Distributed Ledger Technology in Autonomous Driving: A Security Protection Layer

Nicola Raemy[1], *Galia Kondova*[2]

[1] School of Business FHNW
Olten, 4600, CH

[2] School of Business FHNW
Basel, 4002, CH

ABSTRACT

Cybersecurity in autonomous driving is of utmost importance since a hacked self-driving car could turn into a remote-controlled weapon. Appropriate measures must be taken and implemented to ensure future road safety. The substantially shorter renewal cycles in the hardware (e.g., sensors, computer hardware) and especially software domain compared to the current service life of a vehicle represent a further challenge The use of blockchain technology could enhance security in autonomous driving and thus reduce cybersecurity risks. This paper studies current developments of Swiss pilot projects in autonomous driving and discusses existing solutions for increasing safety of autonomous driving through blockchain.

Keywords: Autonomous Driving, Blockchain, Data Security, Cybersecurity, DLT

INTRODUCTION

For the automotive industry, especially in terms of autonomous driving, cybersecurity is particularly important because a hacked self-driving car could easily become a remote-controlled weapon if taken over by malicious hands (ITU, 2022). At the same time, distributed ledger technology (DLT or blockchain) offers characteristics that enhance personal mobility data privacy and security.
Thus, a significant potential for blockchain in IoT applications including autonomous driving has been identified in the existing literature (Peng et al., 2020). The future integration of the technology into the process and product range is considered vital and thus a future strategic potential for success in the automotive industry (Boyle et al., 2022).

Autonomous driving standards and requirements

Mahmood (2022) defines the connected car as an integral part of the Internet of Vehicles (IoV), which is an application field of Internet of Things (IoT) for the automotive sector. Crucial technologies for this purpose are the internet of everything (IoE), artificial intelligence (AI), machine learning (ML), neural networks, sensor technology edge, and cloud computing. Connectivity among different vehicles is achieved by communicating between sensors and smart devices in the vehicles and other smart systems in the environment.
Vehicular networks were originally created to enable date-driven services and applications in cars or other vehicles. Vehicular ad hoc networks (VANETs) mostly run in ad hoc mode and usually set their scope on traffic safety applications between vehicles and their connection to roadside units (RSUs). Dedicated short-range communication and the Car-2-Car Communication Consortium have been deployed in many places to improve these inter-vehicle communications. Combined with the emergence of IoT technology, traditional VANETs have evolved into IoV (Shen et al., 2020), which combines IoT, VANET, and mobile cloud computing.
Cloud computing allows one to store and analyze various kinds of data and make this data available to a wide range of services at any time. In vehicle-to-cloud (V2C) technology, every vehicle in the VANET communicates with the cloud ecosystem and provides services based on this environment (Gupta et al., 2021; Mahmood, 2022). In IoV, data is instantaneously exchanged between vehicles and RSUs using cellular technology, GPS systems, smart terminals, and information platforms. The result is an exchange of information that favors interaction and becomes a driving-guidance- controlling network system. The Internet of Vehicles is the logical evolution of vehicle-to-vehicle (V2V) connectivity, which further develops the assistance systems for complete autonomous driving. This development of assistance systems is achieved by vehicle AI, which recognize the environment and other road users and can process this information accordingly. Subsequent interactions in IoV are possible (CAAT, 2022; Mahmood, 2022; USDOT, 2022) such as cloud and vehicle interaction (V2C), device-to-device interaction, personal devices and vehicle interaction, V2V interaction, vehicle and infrastructure interaction (V2I), etc.

"Vehicle-to-everything" is used as an umbrella term for the mentioned interactions (Mahmood, 2022).

Automated driving is part of Switzerland's digital strategy aiming to be smart, connected, and efficient in all areas (Bundeskanzlei BK, 2022) while with a minimal risk regarding cybersecurity in automated driving (Bundeskanzlei BK, 2022).
Since 2015, automated vehicles have been operating on public roads in Switzerland as part of pilot projects. According to statements by ASTRA (ASTRA, 2022), Switzerland holds a leading position worldwide in the field of public passenger transport with its automated test vehicles. Various reports provide insight into the tests and the knowledge gained from them, presenting information on the respective state of the art and explaining how the complex topic is approached. The execution of the automated vehicle trials is the responsibility of the respective companies. The following projects took place in Switzerland (ASTRA, 2022): Transports publics genevois (TPG) - Belle-Idéé X2, Transports publics fribourgeois (TPF) - MARLY-MIC, Verkehrsbetriebe Schaffhausen (VBSH) - Linie 12, Bernmobil (SVB) - Selbstfahrendes Fahrzeug (SFF), PostAuto - SmartShuttle Sion 2.0, SBB - MyShuttle.

In addition, the institution ROSAS (Robust and Safe Systems) recently announced it was conducting research in the field of cybersecurity for autonomous vehicles (SRF, 2022). The primary aim of this project was to gain experience in the field of teleoperation and bring the research for all transport operators to the next level. Through the findings from the ROSAS project, there is no longer any need for an accompanying person to be present in the self-driving vehicle (ROSAS, 2022). Figure 1 provides a simplified illustration of the remote-control concept for automated and networked vehicles on the basis of safety and cybersecurity requirements.

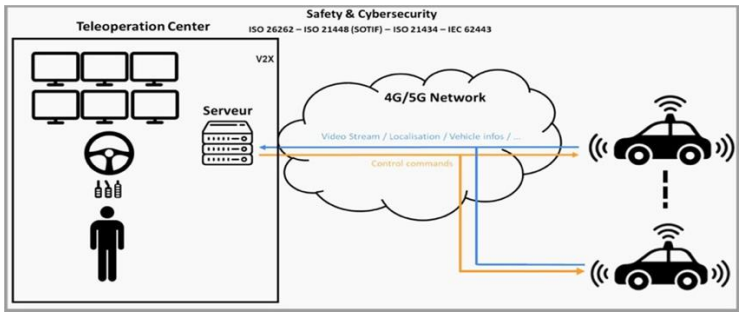

Figure 1. Concept for centralized teleoperation for remote control of automated and networked vehicles (Scherwey, 2022)

Scherwey (2022) notes that from a technical perspective, the challenge is to develop a centralized teleoperation system that allows automated and connected vehicles to be controlled remotely while ensuring reliability and safety (including cybersecurity).

Autonomous Driving Risks and Mitigation

Increasing interconnectivity and intensified data exchange between different technical systems raises questions about security. These concerns are particularly relevant in the area of automated vehicles. Thus, the importance of cybersecurity is correspondingly high. Suitable measures must be defined and implemented. The life cycles for hardware (e.g., computing hardware or sensors) and especially software will be substantially shorter in the future compared to today's vehicle lifetimes and pose a particular challenge. However, the vehicles are only one aspect of the automated driving ecosystem. The entire surrounding area must also be adequately considered in terms of cybersecurity and developed accordingly. This process requires, for example, that the various stakeholders exchange information about cybersecurity incidents, as now occurs in the software industry and in the air traffic domain. This exchange is the only way to ensure that incidents can be dealt with quickly across the transport system (UVEK, 2022). In its conclusion, the Federal Department of Environment, Transport, Energy and Communications (UVEK, 2022) report classifies the anchoring of cybersecurity in law as a high-priority issue. The final report of the Road Safety Fund (Willi et al., 2018) determined that, depending on the scenario, accident reductions due to new hazard patterns (environmental instead of driver-related) in automation levels 4 and 5 could exceed the previous safety gains in road traffic. The study therefore recommends further research in the area of automotive cybersecurity and resilience. In another, global study, there were also security concerns about new threat patterns, such as software hacking (Kyriakidis et al., 2017).

To mitigate future risks regarding automated driving, ASTRA has defined four key directions. One is to “increase road safety and ensure data protection. ”This road safety and data protection includes data exchange (e. g. vehicle-to-everything communication [V2X] and V2V) and dealing with cybersecurity (Fehlberg et al., 2022; Oehry et al., 2022). For an automated transport system, in terms of cyber resilience, there are significant challenges to securing against cyber-attacks and maintaining adequate protection over the lifetime/deployment of the relevant systems while maintaining interoperability. Guidelines on how cantons and municipalities can deal with the challenges of V2I need to be developed (Oehry et al., 2022). As a further measure, the panel recommends care be taken in Switzerland to ensure that there is no legal requirement to provide externally accessible interfaces to automated vehicles. The OEM is held responsible for resilience in general (Oehry et al., 2022). Finally, handling data traffic from automated driving must be clarified. Extensive amounts of information are generated, exchanged, processed, and in some cases stored during operation. In addition to clear regulations, minimum requirements and standards are also needed. These include points such as encryption, reliability, and data quality. Data storage must be clarified nationally or in coordination with foreign stakeholders. Redundancy must be ensured in the IT systems (Oehry et al., 2022).

The risks and challenges highlighted above in relation to data protection and road safety in connection with automated driving can be mitigated by possible blockchain solutions.

Blockchain Solutions to Increase Security in Autonomous Driving

The risks and challenges highlighted above in relation to data protection and road safety in connection with automated driving can be mitigated by possible blockchain solutions. Patsakis et al. (2019), for example, consider the blockchain a security protocol based on an external database in addition to the DLT (see Figure 2).

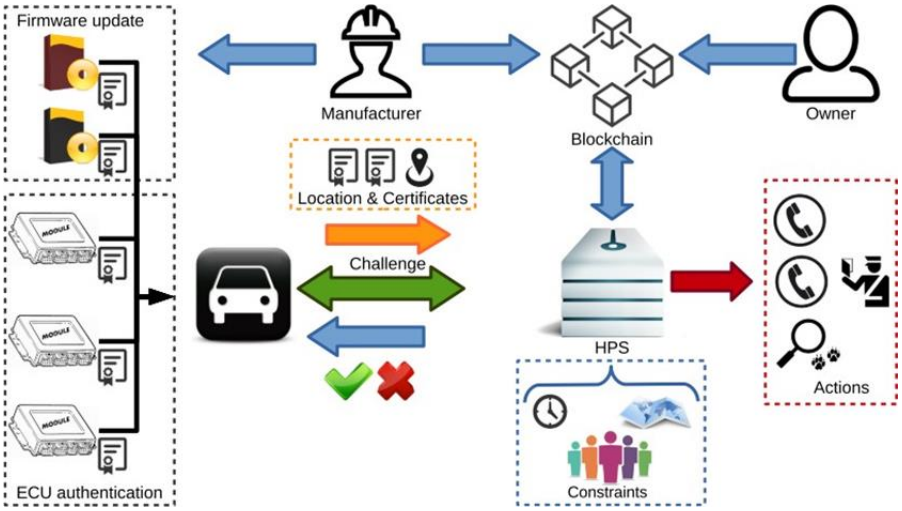

Figure 2. The proposed infrastructure from Patsakis et al. (Patsakis et al., 2019)

The blockchain and the database are connected to the immobilizer. The system detects manipulations and can thus mitigate attacks by unauthorized users. The presented solution introduces minimal overhead and provides an extra security layer. This extra security tier enables detection, blocking, and tracking of various attacks. The introduction of the proposed solution requires several changes in the structure of the car architecture and its components. Because vehicles will be subject to enormous changes in the near future, it is the right time to reconsider how to implement long-known and long-lasting safety mechanisms into vehicles and ensure these mechanisms are appropriate for the vehicles' real-time requirements (Patsakis et al., 2019).

Another promising solution, presented by Jabbar et al. (Jabbar et al., 2020), is the new decentralized IoT solution for vehicle communication. One challenge in IoV (particularly in V2V or V2I communication) is ensuring data is sent quickly and is securely recorded. To overcome these challenges, Jabbar et al. (Jabbar et al., 2020) adapted the blockchain technology for real-time applications to solve V2X communication problems. Their system establishes secure communication and provides a decentralized cloud computing platform. In addition, Jabbar et al. tested the performance and resilience of the proposed system against current security attacks. Initial stress tests indicated that their proposed solution solved the main challenges of V2X communication, such as centralization, security, and lack of privacy. Moreover, their solution guaranteed uncomplicated data exchange between

different ITS actors. Figure 3 depicts the high-level architecture of Jabbar et al.'s proposed IoT solution.

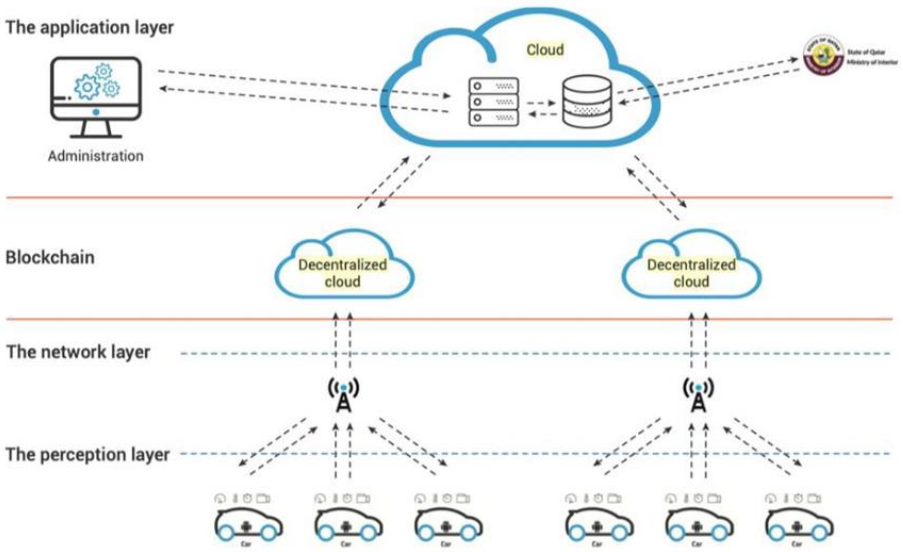

Figure 3 Architecture of proposed IoT solution (Jabbar et al., 2020)

The model provides secure communication between vehicles and other actors in the ITS. Because the model tries to overcome limitations such as execution time, it improves performance. The model is based on an IoT architecture and includes three layers: The perception layer, the network layer, and the application layer (as shown in Figure 3). The layers are briefly described below (Jabbar et al., 2020).

The perception layer is a physical layer composed of many different IoT devices equipped with sensors. The sensors identify and gather information about the environment or detect nearby (smart) objects. The implemented Android application for vehicles collects and analyzes data about the driving, the vehicle itself, and the driver's driving behavior. The Android application for infrastructure emulates the IoT devices embedded in the streets, such as traffic lights, RSUs, radars, and signs.

The network layer is responsible for the connection between sensors to other servers, network devices, smart devices, and the transmission/processing of sensor data.

The application layer includes the blockchain application as well as the central cloud server. The application layer delivers application-specific services to the IoT devices. Specifically, the blockchain application handles the communication between vehicles and other entities in the ITS. The central cloud server processes and analyzes the collected data and handles the invitations from other actors.

CONCLUSIONS

This paper has taken stock of existing challenges facing autonomous driving based on several pilot projects in Switzerland. In particular the cybersecurity risk has been identified as a significant challenge. At the same time, the blockchain technology promises solutions to enhance data protection and security. The models proposed by Patsakis et al. (Patsakis et al., 2019) and Jabbar et al. (Jabbar et al., 2020) have been presented in this article, showing how a potential infrastructure architecture for autonomous driving could look like by applying blockchain for enhancing cybersecurity.

REFERENCES

ASTRA. (January 14, 2022). Erkenntnisse aus Pilotversuchen mit automatisierten Fahrzeugen. Intelligente Mobil. Pilot. Website: https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet/pilotversuche/erkenntnisse-aus-pilotversuchen.html

Boyle, B., Janssens, S., Brenner, A., Rasmoela, M., Steger, S. (January 14, 2022). The blockchain bandwagon – Is it time for automotive companies to start investing seriously in blockchain? Roland Berg. Website: https://www.rolandberger.com/en/Insights/Publications/Blockchain%27s-potential-in-the-automotive-industry.html

Bundeskanzlei BK. (January 14, 2022). Sicherheit im Bereich automatisiertes Fahren. Strateg. Digit. Schweiz. Website: https://www.digitaldialog.swiss/de/sicherheit-im-bereich-automatisiertes-fahren

CAAT. (January 14, 2022). Connected and Automated Vehicles. Cent. Adv. Automot. Technol. Website: http://autocaat.org/Technologies/Automated_and_Connected_Vehicles/

Fehlberg, H., Pirkelbauer, S., Wieland, E., Antz, A., Bruckmann, D., Chanard, T., Sauter-Servaes, T., Müggler, M., Lehrmann, A., Egeler, C. (January 14, 2022). Auswirkungen des automatisierten Fahrens; Erkenntnisse und Massnahmen aus Sicht des ASTRA. Forschungsprojekt ASTRA 2017004. Website: https://www.mobilityplatform.ch/fileadmin/mobilityplatform/normenpool/21781_1691_Inhalt.pdf

Gupta, N., Prakash, A., Rajeev, T. (2021). Internet of Vehicles and its Applications in Autonomous Driving. Cham, Springer Nature Switzerland AG.

ITU. (January 14, 2022). Cybersecurity in the automotive industry challenges to overcome. Website: https://www.itu.int/en/myitu/News/2020/04/14/12/03/Cybersecurity-in-the-automotive-industry-challenges-to-overcome

Jabbar, R., Kharbeche, M., Al-Khalifa, K., Krichen, M., Barkaoui, A.K. (2020). Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum. Sensors 20 (14), 3928.

Kyriakidis, M., de Winter, J.C.F., Stanton, N., Bellet, T., van Arem, B., Brookhuis, K., Martens, M.H., Bengler, K., Andersson, J., Merat, N., Reed, N., Flament,

M., Hagenzieker, M., Happee, R. (2017). A human factors perspective on automated driving. Theor. Issues Ergon. Sci. 20, 223–249.
Mahmood, Z. (2020). Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV, 1st ed. Cham, Springer Nature Switzerland AG
Oehry, A.B., Jermann, J., Bohne, S., Frick, R., Ickert, L., Greinus, A., Schippl, J., Fleischer, T. (January 14, 2022). Auswirkungen des automatisierten Fahrens; Teilprojekt 1: Nutzungsszenarien und Auswirkungen. Website: https://www.mobilityplatform.ch/fileadmin/mobilityplatform/normenpool/21778_1681_Inhalt.pdf
Patsakis, C., Dellios, K., De Fuentes, J.M., Casino, F., Solanas, A. (2019). External Monitoring Changes in Vehicle Hardware Profiles: Enhancing Automotive Cyber-Security. J. Hardw. Syst. Secur. 3, 289–303.
Peng, C., Wu, C., Gao, L., Zhang, J., Alvin Yau, K.-L., Ji, Y. (2020). Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues. Sensors 20 (18), 5079.
ROSAS. (January 14, 2022). Teleoperation of autonomous vehicles. Website: https://www.rosas.center/en/projects/teleoperation-of-autonomous-vehicles/
Scherwey, R. (January 14, 2022). NRP - Téléopération. Inst. Smart Secur. Syst. ISIS. Website: https://www.heia-fr.ch/de/anwendungsorientierte-forschung/institute/isis/forschungsprojekte/nrp-teleoperation/
Shen, X., Fantacci, R., Chen, S. (2020). Internet of Vehicles. Proc. IEEE 108, 242–245.
SRF. (January 14, 2022). Tagesschau vom 18.05.2021: Hauptausgabe . Ferngesteuerte Auton. Fahrzeuge. Website: https://www.srf.ch/play/tv/tagesschau/video/tagesschau-vom-18-05-2021-hauptausgabe?urn=urn:srf:video:d5d993c4-5a16-47a1-859b-d06323ffaa9f
USDOT. (January 14, 2022). Vehicle-to-Pedestrian (V2P) Communications for Safety. Intell. Transp. Syst. Website: https://www.its.dot.gov/research_archives/safety/v2p_comm_safety.htm
UVEK. (January 14, 2022). Bereitstellung und Austausch von Daten für das automatisierte Fahren im Strassenvekehr . Website: https://www.astra.admin.ch/dam/astra/de/dokumente/abteilung_strassennetzeallgemein/bereitstellung-austausch-daten-automatisiertes-fahren.pdf.download.pdf/Bereitstellung und Austausch von Daten für das automatisierte Fahren im Strassenverkehr.pdf
Willi, C., Deublein, M., Hafsteinsson, H. (January 14, 2022). Automatisiertes Fahren: Auswirkungen auf die Strassenverkehrssicherheit . Fonds Für Verkehrssicherheit EBP Schweiz AG. Website: https://www.astra.admin.ch/dam/astra/de/dokumente/abteilung_strassennetzeallgemein/automatisiertes-fahren_auswirkungen-auf-die-strassenverkehrssicherheit.pdf.download.pdf/2018-05-31_Schlussbericht_aFn.pdf