Asian Journal of Research in Computer Science

Volume 17, Issue 2, Page 1-14, 2024; Article no.AJRCOS.107723
ISSN: 2581-8260

How can Blockchain be Integrated into Autonomous Systems to Ensure Data Integrity and Trustworthiness, and What are the Potential Pitfalls in Decentralized Autonomous System Operations?

Arda Mesci [a*] and Efe Eren [a]

[a] *Üsküdar American Academy, Turkey.*

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2024/v17i2413

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/107723

Review Article

Received: 15/10/2023
Accepted: 21/12/2023
Published: 06/01/2024

ABSTRACT

Real-time applications always have security issues present in their ecosystem which needs to be improved. Blockchain technology can be considered as a solution that can ensure network security. The integration of blockchain technology into autonomous systems has now become an important candidate to resolve network security issues in devices that work on p2p communications. As humans become more reliant on autonomous vehicles, the importance of finding a solution to the problems linked with data security needs to be addressed to comply with international security laws. The paper aims to find the importance of blockchain technology and how it can be integrated into different classes of autonomous vehicles. In the research, an analysis of existing papers will be

Corresponding author: E-mail: gafasa07@gmail.com,ggrimzgod@gmail.com;

included along with a proposed design that can be deployed to solve the problems associated with data security using blockchain technology. Besides the improvements offered by blockchain technology, all the additional challenges associated with designing a new system and deploying this technology will be reviewed. The limitations of the works along with the future research opportunities that might open up will be presented in this paper.

Keywords: Blockchain technology; network security; autonomous vehicles work; environmental boards.

1. INTRODUCTION

Autonomous vehicles work on the basis of heaps of fresh training data, from various input sources such as GPS, Sensors, communication networks, Radars, and environmental boards to make real-time decisions allowing them to cruise and navigate the environment safely and efficiently. It is important that the data that is received is from a trustworthy source and it is accurate i.e., no additional inputs are present in the data stream that might poison the integrity of the data under consideration. The accuracy of the data would allow these autonomous vehicles to build public confidence in these technologies enabling them to pass the safety requirements and regulations allowing them to work in delicate situations where human lives are at stake. Blockchain networks offer the principles of decentralization, immutability, and transparency which is the key characteristics required for making it an objectively better solution to enable data security and confidentiality while data is being fed to these autonomous vehicles.

In this research paper, the potential benefits and the challenges of integrating blockchain technology into autonomous systems will be explored, the primary methods that can be used to enhance the data security enabled by blockchain to ensure the trustworthiness of the system to allow safer operations will be examined. The potential drawbacks along with the flaws in the current designs that have been proposed would be examined to understand the areas of improvement and opportunities that are offered by using blockchain in a system of autonomous vehicles.

1.1 Problem Statement

Autonomous systems, such as self-driving cars and drones, are rapidly improving ensuring efficiency in commute and deliveries while maintaining a standard of safety. The reliable operations of these vehicles rely on the accurate data inputs received from the different components, sensors, and networks. Ensuring the integrity of data in autonomous environments remains a challenge. Traditional methods for data validation and security fall short while dealing with continuous live data as it can be breached easily, raising a need for a system that could address the challenges associated with investigating and designing a solution using blockchain for improved security and trust in autonomous data processing and transmission.

2. BACKGROUND OF AUTOMATION IN VEHICLES

To understand the network of vehicles and levels of automation, the vehicles themselves can be further categorized into 5 stages. All of these levels are more assistive towards the driver from basic driving to fully automated vehicles. The categories of vehicles are further described in the section below.

Level 0 (No Automation): In this level, there is no automation, and the human driver is responsible for all aspects of driving. Basic driver assistance systems like ABS and traction control may be present, the driver may have electrical assistance but no proper automation.

Level 1 (Driver Assistance): Level 1 vehicles offer driver assistance features, such as adaptive cruise control or lane-keeping assistance. The system can assist the driver but attention to the road is required.

Level 2 (Partial Automation): Level 2 vehicles have more advanced driver assistance systems that can simultaneously control both steering and acceleration/deceleration. Driver monitoring is still required but the level of focus is a bit relaxed.

Level 3 (Conditional Automation): At this level, the vehicle can manage most aspects of driving under certain conditions. The driver can disengage from active control but must remain ready to intervene when the system requests. Traffic assistance and parking assistance are some examples that can be considered as level 3 automation.

Level 4 (High Automation): Level 4 vehicles are highly autonomous and can operate without human intervention in specific environments or conditions. Human oversights are not required in such vehicles.

Level 5 (Full Automation): Level 5 represents fully autonomous vehicles that can work without any human involvement. These vehicles are not bound by any conditions and can function similarly to a human driving or better [1].

2.1 Technologies Part of the Autonomous Vehicle Systems

1. Sensors: Numerous sensors are required for an autonomous vehicle to function properly, light detection and radar being the basic sensors for data input for the vehicle. Moreover, cameras and Ultrasonic sensors can be used to measure distances from other vehicles and analyze upcoming traffic. Other sensors include central compute engines and odometry sensors that can be used to monitor and maintain the alignment and speed of the car. The following diagram can help in explaining how each sensor can be used in an auto-driving vehicle.

2. GPS and IMU: The location data is received using a transmitter that processes the GPS data to determine the vehicle position and the IMUs part of the vehicle can determine the navigation accuracy, and the speed [52].

3. Control Systems: The vehicle itself is dependent on the control system, the ECUs are deployed that are responsible for the engine braking and steering, whereas the overall car electronics and mechanical vehicle features are controlled by a dedicated drive-by system.

4. Connectivity: V2X technology enables communication between vehicles and infrastructure or other vehicles. This enhances safety and can provide real-time traffic information, for instance, if multiple AVs are stuck in a traffic jam it can alert other AVs part of the system to use a different route not causing a traffic jam.

5. High-Performance Computing: AVs use powerful CPUs to process data from sensors to make real-time driving decisions. To process the large number of queries for performing complex calculations and decision making a GPU is used in the AV.

6. Machine Learning and Artificial Intelligence: AVs often use machine learning and AI algorithms to interpret sensor data and recognize objects based on their training data to make driving decisions.

2.2 Data Processing and Capture in an Autonomous Vehicle Network

The Autonomous works on the basis of data processing and manipulation, the whole process starts with data collection when high-performance sensors explained in the above section are used to collect data from the vehicle surroundings, creating a stream of raw data. Once the data has been collected, the sensor data is fused to create a representation of the environment that can help in understanding the scenario. AI and machine learning algorithms are now used to identify the objects from the fused data, the perception stage extracts the valuable information i.e. road features, vehicles and pedestrians from the fused sensor data [51].

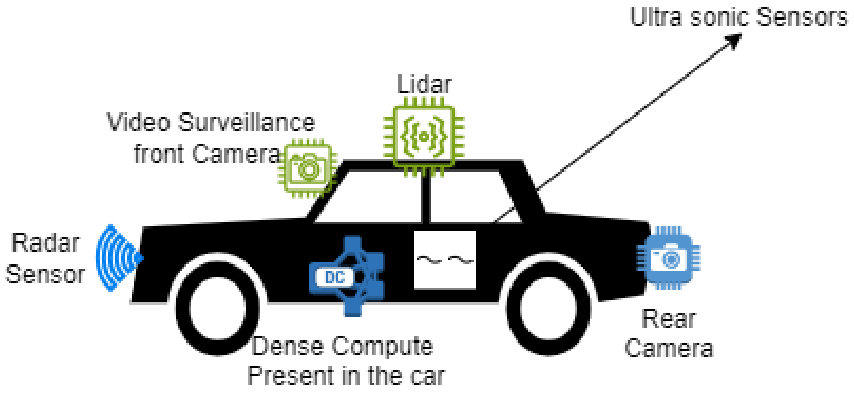

Fig. 1. Sensors in autonomous vehicles [34]

The additional networks assisting the driving such as GPS and IMUs map the data to accurately determine the vehicle's position within its environment for safety. Based on the localized data, a path can be planned that would be followed by the AV, and the acceleration, braking and driving decisions would be processed in real time using sensor fusion and high-performance computing [50]. The control system present in the dense compute engine makes sure that the vehicle follows the traffic rules and safety requirements. The controls trigger the actuators allowing the vehicle to gas and steer accordingly [49].

Data related to the vehicle's operation, sensor inputs, and decisions are typically logged and stored for analysis, debugging, and post-incident investigation. The data that is processed can be used in machine learning for improvement in autonomous driving systems.

The diagram below would help in understanding how the autonomous vehicles work, and how data is processed in the whole scenario.

2.3 Introduction to Blockchain Networks

In recent years, the integration of blockchain to solve security issues in complex network structures has now emerged as a transformative solution to address challenges related to secure data processing and storage. Traditional methods involving data handling and managing security often fall short in ensuring integrity for complex networks requiring newer solutions to manage the needs. Blockchain, initially devised as the foundational technology behind cryptocurrencies can be used to address data management and security issues [10].

The fundamental characteristic of a blockchain network that makes it a considerable option for secure data transformation is the decentralized nature and distributed ledger system in which changes are not possible unless the nodes are notified. These core features offered by blockchain make it an optimal choice for Autonomous vehicle networks as it is capable of addressing the following challenges with ease.

Ensuring data integrity is critical for AVs, as any tampering with sensor data or navigation instructions could lead to safety risks. Blockchain's immutability guarantees that once data is recorded, it cannot be altered or manipulated without consensus. Enhancing the overall reliability of data that is being used for decision-making. Autonomous vehicles often operate using a network of connected vehicles and infrastructure. Decentralization reduces the vulnerability to points of failure caused at a central point, making it more resilient to attacks [48].

Transparency ensures that AV data can be audited and traced back to its source. In the event of an accident, an audit trail can help determine the cause and responsibility enabling the regulators and insurance providers to trust the Autonomous Vehicle Systems.

Moreover, blockchain also offers smart contracts that can automate different features of AV operations, such as toll payments, insurance claims, or charging fees for electric AVs. These

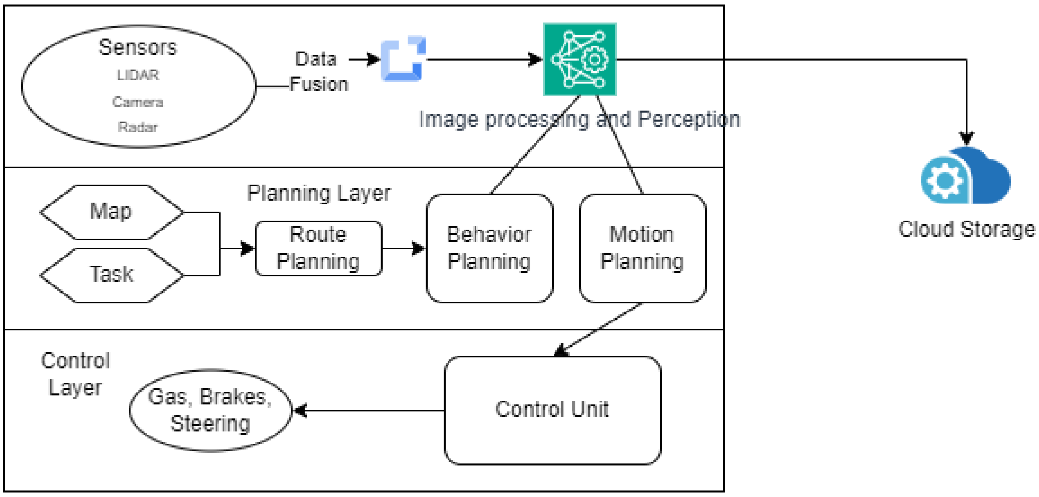

Fig. 2. Data processing in autonomous vehicles [35]

contracts can execute predefined rules autonomously, reducing the overheads associated with the administration as all of the work would then become automated ensuring compliance with regulations. Lastly, Blockchain offers data sharing that is secure and consensus among the entities involved. For example, traffic data shared through blockchain can help these vehicles optimize routes, and reduce traffic jams.

3. USE OF BLOCKCHAIN TO IMPROVE AUTONOMOUS VEHICLE FUNCTIONALITIES

The integration of blockchain technology into AV ecosystems has the potential to become a solution to data security challenges. Blockchain, renowned for its decentralized ledger and immutable record-keeping capabilities, offers a shift in the traditional method for storing and transporting data. As the technology has progressed the focus of using blockchain for Autonomous vehicles has gained attention from researchers and industry stakeholders. Numerous pieces of research under different areas linked with the functionalities of Autonomous vehicle networks have been published that offer enhanced protection and improvement in the features using blockchain [46]. The following section will focus on highlighting some papers associated with improving AV functionalities using blockchain technology. The review would highlight the challenges addressed and the methodologies proposed by scholars in this field. Moreover, it would aim to shed light on the proposed designs and frameworks that use blockchain to enhance the capabilities of autonomous vehicles. From data integrity and secure communication to optimized routing and smart contract-driven automation performance can be optimized as several studies and safety measures have been described in the literature part of this section [47].

3.1 Vehicle Ad-hoc Network Using Blockchain

A Vehicle Ad hoc Network (VANET) is a communication network among vehicles and roadside infrastructure. It enables real-time data sharing for purposes like traffic management and road safety. Blockchain can enhance VANETs by providing secure data sharing. Smart contracts can automate toll payments and traffic coordination, blockchain can also prevent data manipulation or hacking attempts in these networks [10].

A research survey conducted by Jyoti Grover in 2022 focused on highlighting several pieces of research that used blockchain to improve VAnet security. The paper highlighted the existing challenges present in the ad-hoc network and how these challenges can be addressed using blockchain. The advantages of blockchain such as its decentralized nature and immutability were highlighted in the paper, as it makes it easier for the network to record transactions. The technical issues related to the widespread acceptance of the idea were highlighted, as employing a new technique can be a difficult job in an existing market [2]. Another research was conducted by Sanjeev et Al, which focused on blockchain-based ad-hoc networks for AV applications. It highlighted research that included blockchain for facilitating secure data transfer along with sharing critical information, a literature review was presented that focused on the application of different blockchain networks and how these private networks be embedded in the system of AV for data security and transportation. The application assists the use of blockchain for building smart cities powered by Autonomous vehicles and how can cooperation between these vehicles ensure that additional overheads such as traffic congestion and authenticity of service providers be resolved by employing a distributed ledger protocol [3].

Another research was presented by Benjamin Leiding et al. in which an Ethereum-based network allows the application of rules for the users that were part of the system. The transactions that were made on the platform had to pay a price that allowed running the service on the Ethereum node [45]. The automation in the network was to improve the loyalty program of the customers by processing the transaction and providing a secure method for charging their cars. The whole Vehicular ad-hoc was designed to entertain self-driving and regular cars so that they could easily charge their electric vehicles while the payment was processed using the Ethereum blockchain, an automated subscription model was introduced to facilitate the loyal customers of the network that was deployed on Ethereum. The diagram below shows the working of the design which was proposed in the paper [4].

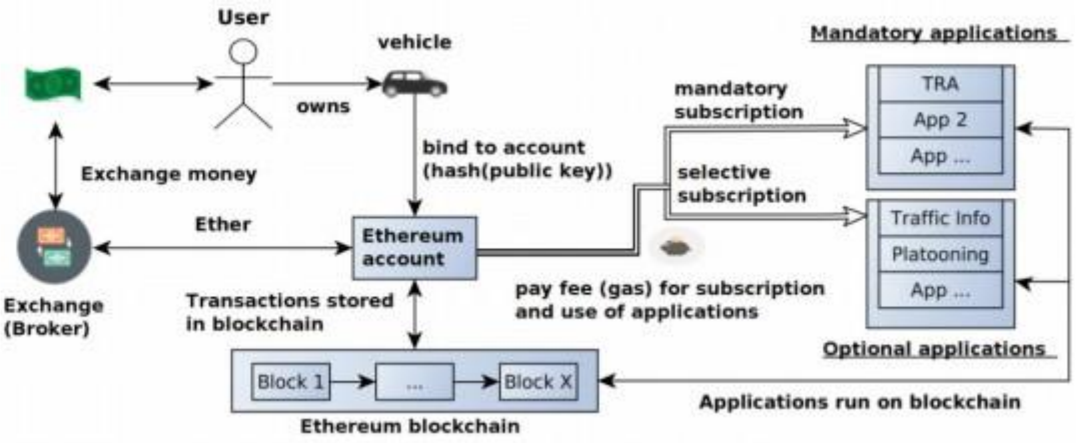

Fig. 3. Use of ethereum in autonomous vehicles [36]

3.2 Blockchain-based Design to Reduce Data Spoofing

GPS spoofing is a cybersecurity flaw in which false coordinates are generated to deceive GPS receivers and mislead them about their actual location. This manipulation of location data can significantly impact Autonomous Vehicles by causing them to navigate incorrectly or follow different routes. AVs rely heavily on accurate GPS data for precise navigation. GPS spoofing attacks can lead AVs to lose control and potentially result in accidents or unauthorized access to sensitive areas. The following diagram demonstrates how a GPS spoofing attack works [11].

Blockchain has the potential to reduce GPS spoofing significantly as blockchain records data in a tamper-resistant ledger. GPS data stored on the blockchain cannot be altered without consensus from the network participants. This ensures that once GPS coordinates are recorded, they remain unchanged and reliable. Moreover, cryptographic techniques for data verification in blockchain-based networks. GPS data is cryptographically signed, making it extremely difficult for malicious actors to manipulate or spoof location information without detection. Data on the blockchain is transparent and visible to all network participants. Any discrepancies in GPS data would be quickly identified by network users, making spoofing attempts more likely to be detected.

Research conducted by Sateesh Kumar et al. highlighted the vulnerabilities of UAVs making them susceptible to GPS spoofing attacks. The research proposes the development of an energy-intensive blockchain-based platform designed to control drone operations. This platform is intended to ensure trust and security for all parties involved in drone operations. Blockchain technology is leveraged to enhance security, data integrity, and trust within the UAV ecosystem. The primary objective of the paper was to address the vulnerability of UAVs to GNSS spoofing attacks. The research acknowledges that existing algorithms for countering spoofing attacks have limitations within the long-term errors that gather over time. To overcome this, the proposed approach introduces an innovative use of Ethereum Blockchain to create a blockchain network aimed at mitigating spoofing attacks effectively. The blockchain network is used to register components and relevant data associated with UAV operations. The ledger within the blockchain ensures data integrity and cryptographic keys, making it resistant to tampering. Geolocation data is periodically verified by the blockchain network to detect and eliminate any outliers or erroneous data [8].

Research conducted by Rajesh et al. addressed cybersecurity and privacy concerns related to autonomous vehicles in an ecosystem where smart transportation is common. The paper conducts a comprehensive analysis of threat classifications specific to autonomous vehicles. It focuses on threats that AVs may encounter. Moreover, the research also highlights countermeasures and security measures to mitigate cyberattacks on AVs. It explores potential solutions to address the identified threats while emphasizing the importance of safeguarding AV passengers. The paper introduces blockchain technology as a means to address the security and privacy concerns associated with AVs. It discusses how blockchain can offer a decentralized and secure framework that reduces the risk of single points of failure and enhances the overall security of AV operations The research further proposes a blockchain-based integrated architecture for AVs, that could mitigate security and privacy issues while ensuring service availability [9].

3.3 Use of Blockchain in Real-world Autonomous Systems

Research conducted by Choi et al. proposed a system for AV communication that improved their efficiency and security. The data packet while the transmission was encrypted, the design used FL to ensure the privacy of the data exchanged. A mathematical framework was used using a controlled blockchain network. The block size, arrival rate, and other attributes were analyzed which helped in identifying the data packet. The study further identified challenges in existing autonomous communication, and what different threats were present to wireless communication of Avs [15]. Another use case of a blockchain-based ride-hailing platform was presented in a research conducted by Srikanth et al. The network of vehicles used in their service included AVs. The design presented how efficiently blockchain was able to distribute the workload [16].

Another design was proposed by Jiang et al. in 2020 in which he discussed the use of object detection and object sharing for autonomous driving for improved performance. The design featured a blockchain network based on mobile devices for reducing the compute overhead with the help of blockchain. The reliability of the network was improved significantly by Implementing smart contracts in the system [17]. Record keeping is one of the most challenging tasks in a system where machine learning and AI are involved due to the heaps of data being processed, a research conducted by Ayvaz et al. focused on an intelligent system that uses the distributed ledger characteristic of blockchain for record-keeping in autonomous systems the study can be implemented on a system of vehicular networks as well [18]. Another design was proposed by Guo et al. in which a secure firmware was used for AVs, the security gaps were addressed in data communication by implementing data security. A data manipulation and monitoring system was proposed in the perception layer that would prioritize data security during transmission [19].

3.4 Secure Payments, Vehicle Sharing, and Freight Industry

The convergence of autonomous vehicles and blockchain technology represents a shift in the mode of transportation and logistics. As AVs continue to evolve, they are becoming safer and cheaper for the users to employ instead of human labor, the following section will look into some research on how autonomous vehicles can improve payment gateways, vehicle sharing, and mass freight transport and what impact of using blockchain-based alternatives would present on this market [20].

Research conducted by Abubakar et al. presented a paper in which a blockchain-based protocol was present for the management of vehicles that are being used by service providers as it helped in tracking the location and the active status of autonomous vehicles. For the consensus mechanism, a Proof-of-Work algorithm was selected as validation was required to overcome the demand response events. The paper provided a design in which adding new vehicles to the fleet was possible along with hiring drivers and processing their details securely in the ad-hoc network using blockchain [5].

In 2019 Dogar Ghulam conducted research that focused on the system in which an autonomous fleet of vehicles could become a part of a system that had an intelligent transport network. The fleet was responsible for providing services to the autonomous vehicles that were linked with any jobs or registered to any organization. The vehicles part of a job or a company were registered on the network which allowed the stakeholder to manage the attributes and fill in the job details securely once the vehicle was part of the Intelligent trust point mentioned in the research. The paper presented a design that could help in job scheduling, and task completion as an incentive-based fleet management system was developed that was powered by blockchain in which the worker nodes were awarded [6].

3.5 Analysis of the Use Cases

The integration of blockchain technology into autonomous vehicles presents an opportunity to address the critical challenges for management and enhancing operations helping it to innovate. As the paper has presented a number of use cases of blockchain for enhanced security and automation in AV systems, the section will provide an overview of the analysis of the presented systems [21].

3.6 Tamper Resistance

Tamper resistance in blockchain significantly improves the security of a system, it allows defense against different types of alteration in the context of any network. The core feature offered by blockchain is immutability, meaning that once data is recorded in a block and added to the chain, it cannot be altered or deleted without consensus from the network participants. This property ensures data integrity on the blockchain network. In the case of Autonomous vehicles, accurate data is critical for decision-making as navigation and safety are dependent heavily on the input [44]. Malicious actors may attempt to tamper with data, such as altering sensor readings or manipulating vehicle instructions, the consensus mechanism offered by the distributed ledger ensures that any unauthorized attempts to modify data are detected and prevented. Many Research papers have focused on delivering a tamper-free ledger system that could ensure the integrity of data while in communication. The papers provide an understanding of what notable advantages in terms of protocols are offered by blockchain that make the network resilient enough to sustain tampering attacks [7].

3.7 Lack of Appropriate Consensus Mechanism

Blockchain technology has revolutionized various industries by providing a secure means of recording and verifying transactions. However, the current consensus mechanisms, Proof of Work, Proof of Stake, and Proof of Authority have faced criticism in research papers for their limitations in maintaining decentralization and ensuring the integrity of on-chain data. The backlash is particularly increased when using blockchain applications to improve a potential supply chain. The first concern is flaws in the decentralization methods as power tends to get concentrated in PoW, PoS, and PoA mechanics if any region is providing higher computational power [22]. This centralization of control raises questions on the characteristics of a blockchain network and theoretically, this could be a flaw that any malicious user can misuse for personal gains [23]. Secondly, the alternatives to these consensus mechanisms that are proposed in the research papers, have faced criticism for their failure to provide incentives to the participant nodes. Incentives motivate participants to validate transactions and maintain the blockchain's security and integrity [6].

3.8 Future of the AV Industry

The future of autonomous vehicles promises convenience and improves security through the integration of blockchain technology. Some of the potential ways blockchain could improve the widespread use of Autonomous Vehicles are the following:

Secure Vehicle-to-Everything Communication: Blockchain can secure vehicle communication by enabling vehicles to exchange data in a tamper-resistant and authenticated manner. This ensures that information shared among AVs, infrastructure, and other connected entities remains unaltered, reducing the risk of data manipulation or cyberattacks [24]. The critical safety-related communications are kept unaltered, making the data shared within the systems resilient against malicious interference and unauthorized access [12].

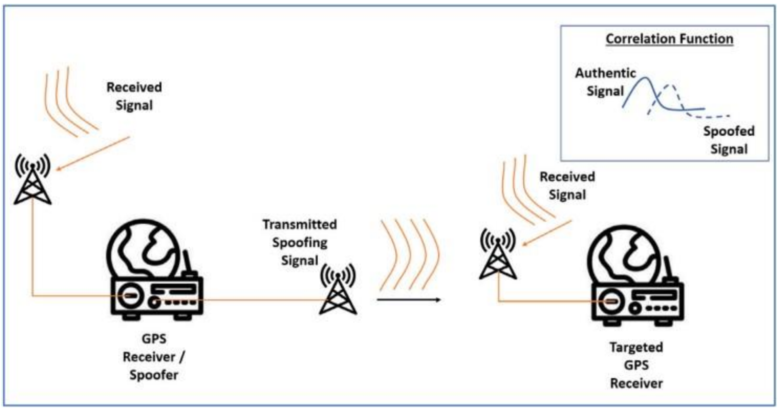

Fig. 4. GPS spoofing attack [33]

Secure Over-the-Air (OTA) Software Updates: AVs regularly receive software updates for enhanced functionality and security. Blockchain can ensure the integrity and authenticity of OTA updates. AVs can verify the source and content of updates, reducing the risk of malicious software infiltration and unauthorized modifications [25]. By preventing unauthorized software changes, blockchain can improve the overall cybersecurity posture of AVs [13].

Autonomous Vehicle Identity and Authentication: Blockchain can be used to establish and manage unique digital identities for AVs, allowing for secure authentication in various scenarios [26]. AVs can securely identify themselves to other vehicles, infrastructure, and service providers, reducing the risk of impersonation and unauthorized access. This use case enhances the overall security of AV networks by ensuring that only authenticated vehicles can participate [14].

4. ISSUES WITH THE USE OF BLOCKCHAIN IN AV SYSTEMS

If autonomous vehicles are set up correctly and used in an environment where relative technologies are also present, they have the potential to transform the commute and delivery system in busy cities. The integration of blockchain is a promising solution to deal with the security concerns that might be raised while sharing and processing data in AV systems but the integration of blockchain technologies in existing networks can be a difficult task to monitor and perform [27]. Blockchain in itself is capable of providing security and addressing scalability issues as part of any supply chain due to its decentralized nature, it also presents specific issues that need to be addressed before it is considered to be deployed on a larger scale. Some of the issues of using blockchain in AV networks are discussed in this section [28].

4.1 Scalability Issues

One of the foremost challenges in deploying blockchain within AV systems is scalability. Blockchain networks, especially public ones like Ethereum, can struggle to handle a high volume of transactions in a timely manner. This can be a concern for AV networks, where real-time data sharing and decision-making are important [29]. As Ethereum in itself is a relatively bigger blockchain network it tends to lack while processing a large number of transactions making it difficult for the AV networks to choose it as the optimal choice. AV fleets have the potential to grow in the upcoming future and if a blockchain-based network is used for storing and processing the data, it can be difficult to upscale and process a larger number of requests and it may result in a bottleneck [43]. There are solutions present to resolve the scalability issues such as using a layer-2 blockchain network. Researchers are working on designing a network that can process a large number of transactions that could potentially satisfy the scalability and bottleneck issues of the whole system [30].

4.2 Computational Issues

Blockchain transactions involve complex cryptographic operations that demand computational resources. For AVs, which often operate on resource-constrained hardware, the computational overhead of blockchain transactions can be a significant concern. AV networks rely on the data generated from sensors and microprocessors are present in the vehicles that can only compute a limited complexity problem [31]. The low processing powers of Autonomous vehicles can affect the efficiency of real-time processing and decision-making, potentially impacting safety-critical functions. The only solution presented to this problem is to optimize the cryptographic algorithms that are being used and to integrate specialized hardware that could solve some of the computational issues that any vehicle would face [5].

4.3 Lack of Knowledge

The successful integration of blockchain into AV systems requires an understanding of both domains, since both technologies are new, very few experts are present that could help in providing insights into the system flaws. The knowledge gap of both fields being new is a hurdle for the researchers that they need to overcome. Bridging the knowledge gap is essential to designing robust blockchain-based networks for vehicles. Collaboration between the domain experts of both fields is necessary to ensure that the blockchain network is implemented perfectly to align with the safety standards and regulations allowing drones and autonomous vehicles to operate freely [14].

4.4 Limited Existing Systems

Since blockchain itself is a relatively new technology it can be difficult to incorporate blockchain-based networks in the field of autonomous vehicles as no proper wide-scale implementation is present that would allow us to analyze the potential flaws of such a system and the costs along with the overheads associated with managing a system of this type. While there are notable research projects and proof-of-concept demonstrations, these have not yet reached widespread adoption in the AV industry. The limited existing systems represent both a challenge and an opportunity [32]. The lack of wide-scale deployment of architecture shows that the scarcity of real-world applications indicates that the technology is in its base state, if proper experimentation is conducted any potential regulatory flaws present in the system can be identified and fixed prior to setting it up for global use. Moreover, it also provides researchers an open ground for research as promoting research in this field would help in developing two relatively new fields of blockchain and Autonomous vehicles, as we could potentially highlight the technological and security flaws that may arise by integrating the two networks [37].

While blockchain holds promise for enhancing the security of autonomous vehicle systems, it is essential to address challenges to fully utilize the potential efficiency of the network [38]. Overcoming these issues will require collaboration between the stakeholders, testing new designs on the live data so that the regulatory flaws can be identified, and ongoing research efforts for the seamless integration of blockchain technology into the future of autonomous transportation [11].

4.5 Resolution of Security Issues

Autonomous vehicles rely on data from different sources, making them an easier target for attacks as besides the data being transferred, a large number of communications between the vehicles are also included which can potentially be hijacked by an attacker for malicious purposes. Research conducted by Vrizzlyn et al. classified the different types of attacks that are susceptible to these AVs, the broad classification included physical attacks and remote attacks, in physical attacks, code modification, and code injection were common whereas signal spoofing and packet jamming along with modification of the data transfer packets were all associated with remote attacks. The paper highlighted the ways all of these attacks can impact an AV and how blockchain could be deployed to solve most of these problems [7].

The following section will provide an overview of the ways blockchain can be used to mitigate the issues highlighted in the research.

Code Modification: Blockchain maintains an immutable ledger of code and data, making it extremely difficult to modify code without detection. Smart contracts execute the code on the blockchain, which can be used to enforce code integrity, ensuring that only authorized and validated code is executed [41].

Code Injection: Blockchain's transparency and tamper-resistant nature help prevent code injections. Only code that passes validation and consensus can be executed, reducing the risk of malicious code injection [42].

Signal Spoofing: Blockchain can enhance the security of communication and signal integrity in autonomous systems. Using cryptographic keys and digital signatures, blockchain can validate the authenticity of signals and ensure that they are not spoofed. This ensures that signals received from other vehicles or infrastructure are trustworthy [39].

Packet Jamming: Blockchain's decentralized nature can mitigate packet jamming. Decentralized networks are more resilient to localized disruptions, as data can be relayed through alternative routes. Additionally, blockchain can be used for critical traffic control to ensure it reaches its destination, even in the presence of jammed channels [40].

Modification of Data Transfer Packets: In a blockchain network, data transfer packets cannot be altered without leaving a trace. When data is recorded on the blockchain, any attempt to modify it would require consensus from network participants, making unauthorized data modification extremely challenging [8].

5. CONCLUSION

In conclusion, the integration of self-driving cars and blockchain technology can revolutionize the transport and logistics industries. Innovation in the field can make transportation secure, efficient, and reliable. The application of blockchain in autonomous vehicles can enhance data security, particularly in secure payments, and management of a large number of AVs, moreover the functionalities of the existing AVs can also be improved if blockchain-based transaction processing is applied. It enables transparent transactions, improving the overall trustworthiness of the system. Moreover, it offers the potential for services that can manage the fleet of AVs, optimize routes that have autonomous vehicles to reduce traffic congestion, and better management of freight operations. All of these aspects can help in making a smarter transportation ecosystem [4].

As these technologies continue to advance and gain wider adoption a future where more blockchain-based applications are common can be observed. Moreover, the smart supply chain that is powered by the network would also enable accessible, and environmentally friendly options for the users. While there are challenges to address, ongoing research and development in this area can offer improvements in transportation if widespread adoption is successful. In summary, the combination of autonomous vehicles and blockchain technology represents the right step in the future direction where traditional methods are ignored to promote technologically advanced solutions for cutting overhead costs and revolutionizing nthe transport system globally in the upcoming years.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

1. Narbayeva S, Bakibayev T, Abeshev K, Makarova I, Shubenkova K, Pashkevich A. Blockchain technology on the way of autonomous vehicles development. Transportation Research Procedia [Internet]. 2020;44:168–75. Available:https://doi.org/10.1016/j.trpro.2020.02.024
2. Grover J. Security of vehicular ad hoc networks using blockchain: A comprehensive review. Vehicular Communications [Internet]. 2022;34: 100458. Available:https://doi.org/10.1016/j.vehcom.2022.100458
3. Dwivedi SK, Amin R, Das AK, Leung MT, Choo KKR, Vollala S. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. Ad Hoc Networks [Internet]. 2022;137:102980. Available:https://doi.org/10.1016/j.adhoc.2022.102980
4. Leiding B, Memarmoshrefi P, Hogrefe D. Self-managed and blockchain-based vehicular ad-hoc networks. ACM [Internet]; 2016. Available:https://doi.org/10.1145/2968219.2971409
5. Abubaker Z, Gurmani MU, Sultana T, Rizwan S, Azeem M, Iftikhar MZ, et al. Decentralized mechanism for hiring the smart autonomous vehicles using blockchain. In: Lecture notes in networks and systems [Internet]. 2019;733-46. Available:https://doi.org/10.1007/978-3-030-33506-9_67
6. Pournader M, Shi Y, Seuring S, Koh SCL. Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. International Journal of Production Research [Internet]. 2019;58 (7):2063–81. Available:https://doi.org/10.1080/00207543.2019.1650976
7. Thing VLL, Wu J. Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. IEEE International Conference on Internet of Things (iThings) [Internet]; 2016. Available:https://doi.org/10.1109/ithings-greencom-cpscom-smartdata. 2016.52
8. Kumar MS, Vimal S, Jhanjhi NZ, Dhanabalan SS, Alhumyani H. Blockchain based peer to peer communication in autonomous drone operation. Energy Reports [Internet]. 2021;7:7925–39. Available:https://doi.org/10.1016/j.egyr.2021.08.073
9. Gupta R, Tanwar S, Kumar N, Tyagi S. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. Computers & Electrical Engineering [Internet]. 2020;86:106717. Available:https://doi.org/10.1016/j.compeleceng.2020.106717
10. Li XJ, Ma M, Yong YX. A Blockchain-Based security scheme for vehicular ad hoc networks in smart cities. TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON) [Internet]; 2021. Available:https://doi.org/10.1109/tencon54134.2021.9707356
11. Sung YH, Park SJ, Kim DY, Kim S. GPS spoofing detection method for small UAVs using 1D convolution Neural Network. Sensors [Internet]. 2022;22(23):9412.

Available:https://doi.org/10.3390/s22239412

12. Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z. Blockchain-Based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal [Internet]. 2017;4(6):1832–43.
Available:https://doi.org/10.1109/jiot.2017.2740569
13. He X, Alqahtani S, Gamble RF, Papa M. Securing Over-The-Air IoT Firmware Updates using Blockchain. ACM [Internet]; 2019.
Available:https://doi.org/10.1145/3312614.3312649
14. Das D, Dasgupta K, Biswas U. A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems. Computers & Electrical Engineering [Internet]. 2023;105: 108535.
Available:https://doi.org/10.1016/j.compeleceng.2022.108535
15. Pokhrel SR, Choi J. Federated Learning with Blockchain for autonomous Vehicles: analysis and design challenges. IEEE Transactions on Communications [Internet]. 2020;68(8):4734–46.
Available:https://doi.org/10.1109/tcomm.2020.2990686
16. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain and autonomous vehicles: recent advances and future directions. IEEE Access [Internet]. 2021;9:130264-328.
Available:https://doi.org/10.1109/access.2021.3113649
17. Jiang X, Yu FR, Song T, Leung VCM. Intelligent resource allocation for video analytics in Blockchain-Enabled internet of autonomous vehicles with edge computing. IEEE Internet of Things Journal [Internet]. 2022;9(16):14260-72.
Available:https://doi.org/10.1109/jiot.2020.3026354
18. Ayvaz S, Cetin SC. Witness of things. International Journal of Intelligent Unmanned Systems [Internet]. 2019;7(2): 72-87.
Available:https://doi.org/10.1108/ijius-05-2018-0011
19. Guo H, Meamari E, Shen CC. Blockchain-inspired event recording system for autonomous vehicles. Journal of Sensors [Internet]; 2018.
Available:https://doi.org/10.1109/hoticn.2018.8606016
20. Guo H, Li W, Nejad M, Shen CC. Proof-of-Event Recording System for autonomous Vehicles: A Blockchain-Based solution. IEEE Access [Internet]. 2020;8:182776-86.
Available:https://doi.org/10.1109/access.2020.3029512
21. Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A. Blockchain for AI: Review and Open Research Challenges. IEEE Access [Internet]. 2019;7:10127-49.
Available:https://doi.org/10.1109/access.2018.2890507
22. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security [Internet]. 2018 ;78:126–42.
Available:https://doi.org/10.1016/j.cose.2018.06.004
23. Chattopadhyay A, Lam KY. Security of autonomous vehicle as a cyber-physical system. IEEE Xplore [Internet]; 2017.
Available:https://doi.org/10.1109/ised.2017.8303906
24. Jabbar R, Fetais N, Kharbeche M, Krichen M, Barkaoui K, Shinoy M. Blockchain for the internet of vehicles: How to use blockchain to secure Vehicle-to-Everything (V2X) communication and payment? IEEE Sensors Journal [Internet]. 2021;21(14): 15807–23.
Available:https://doi.org/10.1109/jsen.2021.3062219
25. Yeasmin S, Haque A. A Multi-factor authenticated blockchain-based OTA update framework for connected autonomous vehicles. 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) [Internet]; 2021.
Available:https://doi.org/10.1109/vtc2021-fall52928.2021.9625372
26. Dorri A, Steger M, Kanhere SS, Jurdak R. BlockChain: A distributed solution to automotive security and privacy. IEEE Communications Magazine [Internet]. 2017;55(12):119-25.
Available:https://doi.org/10.1109/mcom.2017.1700879
27. Hasan GMM, Datta A, Rahman MA. Poster Abstract: Chained of Things: A Secure and Dependable Design of Autonomous Vehicle Services. IEEE Xplore [Internet]; 2018.

Available:https://doi.org/10.1109/iotdi.2018.00048

28. Wang JZ, Li M, He Y, Li H, Xiao K, Wang C. A blockchain based Privacy-Preserving incentive mechanism in crowdsensing applications. IEEE Access [Internet]. 2018;6:17545–56. Available:https://doi.org/10.1109/access.2018.2805837
29. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain and autonomous vehicles: recent advances and future directions. IEEE Access [Internet]. 2021;9:130264-328. Available:https://doi.org/10.1109/access.2021.3113649
30. Du Z, Wu C, Yoshinaga T, Yau KA, Ji Y, Li J. Federated learning for vehicular internet of things: recent advances and open issues. IEEE Open Journal of the Computer Society [Internet]. 2020;1:45–61. Available:https://doi.org/10.1109/ojcs.2020.2992630
31. Badr MM, Amiri WA, Fouda MM, Mahmoud M, Aljohani AJ, Alasmary W. Smart parking system with privacy preservation and reputation management using blockchain. IEEE Access [Internet]. 2020;8:150823-43. Available:https://doi.org/10.1109/access.2020.3016945
32. Lai C, Zhang M, Cao J, Zheng D. SPIR: a Secure and Privacy-Preserving Incentive Scheme for Reliable Real-Time Map updates. IEEE Internet of Things Journal [Internet]. 2020;7(1):416-28. Available:https://doi.org/10.1109/jiot.2019.2953188
33. Kamal M, Barua A, Vitale C, Laoudias C, Ellinas G. GPS location spoofing attack detection for enhancing the security of autonomous vehicles. 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall) [Internet]; 2021. Available:https://doi.org/10.1109/vtc2021-fall52928.2021.9625567
34. Lattarulo R, Pérez J, Dendaluce M. A complete framework for developing and testing automated driving controllers. IFAC-PapersOnLine [Internet]. 2017;50(1):258–63. Available:https://doi.org/10.1016/j.ifacol.2017.08.043
35. Zhu Z, Zhao H. A survey of deep RL and IL for Autonomous Driving Policy learning. IEEE Transactions on Intelligent Transportation Systems [Internet]. 2022;23 (9):14043–65. Available:https://doi.org/10.1109/tits.2021.3134702
36. Jabbar R, Kharbeche M, Al-Khalifa KN, Krichen M, Barkaoui K. Blockchain for the Internet of Vehicles: a decentralized IoT solution for vehicles communication using Ethereum. Sensors [Internet]. 2020;20(14): 3928. Available:https://doi.org/10.3390/s20143928
37. Banabilah S, Aloqaily M, Alsayed E, Malik N, Jararweh Y. Federated learning review: Fundamentals, enabling technologies, and future applications. Information Processing and Management [Internet]. 2022;59(6): 103061. Available:https://doi.org/10.1016/j.ipm.2022.103061
38. Fagnant DJ, Kockelman KM. Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transportation Research Part A-policy and Practice [Internet]. 2015;77:167–81. Available:https://doi.org/10.1016/j.tra.2015.04.003
39. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain and autonomous vehicles: recent advances and future directions. IEEE Access [Internet]. 2021;9:130264–328. Available:https://doi.org/10.1109/access.2021.3113649
40. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems [Internet]. 2018;82:395-411. Available:https://doi.org/10.1016/j.future.2017.11.022
41. Shermin V. Disrupting governance with blockchains and smart contracts. Strategic Change [Internet]. 2017;26(5):499-509. Available:https://doi.org/10.1002/jsc.2150
42. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access [Internet]. 2019;7:82721-43. Available:https://doi.org/10.1109/access.2019.2924045
43. Sanka AI, Cheung RCC. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. Journal of Network and Computer Applications [Internet]. 2021;195:103232. Available:https://doi.org/10.1016/j.jnca.2021.103232

44. Angin P, Mert MB, Mete O, Ramazanli A, Sarica K, Gungoren B. A Blockchain-based decentralized security architecture for IoT. In: Lecture Notes in Computer Science [Internet]. 2018;3–18. Available:https://doi.org/10.1007/978-3-319-94370-1_1
45. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain and autonomous vehicles: recent advances and future directions. IEEE Access [Internet]. 2021 Jan 1;9:130264-328. Available:https://doi.org/10.1109/access.2021.3113649
46. Hofmann E, Rüsch M. Industry 4.0 and the current status as well as future prospects on logistics. Computers in Industry [Internet]. 2017;89:23-34. Available:https://doi.org/10.1016/j.compind.2017.04.002
47. Fraga-Lamas P, Fernández-Caramés TM. A review on blockchain technologies for an advanced and Cyber-Resilient automotive industry. IEEE Access [Internet]. 2019;7: 17578–98. Available:https://doi.org/10.1109/access.2019.2895302
48. Luong NC, Hoang DT, Gong S, Niyato D, Wang P, Liang YC, et al. Applications of Deep Reinforcement Learning in Communications and Networking: a survey. IEEE Communications Surveys and Tutorials [Internet]. 2019;21(4):3133-74. Available:https://doi.org/10.1109/comst.2019.2916583
49. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials [Internet]. 2015;17(4):2347-76. Available:https://doi.org/10.1109/comst.2015.2444095
50. Pereira JLF, Rossetti RJF. An integrated architecture for autonomous vehicles simulation. IEEE Xcess [Internet]; 2012. Available:https://doi.org/10.1145/2245276.2245333
51. Erman AT, Van Hoesel L, Havinga PJM, Wu J. Enabling mobility in heterogeneous wireless sensor networks cooperating with UAVs for mission-critical management. IEEE Wireless Communications [Internet]. 2008;15(6):38–46. Available:https://doi.org/10.1109/mwc.2008.4749746
52. Zheng L, Zhu Y, Xue B, Liu M, Fan R. Low-Cost GPS-Aided LiDAR State Estimation and Map Building. Journal of Sensors [Internet]; 2019. Available:https://doi.org/10.1109/ist48021.2019.9010530

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/107723