A Survey of Blockchain Solutions for Autonomous Vehicles Ecosystems

Swati Megha, Hamza Salem, Enes Ayan, Manuel Mazzara
Innopolis University, Russia

Abstract. Since the beginning of the 2010s major car manufacturers progressively started to invest in Autonomous Vehicles (AV). Notable examples are Tesla, Ford, and Toyota. Small startups and tech giants like Google and Yandex are now also entering the competition to propose new solutions. Most of them have already developed their prototypes of driverless vehicles that you can normally observe in the streets of New-York, USA, or Innopolis, Russia. Despite the significant hype on this technology, current solutions are not always optimal and multiple challenges are left open in a domain such as security, data integrity, privacy, and communication. Blockchain is one of the most appealing technologies to be used in this domain since it provides solutions for some of these challenges. In this paper, we describe, categorize, and evaluate different solutions of the Autonomous Vehicles Industry that makes use of Blockchain. We use a software engineering approach to organize the existing work in multiple categories such as challenges addressed, quality attributes promoted. This work is intended to provide researchers in the field with a well-defined and structured categorization, plus insights into the existing literature.

Keywords— Autonomous Vehicles (AV), Blockchain, Smart Contract, Quality Attributes

1. Introduction
When visiting for the first time Innopolis City in Tatarstan, Russia, the experience that cannot be missed is a ride on a "Yandex Self-Driving Taxi" [7]. These cars are the first driverless vehicles operating on actual streets in Russia, together with regular human drivers. Innopolis is the visionary city of the future depicted in the dream of artists, novelists, philosophers, scientists, and movie makers for more than one century [12]. An AV Ecosystem is the pillar of that dream. This research field has recently become an important direction for companies and car manufacturers to show their ability in building strong and stable solutions to automate the process of driving, gas filling, and other multiple micro-process such as updating software and communicating and archiving information inside the vehicles. Each solution can be evaluated according to different criteria among which the safety of passengers and pedestrians is the most important of all, and companies are investing billions of dollars in research and development to be at the cutting-edge[7]. Blockchain is one of the technologies that has been a trend and attracted attention in recent years. Founded on its peer-to-peer nature and lack of need for a trusted central authority, Blockchain offers quality attributes such as integrity, security, and privacy to various industries. [24].

An Autonomous Vehicle can operate itself performing all the necessary functions without any human interaction, through the ability to sense its surroundings. It includes an automated driving system to allow the vehicle to respond to external conditions that a human driver would
be able to manage. There are six different levels of automation in AV [18]:

- Level 0 – No Automation.
- Level 1 – Driver Assistance.
- Level 2 – Partial Automation.
- Level 3 – Conditional Automation.
- Level 4 – High Automation.
- Level 5 – Full Automation

At level 0, the car has no control over the driving and the driver will do everything. At level 1, the vehicle’s ADAS (advanced driver assistance system) can help and support the driver with either steering or accelerating and braking. At level 2, the ADAS can oversee steering and accelerating and braking in some conditions, although the human driver is required to continue paying complete attention to the driving environment throughout the process. At level 3, the ADS (advanced driving system) can perform all parts of the driving task in some conditions, but the human driver is required to be able to regain control when requested to do so by the ADS. At level 4, the vehicle’s ADS can perform all driving tasks independently in certain conditions in which human attention is not required. Finally, level 5 involves full automation whereby the vehicle’s ADS can perform all tasks in all conditions, and no driving assistance is required from the human driver. This full automation will be enabled by the application of 5G technology, which will allow vehicles to communicate not just with one another, but also with traffic lights, signage and even the roads themselves [2].

In this paper, we will propose a survey for different solutions to demonstrate how AV can use Blockchain technology to improve and solve future and present challenges. We will first describe in Section 2 what we consider to be the major challenges that the Autonomous Vehicle Ecosystem has to face; then, in Section 3 we will use our experience in Software Engineering and take a requirements engineering approach to determine what requirements for the current AV sector are emerging from the described challenges and which quality attributes are being promoted, based on a literature survey on AV and Blockchain. Finally, section 4 draws some conclusions.

2. Challenges

In this section, we will discuss what we consider the major challenges that the AV Ecosystem has to face to produce real stable products in the market. The following aspects can synthesize our current understanding:

(i) Challenges in Security & Privacy: Cyber-crimes can be the most dangerous challenge in the security field. AVs are very prone to cyber-crimes. Criminals might be motivated to hack into the vehicles’ operating systems and steal some important passenger data, or else change its operation and threaten the passenger’s safety. Malicious attacks can happen via these wireless vehicular networks or via Sybil Attack aiming at P2P networks, where a malicious client pretends to be multiple clients on the network to gain more influence [23]. So privacy, data integrity, and data accuracy are the most important challenges that researchers should focus on, and mitigate different threats and attack models. AV systems should provide proof of safety for drivers and others on the road. As we will demonstrate in this paper, several AV pilot systems are already underway in multiple countries, so far, and no security issues related to hacking have been observed yet.

(ii) Challenges in Availability: Centralized systems are systems that use client-server architecture where one or more client nodes are directly connected to one central server. This is the most commonly used type of system, the nodes send a request and the server replies with a response and the node receives the response. However, these systems
have different challenges. For example, the system is highly dependent on the network connectivity, so it can fail if the nodes lose connectivity as there is only one central node. Also, less possibility of data backup. For example, if the server node fails and there is no backup, you lose the data straight away. In this paper, we will demonstrate multiple centralized systems used in AV. For example, one of the papers will demonstrate an "update scheme" using the third party. Also, we will see how Blockchain will help to replace the centralized third parties to distribute the new updates with the node participants in the network to do the distribution process and take advantage of their mobility to guarantee high availability and fast delivery of the updates.

(iii) **Challenges in Scalability & Performance**: Communication in AV systems is one of the most critical parts and cybercrimes are one of these examples. Cyber attacks are not just aiming for manipulating the data, it can aim to flood the system with fake requests to make the service stop. DoS or Denial-of-service attack [22] is an example of that. One of the main AV systems receives some information from IoT devices and stores records to ensure the customer’s safety. However, some malicious users on the internet of vehicles may mislead the whole communication where intruders may compromise smart devices to execute a malicious plot or they just want to flood the network with fake requests to cause DoS. Blockchain as a technology can provide a new security mechanism for connected AV services. For example, Blockchain provides transparency among various authorities inside the system. So, this will reduce the users’ fake requests, improve the compromise of IoT devices, and will reflect in both performance and scalability.

(iv) **Challenges in Trustability & Social Welfare**: In the AVs ecosystem, stakeholders always concern about the accidents that will happen for the vehicles. All the efforts from security insurances to the legalization process try to minimize the effect of these accidents. However, for sure the accidents are still an event that can occur for any AV between themselves or with human subjects and the liability must be indubitably decided based on accident forensics. To achieve tractability in such a system Blockchain proposes an event recording mechanism for AV. All indisputable accident forensics by ensuring that event information is trustable and verifiable using a consensus scheme to verify and confirm the new block of event data in an efficient way without any central authority. Considering trustability in AV, Blockchain can also increase social welfare for trading mechanisms between drivers and grid stations. For example, by using an iterative double auction mechanism in localized P2P electricity trading system auctioneers bid their prices, and the process work as any simple auction, every participant in this auction can guarantee transaction security, privacy protection, user satisfaction, and the minimum cost or the best prices.

3. Categorization
The previous section describes four main challenges related to AV Ecosystem. It is important to note here that from a software engineering perspective, all the main challenges, are also quality challenges. And the challenge could be addressed through promoting the associated quality attribute. Based on this software engineering approach we categories each of the literature into one or more quality attribute they are trying to promote. We have therefore divided 17 literature into 6 quality attributes, where most of the papers promote indeed more than one attribute, as it can be observed in Table 1. Data security, privacy, reliability, and human safety are some of the most promoted quality attributes among researchers.

Paper [17] and [3] promote data security and integrating, [17] presents a secured inter-vehicle communication network leveraging side-channels and a Blockchain public key infrastructure. And [3] discusses a VANET Blockchain implementation to ensure data integrity and security as a possible contribution of Blockchain in vehicle-to-vehicle communication. Data security,
Table 1. Quality Attributes mapping to research papers

| HumanSafety | DataSecurity | Privacy | Transparency | Reliability | Efficiency |
|-------------|--------------|---------|--------------|-------------|------------|
| [17]        | [3]          |         |              |             |            |
|             | [14]         | [14]    | [14]         | [14]        | [14]       |
|             | [19]         |         | [19]         |             |            |
| [1]         | [13]         | [13]    | [13]         |             |            |
| 20          | 20           |         | 20           |             |            |
| 5           | 5            |         |              |             |            |
| 8           | 8            |         |              |             | 8          |
| 16          | 16           | [16]    | [16]         |             |            |
| 15          | 15           | [15]    | [15]         |             | [15]       |
| [6]         |              |         |              | [6]         |            |
| [4]         |              |         |              | [4]         |            |
|              |              |         |              | [11]        |
| [10]        |             |         | [10]         |             | [10]       |
| [9]         |              |         |              | [9]         |            |
| 21          | 21           |         |              |             |            |

integrity, privacy, and availability are the focus of the paper [14]. The paper claims to be the first data and information-centric design of autonomous vehicle architecture, with integrated measures for security, tamper-resilience, and privacy [14].

Paper [19], [1] and [6] proposes a system for IV communication among IVs using the Blockchain technology that promotes security and reliability. Data transparency is the focus of paper [13] and [9], whereas [13] and [21] promote data security and privacy. Paper [13] includes three algorithms Algorithm 1 for Smart contract implementation, Algorithm 2 for Reputation-based DBFT consensus, Algorithm 3 for Dynamic optimal contract assignment, and energy allocation. Extensive numerical results are shown to evaluate and demonstrate the effectiveness and efficiency of the proposed scheme through comparison with other conventional schemes. Paper [21] Propose a contract-based energy Blockchain for secure EV charging in SC. Paper [9] presents a primary prototype based on Ethereum is analyzed and implemented for illustration also includes source code.

Paper [20],[5], [8], [16] and [15] focuses on a different aspect i.e. human safety and aftermath of an accident. Paper [20] proposes the system is reward-based with crypto IV-TP that also includes unambiguous availability of records in case of accidents. In the future proposes, to test the system on real-time traffic data. And paper [5] proposes a Multi-Agent AIM(MA-AIM) system based on V2I/I2V communication to securely manage vehicles crossing through an intersection by leveraging Blockchain facilities. Paper [8] and [15] addresses Possible data tampering after autonomous vehicle accidents can lead to wrong accident forensic leading to unfair liability.

Paper [16] deals with secure information exchange in real-time among connected and autonomous vehicles. Paper [4] and [10] addresses efficiency. Paper [4] proposes a distributed firmware update scheme for the AVs’ subsystems, leveraging consortium Blockchain, and smart contract technology. Paper [10] proposes, and the optimal charging scheduling algorithm for hybrid vehicle charging scenarios. Paper [11] Proposes a localized Peer-to-Peer(P2P) electricity trading model for locally buying and selling electricity among Plug-in Hybrid Electric Vehicles (PHEVs) in smart grids that have a focus on cost optimization with other quality attributes.
4. Conclusion
Blockchain is a new system of trust. With this technology for authentication, which uses ledgers that never lose data, and applying it to the AV Ecosystem, different challenges can be solved in security, privacy, availability, and performance. In this paper, we analyzed different AV solutions and their challenges, and how Blockchain as technology can provide multiple solutions. We used a software engineering approach to categorize the existing work in several categories based on addressed challenges and quality attributes. The findings of this study indicate that none of the papers that we have analyzed reached the product or profit stage. However, according to expectations AV applications interact with different elements of the environment, including people and cars on the road, traffic lights, and signs, therefore making any solution dangerous if not released after years of prototyping. With this paper, we aimed at providing an adequate background for scientists interested in applying their expertise in this specific field. Taken together, 17 solutions categorized to six quality attributes; Human Safety, Data Security, Privacy, Transparency, Reliability, and Efficiency, and each challenge in section 2 have been addressed in these papers and show how Blockchain can solve that challenge. The work can be seen as a starting point for more investigation on the adoption and implementation of Blockchain in AV Ecosystems.

References
[1] Arushi Arora and Sumit Yadav. “Block Chain Based Security Mechanism for Internet of Vehicles (IoV)”. In: SSRN Electronic Journal (Jan. 2018). doi: 10.2139/ssrn.3166721.
[2] Autonomous Cars Won’t Work - Until We Have 5G. URL: https://www.forbes.com/sites/bijankhosravi/2018/03/25/autonomous-cars-wont-work-until-we-have-5g.
[3] Reid Barber. “Autonomous Vehicle Communication Using Blockchain. Honors Theses. 789.” In: (2018).
[4] M. Baza et al. “Blockchain-based Firmware Update Scheme Tailored for Autonomous Vehicles”. In: (Apr. 2019). issn: 1525-3511. doi: 10.1109/WCN.2019.8885769.
[5] Alina Buzachis et al. “A Secure and Dependable Multi-Agent Autonomous Intersection Management (MA-AIM) System Leveraging Blockchain Facilities”. In: 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion) (2018), pp. 226–231.
[6] C.Oham et al. “B-FICA: BlockChain based Framework for Auto-insurance Claim and Adjudication”. In: (Jan. 2018). doi: 10.1109/Cybermatics_2018.2018.00210.
[7] Europe’s First Driverless Taxis to Launch in Russia. https://www.themoscowtimes.com/2018/08/28/europes-first-driverless-taxis-to-launch-in-russia-a62694. Accessed: 26/02/2020.
[8] H. Guo, E. Meamari, and C. Shen. “Blockchain-inspired Event Recording System for Autonomous Vehicles”. In: (Aug. 2018), pp. 218–222. issn: null. doi: 10.1109/HOTICN.2018.8606016.
[9] Song Hua et al. “Apply blockchain technology to electric vehicle battery refueling”. In: (Jan. 2018). doi: 10.22451/HICSS.2018.567.
[10] Xiaohong Huang et al. “An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains”. In: Future Generation Computer Systems 91 (Sept. 2018). doi: 10.1016/j.future.2018.09.046.
[11] J. Kang et al. “Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains”. In: IEEE Transactions on Industrial Informatics 13.6 (Dec. 2017), pp. 3154–3164. ISSN: 1941-0050. DOI: 10.1109/TII.2017.2709784.

[12] Knight Rider. https://en.wikipedia.org/wiki/Knight_Rider. Accessed: 26/02/2020.

[13] H. Liu, Y. Zhang, and T. Yang. “Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing”. In: IEEE Network 32.3 (May 2018), pp. 78–83. ISSN: 1558-156X. DOI: 10.1109/MNET.2018.1700344.

[14] 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) (2018), pp. 548–551.

[15] Chuka Oham et al. “A Blockchain Based Liability Attribution Framework for Autonomous Vehicles”. In: ArXiv abs/1802.05050 (2018).

[16] Geetanjali Rathee et al. “A Blockchain Framework for Securing Connected and Autonomous Vehicles”. In: 9 (July 2019). DOI: 10.3390/s19143165.

[17] Sean Rowan et al. “Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels”. In: ArXiv abs/1704.02553 (2017).

[18] Self-driving vehicles: What are the six levels of autonomy? URL: https://newatlas.com/sae-autonomous-levels-definition-self-driving/49947/. (accessed: 26/02/2020).

[19] M. Singh and S. Kim. “Trust Bit: Reward-based intelligent vehicle comminon using blockchain paper”. In: (Feb. 2018), pp. 62–67. ISSN: null. DOI: 10.1109/WF-IoT.2018.8355227.

[20] Madhusudan Singh and Shiho Kim. “Blockchain Based Intelligent Vehicle Data sharing Framework”. In: ArXiv abs/1708.09721 (2017).

[21] Z. Su et al. “A Secure Charging Scheme for Electric Vehicles With Smart Communities in Energy Blockchain”. In: IEEE Internet of Things Journal 6.3 (June 2019), pp. 4601–4613. ISSN: 2372-2541. DOI: 10.1109/JIOT.2018.2869297.

[22] Understanding Denial-of-Service Attacks. URL: https://www.us-cert.gov/ncas/tips/ST04-015.

[23] What’s a Sybil Attack & How Do Blockchains Mitigate Them? URL: https://coincentral.com/sybil-attack-blockchain/.

[24] Rui Zhang, Rui Xue, and Ling Liu. Security and Privacy on Blockchain. 2019. arXiv: 1903.07602 [cs.CR].