, participants would submit the state back to the AV blockchain, which would close the state channel and unlock the state again.

Steps 1 and 3 (as above) involve blockchain operations which are published to the network and have to wait for peer validation However, Step 2 does not involve the main chain at all. It can contain an unlimited number of updates and can remain open indefinitely. In this sense, the AV blockchain can be used purely as a settlement layer to process the data aggregation instances, which helps lifts the burden from the underlying blockchain network. Not only can the transactional capacity be increased with state channels, but they can also provide two other crucial benefits — increased speed and lower overhead.

Plasma network — Plasma is a recently introduced technology and is a promising solution for scaling blockchain computation.[38] It can be visualised as a series of contracts running on top of a root blockchain. The validity of the state is enforced by the root blockchain in the Plasma chains using 'fraud proofs', which is a mechanism by which nodes can determine if a block is invalid. To implement this, the AV blockchain must be structured in a tree hierarchy, where each branch must be treated as a blockchain that has its own blockchain history and computations that are map-reducable. The child chains can be called 'Plasma blockchains', each of which are a chain within the main AV blockchain. The Plasma blockchain does not disclose the contents of the blockchain on the root chain. Instead, only the block header hashes are submitted on the root chain, which is enough to determine validity of the block. If there is proof of fraud submitted on the root chain, then the block is rolled back and the block creator is penalised. As a result, the root blockchain would process only a tiny amount of commitments from child blockchains, which in turn decreases the amount of data passed onto the root blockchain and allows for a much larger number of computations. In addition, data is only propagated to those who wish to validate a particular state. This makes the validation process for data aggregation instances in AVs more scalable by eliminating the need for every node to watch every chain. Instead, they only watch the ones they are impacted by in order to enforce correct behaviour and penalise fraud. Fraud proofs allows any node to enforce invalid blocks and ensure that all state transitions are validated. Additionally, if there is an attack on a particular chain, participants can rapidly and cheaply do a mass-exit from the corrupt child chain.

Off-chain computations — Such computations can be enabler in scaling transactions in blockchain networks (like TrueBit for smart contracts[39]). Essentially, just like state channels, this approach would use a layer outside the

[38] Joseph Poon and Vitalik Buterin, *Plasma: Scalable Autonomous Smart Contracts*, `http://plasma.io/plasma.pdf`, 2017.

[39] Jason Teutsch and Christian Reitwießner, *A scalable verification solution for blockchains*, `https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf`, 2017.

blockchain to do the heavy lifting. It is a system that verifiably executes computations off-chain that would be otherwise computationally expensive to execute on-chain. It can be implemented for the AV blockchain as follows.

1. Instead of every node participating, specific participants in the network (Solvers) perform the computations made by data aggregation smart contracts and submit the transaction log, along with a virtual deposit. If the log is correct, then the Solver is rewarded and its deposit is returned. If the Solver cheats, its deposit is forfeited and any dispute is resolved on the AV blockchain using the 'Verification Game'. The V2X, V2I, V2P entities in the smart mobility blockchain architecture may act as the Solvers.

2. Verification Game — A pre-defined set of participants in the network (Verifiers) check the Solvers' work off the chain. The solution is accepted by the system if no error is reported by any Verifier. If a Verifier does dispute the correctness of the Solver's solution, the game proceeds in a series of rounds to settle the dispute on the blockchain, where 'Judges' in the network with limited computational power adjudicate all disputes. The system is built to ensure that in a modest round of interactions the Judges can settle the dispute with a relatively small amount of work compared to that required for performing the actual task off the chain. infrastructural entities may act as Verifiers, while the Government may act as Judge.

3. At the end of this game, if the Solver was in fact cheating, it will be discovered and penalised. If not, then the challenging Verifier will pay for the resources consumed by the false alarm, thus balancing the system.

Overall, the protocol allows any information module (node) in the AV to initiate a data aggregation instance, and any other module (node) to receive a reward for completing it, while the system's incentive structure guarantees the correctness of the data aggregation transaction log. And by moving the computations and verification process off the blockchain into a separate protocol, it can scale to large numbers of transactions per unit time without significant constraints.

Sharding — This is similar to database sharding in traditional software systems. A shard is a horizontal partition of the data in a database, where each shard is stored on a separate server instance. This helps spread the load across different servers. Similarly, with blockchain sharding, the overall state of the blockchain is separated into different shards, and each part of the state would be stored by different nodes in the network.[40] Transactions that occur on the network are directed to different nodes depending on which shards they affect. Each shard only processes a small part of the state and does so in parallel. In order to communicate between shards, there needs to be some message-passing mechanism. To implement sharding in our AV blockchain, it would necessitate

[40] Loi Luu et al., "A Secure Sharding Protocol For Open Blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016* (2016), 17–30.

the creation of a network where every node only processes a small portion of all transactions (within its own module), while still maintaining high security.

To test the applicability of each of the aforesaid scalability solutions in case of smart mobility, is beyond the scope of this chapter. This, however, may prove to be an exciting future direction of research in smart mobility infrastructure.

5 Conclusion

In this chapter, we highlight how the emergence of autonomous vehicles and the smart mobility infrastructure will revolutionise the concept of Smart City, by promoting a more flexible, efficient, integrated, safe and accessible adoption of future transportation. For this to happen, Level 4 AVs as of 2019, and level 5 AVs of the future, will have to be conceptualised and manufactured as complex Internet-of-Things enabled Cyber-physical Systems embedded within an intelligent grid of static and dynamic information agents.

We reason that the security and safety risks for the autonomy of such self-driving cars outweigh those of conventional cyber-physical systems. We have discussed in detail about several potential attacks, targeted assets security issues and possible countermeasures of the mobility domains. The most crucial undertaking in ensuring autonomous navigation safety is fortifying the 'data aggregation' mechanism both within and outside an AV integrated into a smart mobility framework. We ensure the security and tamper-resilience during data aggregation as a two level distributed ledger structure instantiated as consortium blockchains. The Level 1 blockchain corresponds to the within-AV data aggregation, instantiated within each vehicle, responsible for the secure and tamper-resilient data aggregation initiated from the local information units such as infotainment, body control, chassis control, powertrain, telematics, OBD-II, and V2X modules. And the Level 2 blockchain is necessary to support the smart mobility infrastructure connecting multiple AVs, pedestrians using wearable devices and smart infrastructural elements such as traffic light, lamp post, charging units, etc. This second level global blockchain network can also be a facilitator for secure and tamper-resilient data aggregation encompassing on-road vehicles, roadside infrastructure, electronic road pricing system, parking facilities, electric charging stations, diagnostic networks, AV manufacturers, insurance agencies, service centers etc. As an extension to this work, we plan the practical implementation of our model on an actual AV platform.

References

Abdelhamid, Sherin, Hossam Hassanein, and Glen Takahara. "Vehicle as a resource (VaaR)." *IEEE Network* 29, no. 1 (2015): 12–17.

Accenture. *Autonomous Vehicles: The Race is On.* `https://www.accenture.com/us-en/insights/communications-media/autonomous-vehicles-data-challenges`, 2018.

ARM Limited. *ARM Security Technology – Building a Secure System using TrustZone Technology.* `https://www.arm.com/products/security-on-arm/trustzone`.

Bagloee, Saeed Asadi, Madjid Tavana, Mohsen Asadi, and Tracey Oliver. "Autonomous vehicles: challenges, opportunities, and future implications for transportation policies." *Journal of Modern Transportation* 24, no. 4 (2016): 284–303.

Buterin, Vitalik. *On Public and Private Blockchains.* Ethereum Blog, 2015.

Cachin, Christian, and Marko Vukolic. *Blockchain Consensus Protocols in the Wild*, 2017. eprint: `arXiv:1707.01873v2`.

Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance and proactive recovery." *ACM Trans. Comput. Syst.* 20, no. 4 (2002): 398–461.

Corsaro, Angelo. "Cloudy, Foggy and Misty Internet of Things." In *7th ACM/SPEC on Intl. Conf. on Performance Engg.* 261–261. Delft, The Netherlands, 2016.

Dominic, Derrick, Sumeet Chhawri, Ryan M. Eustice, Di Ma, and André Weimerskirch. "Risk Assessment for Cooperative Automated Driving." In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, Austria*, 47–58. 2016.

Frost and Sullivan. *Future of Mobility.* `https://ww2.frost.com/research/visionary-innovation/future-mobility`.

Garip, Mevlut Turker, Mehmet Emre Gursoy, Peter Reiher, and Mario Gerla. "Congestion attacks to autonomous cars using vehicular botnets." In *NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA*. 2015.

Gerla, Mario, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee. "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds." In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 241–246. IEEE, 2014.

Hearn, Mike. *Corda: A distributed ledger.* `https://docs.corda.net/head/_static/corda-technical-whitepaper.pdf`, 2015.

Intel Corporation. *Intel Trusted Execution Technology.* `https://www.intel.com/content/www/us/en/architecture-and-technology/trusted-infrastructure-overview.html`.

Kokoris-Kogias, Eleftherios, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding." In *2018 IEEE Symposium on Security and Privacy, SP 2018, Proceedings, 21-23 May 2018, San Francisco, California, USA*, 583–598. 2018.

Land Transport Authority, Government of Singapore. *Smart Mobility 2030.* https://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion/intelligent-transport-systems/SmartMobility2030.html, 2014.

Luu, Loi, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. "A Secure Sharding Protocol For Open Blockchains." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, 17–30. 2016.

Miller, Andrew, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. "Sprites: Payment Channels that Go Faster than Lightning." *CoRR* abs/1702.05812 (2017). arXiv: 1702.05812.

Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." *Black Hat USA* 2015 (2015): 91.

Mitra, Sananda, Sumanta Bose, Sourav Sen Gupta, and Anupam Chattopadhyay. "Secure and Tamper-resilient Distributed Ledger for Data Aggregation in Autonomous Vehicles." In *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 548–551. IEEE, 2018.

Parkinson, Simon, Paul Ward, Kyle Wilson, and Jonathan Miller. "Cyber threats facing autonomous and connected vehicles: Future challenges." *IEEE Trans. on Intelligent Transportation Systems* 18, no. 11 (2017): 2898.

Petit, Jonathan, and Steven E. Shladover. "Potential Cyberattacks on Automated Vehicles." *IEEE Trans. Intelligent Transportation Systems* 16, no. 2 (2015): 546–556.

Poon, Joseph, and Vitalik Buterin. *Plasma: Scalable Autonomous Smart Contracts.* http://plasma.io/plasma.pdf, 2017.

Rettore, Paulo H. L., Bruno P. Santos, Andre B. Campolina, Leandro A. Villas, and Antonio A. F. Loureiro. "Towards intra-vehicular sensor data fusion." In *19th IEEE Intl. Conf. on Intelligent Transportation Systems, Brazil*, 126. 2016.

Schellekens, Maurice. "Car hacking: Navigating the regulatory landscape." *Computer Law & Security Review* 32, no. 2 (2016): 307–315.

Seimens AG. *Smart Mobility – A tool to achieve sustainable cities.* http://www.vt.bgu.tum.de/fileadmin/w00bnf/www/VKA/2014_15/150212_Smart_Mobility_v5_TUM.pdf, 2015.

Sung, Gang-Neng, Chun-Ying Juan, and Chua-Chin Wang. "Bus Guardian Design for automobile networking ECU nodes compliant with FlexRay standards." In *IEEE Intl. Symposium on Consumer Electronics*, 1–4. 2008.

Teutsch, Jason, and Christian Reitwießner. *A scalable verification solution for blockchains.* https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf, 2017.

The Linux Foundation. *Hyperledger.* https://www.hyperledger.org/projects/fabric, 2016.

Vogelsteller, Fabian, Vitalik Buterin, et al. *Ethereum Whitepaper.* https://github.com/ethereum/wiki/wiki/White-Paper, 2017.

Wolf, Marko, André Weimerskirch, and Christof Paar. "Security in automotive bus systems." In *Workshop on Embedded Security in Cars.* 2004.

Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle CAN." *IEEE Transactions on Intelligent Transportation Systems* 16, no. 2 (2015): 993–1006.

Zhong, Sheng, Hong Zhong, Xinyi Huang, Panlong Yang, Jin Shi, Lei Xie, and Kun Wang. "Connecting Things to Things in Physical-World: Security and Privacy Issues in Vehicular Ad-hoc Networks." In *Security and Privacy for Next-Generation Wireless Networks*, 101–134. Springer International Publishing, 2019.