Using Blockchain in Autonomous Vehicles

Chapter · May 2021

DOI: 10.1007/978-3-030-74575-2_15

Nidhee Kamble
Veermata Jijabai Technological Institute
5 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Ritu Gala
Veermata Jijabai Technological Institute
6 PUBLICATIONS **8** CITATIONS
SEE PROFILE

Revathi Vijayaraghavan
Veermata Jijabai Technological Institute
5 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Using Blockchain in Autonomous Vehicles

Nidhee Kamble, Ritu Gala, Revathi Vijayaraghavan, Eshita Shukla, Dhiren Patel

VJTI Mumbai, India
{ndkamble, rsgala, rvijayaraghavan, epshukla}_b17@ce.vjti.ac.in,
director@vjti.ac.in

Abstract. Autonomous vehicles have the potential to revolutionize the automotive industry and are gaining immense attention from academia as well as industry. However, facets of autonomous vehicle systems related to the interconnection of independent components pose vulnerabilities to the system as a whole. These vulnerabilities aren't guaranteed to be solved by traditional security methods. Blockchain technology is a powerful tool that can aid in improving trust and reliability in such systems. This paper provides a survey on how blockchain can help in improving not only security but also other aspects of the AV systems, focussing on the two major blockchain ecosystems as of this writing - Ethereum and Bitcoin. Through our survey, we have found that blockchain technology can assist in different use cases related to AVs such as providing shared storage, enhancing security, optimizing vehicular functionalities and enhancing related industries. Through this paper, we suggest directions for improvement in the sectors of Autonomous Vehicles (AV), that can be achieved with the incorporation of blockchain into Intelligent Transport Systems (ITS) or individual vehicular units.

Keywords: Blockchain, Distributed Ledger Technology (DLT), Autonomous Vehicle (AV), Connected Vehicles (CV), Intelligent Transportation System (ITS).

1 Introduction

Transport systems have evolved from being a status symbol to being a necessity in the current day and age. We cannot imagine a world without the means of transport that we have at our disposal today. With the advancement of associated technologies, we see a shift to the usage of electric vehicles and autonomous vehicles, which are expected to reduce the strict operating requirements (e.g. personal driving license), energy usage, and environmental impact. Autonomous Vehicles (AVs) are intended to not only be eco-friendly and energy-conscious, but also provide a comfortable user experience, cause an increase in consumer savings and also reduce the number of traffic deaths. With reduced private ownership of vehicles, the value of the service provided by the AV will not be based on the brand, but the quality of service and experience provided.

However, there are certain issues that need to be addressed before AVs can become ubiquitous. AVs rely on trust in the sharing and communication of information, be it within components of a single vehicular unit, or multiple vehicles interacting with each other in a Vehicular Ad-hoc Network (VANET). AVs use a multitude of technologies to make this communication possible. The state information consists of combinations of location and time references of objects for precise and continuous position tracking, with relation to other objects or vehicles around the AV. The working of the AV happens in stages - sight (sensors), communication (Vehicle-to-Everything (V2X) technology), and movement (actuators). Asmaa Berdigh and Khalid El Yassini (2017)[4] give an overview of these technologies. V2V focuses on wireless communication of relevant information between vehicles to provide a more efficient driving experience, like better safety. Vehicular utilisation of multimedia services using V2I uses cellular network infrastructures. Intelligent Transportation Systems are better managed by Vehicle-to-Roadside or V2R connectivity, using real-time updates on road statuses.

The two main tasks of AVs include perception and prediction. The shared information and data, the signals from LiDAR, GPS, etc. are susceptible to multiple security threats and attacks. Apart from the data security issues, there arises the concern of liability management in case of accidents caused by AVs. Blockchain is most known for being extremely secure for storing data, in the sense that modifying previously entered data is impossible without affecting any other blocks (in the blockchain). Blockchain technology can offer a seamless decentralized platform where information about insurance, proof of ownership, patents, repairs, maintenance and tangible/intangible assets can be securely recorded, tracked and managed. In this paper, we survey the use of blockchain technology to help tackle these issues and concerns in AVs. We also suggest room for improvement in the current vehicular functionalities, and how blockchain technology can be leveraged to improve related industries.

The rest of the paper is organized as follows: Section 2 provides an overview of blockchain and autonomous vehicles and discusses the issues in autonomous vehicles. In Section 3, current use cases which use blockchain to solve these problems in AVs are discussed. Section 4 discusses the analysis of these current use cases, with suggested directions to address them. Conclusion and future directions are presented in Section 5 with references at the end.

2 Background

We define some of the terminologies that are common across different papers that we have reviewed.

2.1 Autonomous Vehicles

The terms ‘self-driving vehicles’ or ‘autonomous vehicles’ refer to vehicles that navigate without human intervention by the integration of hardware sensors and software algorithms of intelligence.

As per the NHTSA [29] guidelines, autonomous vehicles have the following levels:

- Level 0: No Automation
  This level consists of completely manual driving.
- Level 1: Driving Assistance
  The vehicle can assist with steering or accelerating/braking but not both simultaneously. A driver is required to drive the vehicle.
- Level 2: Partial Automation
  At this level, steering and accelerating/braking can be performed simultaneously but the driver must monitor the driving environment and perform the remaining driving operations.
- Level 3: Conditional Automation
  At this level, the car can perform all aspects of driving, but a driver must be present in case the system requests so.
- Level 4: High-Driving Automation
  This a fully functional driving system that requires no assistance and does not need the driver to pay much attention
- Level 5: Fully Autonomous (Unconditional)
  In this system, human occupants are just passengers and not drivers. This is the highest level of automation.

For the purpose of this paper, we will consider autonomous vehicles to be those of Level 3 and higher. AVs use a multitude of technologies integrated with each other and thus have various components. These components all have different uses but should, as explained by Alberto Broggi et al. (2008) [7], contribute to giving five major functionalities to the AV:

1. Vehicular state estimation (static/dynamic);
2. Information retrieval about the surrounding (static/moving objects);
3. Information collection on driver/occupant state (to prevent casualties or report them);
4. Communication with other vehicles and other infrastructure (traffic lights or stop signs);
5. Enabling access to a Positioning System (perhaps GPS).

2.2 Technologies used in AV Systems

Perception in AVs happens through raw information inputted through Vehicle-to-Vehicle (V2V) components or sensors. The critical process of obstacle detection (to detect static and moving objects) is done in the perception task. Based on perception, AVs act in accordance with maps, weather, traffic data, topological conditions, and surrounding vehicles positions. Ultrasonic, LiDAR (light detection and ranging), RADAR (radio detection and ranging), and cameras aid in perception. Ultrasonic sensors are mainly used in parking sensors and radar is only used for extremely long-distance tracking used for Adaptive Cruise Control (ACC). Cameras are generally only used to find lane markings and to display signs such as speed limits on the dashboard of a vehicle. The combination of RADAR and LiDAR can capture images and transfer them through electrical interfaces. The in-vehicle micro-computer will process the information acquired and analyse the data to make driving decisions by making an almost instantaneous 3D map of the area around the vehicle. The use of the created 3D map, in combination with GPS, is used for tackling the problem of identifying an ego vehicle's position, a critical piece of information required for autonomous vehicles.

Accurate perception is the key to ensuring safety in an AV. Perception aids AVs to make decisions spontaneously, using quantifiable variables that estimate environmental factors (surrounding vehicle's location/condition, pedestrians locations/conditions, vehicle occupant's conditions, maps, weather and traffic data). It uses many sensors like GPS (Global Positioning System) LiDAR (Light Detection and Ranging for accurate reliable and cost-effective mapping), RADAR (Radio Detection and Ranging used for Adaptive Cruise Control [ACC]) and ultrasonic sensors (used for Parking). Obstacle Detection (a crucial task) is accomplished using Computer Vision (using a camera that transmits captured information to in-vehicle microprocessors). Some suggested techniques include KITTI for pedestrian and cyclist detection, PSPnet by Zhao et al. (2012) [28].

Technologies used for AVs build upon the native functions of traditional, level 0 vehicles to optimise them specifically. Correa,et al. (2017)[9] propose a design for a parking system for AVs, implemented on a Vehicular Sensor Networks with minimal infrastructural overhead. The research simulates a parking layout using mathematical models, defining its accessibility rate in terms of parking place availability for AVs. Geng and Cassandras (2012)[11] propose methods used by traditional AV systems for navigation in geographical scenarios, like VANETs, ultrasounds, in addition to oft-used GPS and LoS (Line of Sight) with their analyses. Received Signal Strength (RSS), the Time of Arrival (ToA) and the Time Difference of Arrival (TDoA) both in anchor-based solutions and in cooperative approaches, are used in GPS-denied environments. One of the notable mentions in enlisting previous research is of Roadside Units (RSUs), used to utilise unused resources of AVs - like a rechargeable battery and storage capacity - using IPARK [28], a system for guided parking over infrastructure-less VANETs.

2.3 Vehicular ad-hoc Networks (VANETs), Intelligent Transport Systems (ITS) and Connected Vehicles (CVs)

A 'Vehicular Ad-hoc Network (VANET)' is a group of stationary and moving vehicles connected via a wireless network. An 'Intelligent Transport System (ITS)' is an infrastructure where vehicles are connected with each other using smart devices. The term 'Connected Autonomous Vehicles (CAVs)' refers to a group of autonomous vehicles that may connect to the internet and provide improved data sharing in the form of risk data, sensory and localization data and environmental perception.

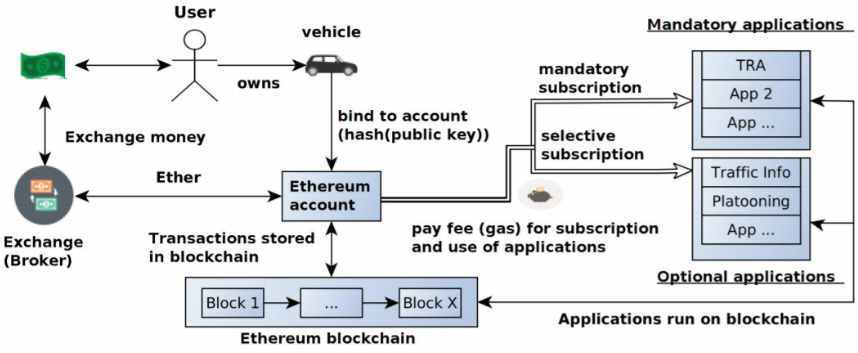

Fig. 1. Ethereum-based service provision and rule enforcement in self-managed VANETs [5]

Figure 1 is the depiction of how network users can access and utilize deployed applications. Each participant is registered on the blockchain (Ethereum blockchain) and has an address (Ethereum address). Benjamin Leiding et al. [5], made possible by Ethereum Blockchain, applications for enforcement of provision rules regarding services are available to all the users of the network. The cost of running the chain is self-regulating, which happens because of a price being paid for each transaction in the form of Ethereum - gas. Consequently, each automobile pays a fee for each transaction made. This concept of making cars pay for the infrastructure and computing has a limitation: The most loyal customers (who use the charging station more frequently), incur more penalty. Although this means that there is a big incentive for providing RSUs and other essential tools, the fee goes to miners and computational services for mining transactions and mining-pools.

2.4 Blockchain

A blockchain[6] is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree)[21]. Blockchains can be either public (everyone can view and verify the data), private (governed by a single entity), consortium (semi-private, shared across different organizations with restricted access) or hybrid (features of both private and public blockchains). The most popular blockchains are the Bitcoin network and the Ethereum blockchain.

The key properties of blockchain are:

1. Decentralized: There is no centralized authority, as the blockchain is not owned by a single entity.
2. Secure: The data stored is in encrypted form using hash functions, making it secure.
3. Immutable: Data once inserted into the blockchain, cannot be changed due to the structure of the blockchain itself, thus making it tamper-resistant.

4. Transparent: Since it is a distributed ledger, the data can be accessed by anyone on the blockchain.

Components of a blockchain are:

1. Node: User or computer within a blockchain network
2. Transaction: the smallest building block of a blockchain system
3. Block: a data structure used for keeping a set of transactions which is distributed to all nodes in the network
4. Chain: a sequence of blocks in a particular order
5. Miners: specific nodes which perform block verification and add nodes to the chain
6. Consensus: a set of rules and regulations mutually agreed upon by all the nodes in the blockchain

A *'state channel'* is an off-chain channel through which two or several blockchain users can atomically exchange blockchain-compliant information to be added on-chain later when closing the channel. The channel is closed on either completion or failure of such atomic transactions (transfer or exchange).

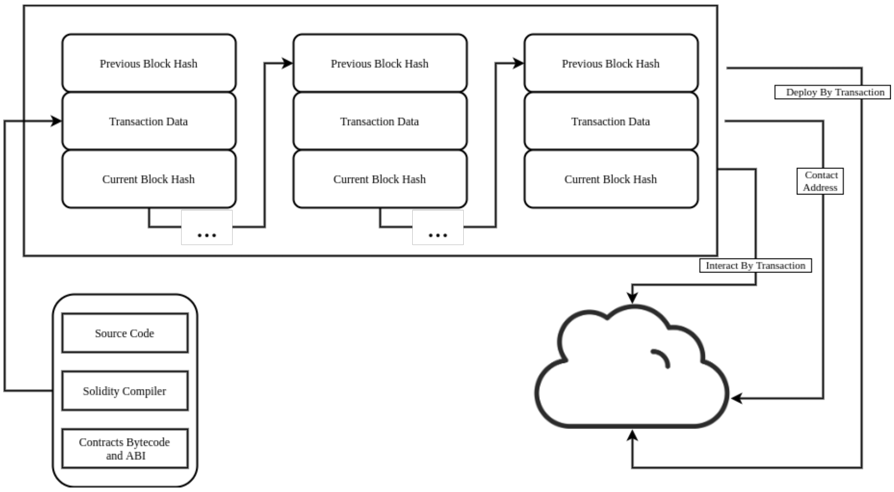

Fig. 2. Structure of Blockchain

2.5 Scalability with Blockchains

Another issue with current IoT networks is that of scalability. As the number of devices connected through an IoT network grows, current centralised systems to authenticate, authorise and connect different nodes in a network will turn into a bottleneck. This would necessitate huge investments into servers that can handle a large amount of information exchange, and the entire network can go down if the server becomes unavailable.

In public blockchains such as Bitcoin, very time and computationally intensive mining-based consensus mechanisms are often used to establish trust between entirely anonymous parties. Thus large transaction times result which results not only in poor performance but also poor scalability. This leads to the creation of side chains so as to offload the transaction processing from the main chain.

In cases of business to business (B2B) and business to consumer (B2C) interactions, the use of private and permissioned blockchain is preferred. Private blockchains have a reduced number of nodes, which results in a far faster consensus mechanism and in general improves scalability and performance.

There are now new blockchains coming up, termed as blockchain 3.0, which are based on the principles of DLT. These blockchains improve scalability and performance by the use of DAG (Directed Acyclic Graph) and novel validation and voting mechanism. [14]

Another mechanism proposed by Lyubomir Stoykov et al. [18] is the VIBES architecture. VIBES uses configurable input parameters like network-information and number of miners, to provide a flexible solution. The simulator provides information about throughput and cost-per-transaction. To bypass a majority of the heavy computations for large scale applications, the paper suggests improving scalability via fast-forward computing. This helps complete simulations before time. Nodes try to estimate computational costs and ask for permission to fast forward. After green-lighting the operation, the orchestrator declares the operation complete and skips forward.

2.6 Consensus Mechanism

A consensus mechanism is used to tackle fault-tolerance. It is used to arrive at a group consensus regarding the data to be added to the network or the state of the network. The famous consensus mechanisms are Proof of Work (used by Bitcoin, Litecoin, and Monero), Proof of Stake (used by Ethereum 2.0 and Dash), Proof of Vote and Proof of Burn.

Ole Meyer et al. (2018) [23] propose a consensus algorithm for autonomous vehicles that does not rely on a central authority for control and monitoring. An autonomous entity in the system, called an agent, can predict dangerous situations and trigger a protocol for resolving or avoiding it. Parallel solutions generated simultaneously might lead to suboptimal solutions. In such cases, priority is allotted based on a parameter specific to the situation. For example, to avoid an impending collision between two autonomous cars, the car about to reach a place first should slow down and the other halt, instead of both the cars halting. The parameter for priority ordering can also be a characteristic that can be independently determined by both the parties, the information regarding which can be easily obtained by them. The protocol must yield invariant solutions. This ensures that the consensus can be achieved even without communication between the participants, reducing overhead for exchange over a network and hardware prerequisites for facilitating it.

2.7 Use of Blockchain to Ensure Security

An important worry within autonomous vehicles is the high dependence on IoT devices. These IoT devices are often vulnerable to Distributed Denial of Service (DDoS) attacks. Blockchain technology can prove to be extremely useful in this aspect. Being decentralized, blockchain eliminates single point of failure based attacks, and also provides a medium for auditable and traceable changes. Further, blockchains provide help with authentication and identification of devices over a distributed database.

2.8 Problems and Improvements Associated with AVs

With the expectation of AVs becoming a norm, the number of AVs on the road will go on increasing. As self-driving vehicles are equipped with more sensors and network connectivity than non-autonomous ones, the number of security vulnerabilities and thus, attack surface of an AV is undoubtedly increased. Adversaries today are becoming increasingly skillful. [27] These skills coupled with feasible low-cost offensive devices can enable them to break into car security systems easily and in the worst case allow unauthorized complete control of the vehicle or data tampering. Further, with autonomy, comes lack of accountability. When autonomous vehicles are involved in accidents (collisions between themselves, or collisions with conventional vehicles, pedestrians or other objects), how should such events be recorded for forensic purposes to determine liability? In addition, how could such recorded events be verified, trusted, and not tampered? Such issues become critical when there exist incentives for different parties involved to tamper with the recorded events to avoid punitive penalties.[8]

The expected functionalities of autonomous vehicles could be enhanced due to the integration of vehicle sensors and blockchain. The revolution of autonomous vehicles along with the aid of blockchain technology could affect closely related industries too. For instance, the use of blockchain in these AVs could negate the need of middle parties, be it brokers in fleet management systems or ride sharing companies like Uber.

3 Use of Blockchain in AVs

3.1 Decentralised storage and security mechanism

On surveying, we noticed that blockchain can serve as shared storage to facilitate accident management and also can be used to tackle security attacks on AVs. Below is the detailed summary of the two cases.

Accident Reporting and Verification. Hao Guo, Ehsan Meamari and Chien-Chung Shenis (2018) [13] focus on event recording mainly for accident forensics. They propose Proof of Event as a consensus mechanism, a recording and broadcasting mechanism for the events that happen. The collections of records are accepted as new nodes to the blockchain depending on the credit score of the verifier and participant nodes (vehicles). The credit score is a measure of how ‘trusted’ a vehicle is. This includes being a witness or a verifier to an accident. Since there is no tangible award provided by the Proof of Event protocol, credit scores are an attempt at incentivisation. Higher credit scores may reflect as lower insurance premiums on the vehicle. Further, they adumbrate the protocols necessary for implementing the system. Proposal for a reward-based smart vehicle data-sharing framework is proposed by Singh (2017) [20] for intelligent vehicle communication using blockchain. The concept is abstract and introduces a blockchain network model for communication over a VCC (Vehicular Cloud Communication) for reporting safety-critical incidents and (the possibility or occurrences of) hazards to drivers. It uses Proof of Driving as the consensus mechanism where the incentivisation is provided by crypto tokens in the form of IVTP (Intelligent Vehicle Trust Points). Narbayeva, Saltanat et al. (2020) [22] present a mathematical foundation to use blockchain technology for increasing information integrity by sending parameters of the current state of each vehicle, verified by the signals of neighbouring vehicles. The authors have developed a tracking system for car actions using the blockchain system based on the Exonum platform.

Security in Connected Autonomous Vehicles. AVs are more susceptible to malicious cyber attacks due to increased Vehicle-to-Vehicle (V2V) communication that occur via VANETs.[15] Vrizlynn L.L. Thing et. al., (2016) [26] classify attacks possible on autonomous vehicles. The two classes of attacks are physical access and remote access attacks. Physical access attacks include invasive attacks like code modification, code injection, packet sniffing, packet fuzzing and in-vehicle spoofing. Remote access attacks include external signal spoofing and jamming. The security issues with respect to CAVs are addressed in the paper by Rathee, Geetanjali, et al. (2019) [25]. They have proposed a blockchain-based solution where each IoT device (sensor/actuator) and the vehicle is registered to the network before they start acquiring any of the services. Initially, the vehicular number along with IoT device data will be stored on the blockchain. In view of the high amount of computation power and time that will be needed for the large amount of data generated further, they propose that only the IoT devices store relevant information to the blockchain, which can also then be analyzed. Any alteration on information can then easily be detected as it will alter previous records as well. To begin with, there is no solid mechanism to keep a track of compromised sensors which are a crucial part of the ecosystem of CAVs. Additionally, in a scenario where CAVs are used for a cab-booking service, technical experts may hack into the system and change important information like accidents the car has been associated with, for personal gains. Data falsification attack is a primary security issue where vehicles in a network rely on information received from other vehicles.

The standard encryption schemes like AES will not be feasible for CVs since they produce a large amount of data as mentioned by Jolfaei, A., & Kant, K (2019) [16]. Key management could become an issue for each device and they cause a potential weakness in the system.

Anil Saini et al. (2019) [3] propose a new blockchain network in order to accomodate priority vehicles. The regular blockchain networks have many drawbacks. Some limitations include dealing via crypto-currencies (instead of trust messages/events) and higher latency (reduced by using 2-levels in the proposed network). The proposed network would use 2-levels and the first level will consist of authorised nodes (placed in different areas). If an RSU node wants to become a participant of the network, it must first get verified by the authorised nodes. The second level consists of registered RSU nodes. The vehicles register with its nearby RSU, after which the RSU verifies the identity of the vehicle and stores it on the blockchain. The RSU also receives information generated by the vehicles, like traffic congestion, accident-related information, etc. This information is distributed to the neighboring roadside nodes for it to be validated in the blockchain network of RSUs. There exists no central authority in this entire process, thus enabling decentralization.

3.2 Blockchain to Improve AV Functionalities

While surveying we noticed that blockchain can improve an autonomous vehicle's functionality in the ways mentioned below.

Verifying Vehicle Lifecycle. The automotive supply chain industry can be quite complex, ranging from government regulatory parties, manufacturers, suppliers, and vendors to spare parts suppliers. *P. K. Sharma, N. Kumar and J. H. Park (2019)* [24] delineate into each phase of the automotive industry (regulator, manufacturer, dealer, leasing company, user, maintenance, scrap) and explained the benefits of using smart contracts for the digitization of this process. They give a complete overview of the process. They propose a blockchain and smart contract-based scalable distributed framework model for the lifecycle tracking of vehicles. A miner node selection algorithm based on the Fruit Fly Optimization algorithm (FOA) has been suggested to avoid the mining process during the block generation carried out by a unique miner pool and limited by miners.

Insurance and Payments. M. Demir, O. Turetken and A. Ferworn (2019) [19] propose a tamper-free ledger of events as an insurance record of motor vehicles for provision of evidence in the event of a dispute. This can include all aspects of insurance transactions. The system uses a permissioned blockchain (Hyperledger based) for obtaining, sharing and verifying insurance records will help stakeholders as a reliable sharing platform and a ledger of events. Alejandro Ranchal Pedrosa and Giovanni Pau (2018) [2] provide a detailed algorithm for the payment of a refueling scenario in autonomous vehicles using Ethereum State Channels. The use of these state channels is aimed at supporting instant and reliable trading of information, goods and currency.

Charging Stations and Power Requirements. Alejandro Ranchal Pedrosa and Giovanni Pau (2018) [2] suggest using Ethereum State Channels as an unforgeable recording, flexibility and scalability for Machine to Machine (M2M) transactions in charging stations. A detailed algorithmic approach has been developed to cover all pertinent use cases which could occur during the interactions between the AV and the charging station. The use of these state channels is aimed at supporting instant and reliable trading of information, goods and currency.

Fabian Knirsch et al. (2017) [17] provides a protocol for allowing the driver of an electric vehicle to find the cheapest charging station in a given location radius. The bids sent by different charging stations are stored on a blockchain to provide transparency and verifiability. The phases of requesting and serving of corresponding charging locations have been elaborated upon.

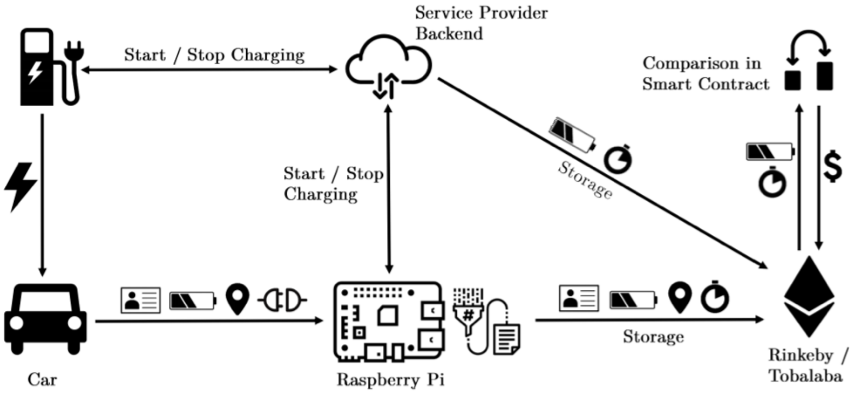

Fig. 3. Details of how a charging event would occur and the entities/tasks involved in this process [10]

Instead of the Vehicle Engine Control Unit, Raspberry Pi is proposed by Felix Kohlbrenner et al. (2019) [10] This can be used to collect the required data and utilize the real vehicle bus data. This provides a similar environment with similar restrictions. Once the charger is plugged in, the event of "start charging is triggered". Various vehicle information is recorded and saved in a hash (updated when required), this upholds the trustworthiness of the charging system, but user-data is saved off-chain due to privacy concerns. With the help of a signed transaction, the charging status is stored on the Ethereum Blockchain. A payment request is triggered when a certain charging threshold is reached (any means of payment can be used).

Parking for AVs. There are intelligent parking management architectures that are suited specifically for the system heterogeneity of AVs. Jennath, H. S. et al. (2019) [15] propose a blockchain-based solution for creation of parking pools using a non-fungible token system for rentals of users' unused land for a stipulated amount of time with little or no legal hassles. Additionally, this method leverages income from unused property, which is an added advantage. Smart contracts over blockchain enforce the contractual agreement between the participants ensuring financial transparency in the proposed system. This system can be implemented in the present scenario for traditional cars, and extended to AVs in the future. With increase in levels of automation, some decision-making tasks - such as inclusion of vehicles in parking pools - may also be taken by AVs instead of humans.

3.3 Optimizing Related Industries

The AV industry is not standalone and affects other related industries, like transport and freight, in terms of human involvement, inter-industry dependency, and consumer experience. Advancements in AV sectors by integration of blockchain will, by extension, have an effect on these industries. Additionally, it can also be used to address corresponding improvements.

Vehicle Sharing. Using Proof of Work consensus algorithm for the validation of Demand Response, Abubaker Zain et al. (2019) [1] present in this paper a block-chain based mechanism to provide users with real-time availability of on-network intelligent vehicles. In the system, vehicles can provide services, as part of a fleet on a single Intelligent Transport System (ITS) network. This paper uses the Proof of Work consensus algorithm for the validation of Demand Response (DR) events.

Freight Industries. *Dogar, Ghulam and Javaid, Nadeem (2019)* [9] proposed a system in which vehicles that belong to a fleet can be part of a single Intelligent Transport System (ITS) network, providing services to all the autonomous vehicles and carrying out their jobs normally. Special vehicles that are part of a fleet will be registered with their respective organization only by registering with the Intelligent Vehicle Trust Point (IVTP). To facilitate the assignment of tasks and task-completion, an incentive-based blockchain-based Fleet Management System (BFMS) is proposed. Such a system can prove extremely useful in the cases of parking and charging where queries (for bids) can be used to provide the intelligent-vehicle options, from which the best can be chosen.

4 Analysis

The analysis of the previous section is divided into the following categories.

4.1 Relevance of Blockchain

DLTs vs Blockchain. While many use cases of AVs rightly require blockchain, there has been a trend to misuse blockchain as a technology, which means using them without a proper consensus mechanism. Many use cases simply require storage immutability, which can easily be provided by permissioned Distributed Ledger Technologies (DLT), and using a blockchain in such cases is not exclusively required.

Tamper Resistance. Certain research papers focus on 'tamper-free' ledgers to ensure data integrity over AV communication. Distinguishing the terms tamper-free, tamper-tolerant, and tamper-resistant, has implications on understanding what the technology provides. A blockchain is tamper-resistant: It resists (the possibility of) being modified, by design. In the possibility of a modification, its protocols are resilient enough for it to resist the effects of tampering. On the basis of our study, the terms tamper-free and tamper-tolerant point at something that is possible to be tampered with, the effects of which can be rectified later - by rollback, late control, or implementational modifications.

Lack of Appropriate Consensus Mechanisms. The prevalent consensus mechanisms for blockchain - Proof of Work, Stake, and Authority - are criticized in a few research papers for their inability to maintain the decentralization of control in the blockchain, eventually resulting in the concentration of power in the regions with higher computational power and resources, respectively. However, proposed alternatives to these, as stated in the papers, lack incentivization. For shared records of AV lifecycle and logs for vehicle sharing, each participant on the chain should be able to verify the on-chain information by the virtue of its existence alone. Since the verification results from the consensus mechanism, which operates only on the on-chain data, it follows that the data source must also be on-chain. These data sources must be intrinsic to the blockchain for verification to happen as a part of the working. Unless it is made possible to embed some kind of metadata in the AV records that make its source on-chain, the verification remains external in all systems currently proposed, rendering the consensus mechanism of little use by itself. Looking at the potential of blockchains as an ecosystem, we opine that in such use cases it remains underutilised.

4.2 Issues with the use of Blockchain in AV Systems

Scalability. The concept of transparency in blockchain is based on the fact that each node in the blockchain stores a separate copy of the entire data present on the blockchain. This isn't feasible for AVs due to rapid generation of large amounts of data. An increase in the number of vehicles (nodes) will add to this data, decreasing the efficiency of the system. A possible solution would be to store only the bare minimum information on the blockchain and store the rest of the data on a shared file system like IPFS.

Feasibility of Computation. Blockchain consensus mechanism requires a large amount of computational power. These computations may not be feasible on AVs which might in turn result in low throughput of the system, by causing an increase in latency.

4.3 Future of Related Industries

Exploring the current proposals and analyzed possibilities, advancements in the AV sector with blockchain or DLTs would improve the experience around providing insurance, with extended services around providing a clean driving record, or for vehicle lending or sharing. DLTs will facilitate mainstream adoption of car sharing by scheduling and matching rides without the need for a middleman. Distributed ledger technologies can allow information on vehicle availability to be made publicly accessible so that users and car owners can match journeys easily.

Blockchain could also aid in effective supply chain management in the freight industry. However, simply using blockchain technology does not ensure the effective transport and delivery of goods. Tampering with RFID tags attached to goods and cases of smuggling can lead to incorrect information stored on the blockchain, which voids the use of blockchain in the first place.

4.4 Using Cryptocurrency

With vehicles becoming driverless, the issue of payment can be tackled by providing a payment method that is intrinsic or facilitated by the blockchain infrastructure itself. This would mean that payments for parking and toll, payment can be done using cryptocurrencies.

However, the use of cryptocurrencies will be unfavourable in case of a 51% miner attack. However, this kind of attack requires massive computation on popular blockchain platforms like Bitcoin and Ethereum. In the case of smaller blockchains, it is not difficult to amass the computational power for these attacks, and such an attack could very much be possible. Therefore, autonomous vehicles must be very careful before selecting their desired blockchain for payments.

Further, the volatility of cryptocurrencies is a significant limitation for the adoption of blockchain-based payments especially if it is to be integrated as a long term solution with autonomous vehicles. This volatility is a consequence of state-specific fiscal policies and standards, and not an innate property of cryptocurrencies itself. An optimistic approach might predict that this stability increases; an overly optimistic approach might say that fiat currencies shall be measured in terms of cryptocurrencies in the future (converse of the present scenario). A practical approach is to gauge the market behaviours due to fiat-crypto exchange interactions and adoptions and see how one system can be used to address the weakness(es) of another.

4.5 Resolution of Security Issues

It is not possible to address all security attacks mentioned in Section 3A, but blockchain-based solutions can be implemented to prevent certain security attacks. The issues of code modification and code injection can be reduced by incorporation of a permissioned blockchain. This will prevent the unauthorized access to the AVs and thus reduce the possibility of such attacks. External signals like GPS and LiDAR signals, can be verified by the use of blockchain to prevent external signal spoofing attacks.

Table 1 summarizes the summarizes the advantages and disadvantages of the proposed methodologies in the use of blockchain in AVs.

Table 1. Advantages and Disadvantages of methodologies in the use of AVs

Reference No.	Use Case in AVs	Purpose	Advantage	Disadvantage
[13]	Accident Reporting	Decentralized storage	Using the data of events from various sources and the generated Hash digest, obtained using the “Proof of Event” mechanism (with Dynamic Federation Consensus).	Proposed mechanism will not work optimally in areas which are sparsely populated as a result of which there may not be verifiers or witnesses.
[20]	Accident Reporting and Verification	Decentralised storage and security mechanism	The proposed intelligent vehicle trust point methodology provides fast and secure communication between intelligent vehicles and stores details about the history of the communication which can be beneficial during accidents.	The current proposed methodology does not cover multiple vehicle communication as of yet.

[22]	Security in Connected Autonomous Vehicles	Decentralized storage and security mechanism	The proposed solution uses the standard ECDSA for confirming transactions and micropayments, which makes it a secure approach. The proposed solution facilitates micropayments in times of emergencies, wherein one car needs to be prioritized over another.	The solution states that the current state of each vehicle will be shared with its neighbours in its vicinity, spanning over a 100-150m radius. However, there is no mention of what the current state of each vehicle would include, and what the messages to neighbouring vehicles would encompass either, to be shared over the blockchain.
[15]	Parking for AVs	Blockchain to improve AV Functionalities	The proposed solution uses non-fungible parking tokens for unused land, and provides transparency and trust in the process through the use of a blockchain system.	The proposed solution does not mention how the blockchain combined with an IoT system will be scaled, as an increase in the number of blockchain nodes will most probably decrease the efficacy of the system due to increased computation.
[25]	Security in Connected Autonomous Vehicles	Decentralized storage and security mechanism	The proposed methodology tracks the information provided by IoT devices, thus ensuring continuous monitoring of data, which provides	The proposed solution mentions the storage of all the data received from IoT devices onto a normal database at first, followed by a

			security and transparency at each step.	permanent storage on the blockchain. This seems unnecessary, as duplicating the data, which will be generated in large amounts, will lead to redundancy.
[18]	Security in Connected Autonomous Vehicles	Decentralised storage and security mechanism	The solution proposed uses a lightweight permutation scheme suitable for encrypting real time data generated by weak devices.	The proposed solution performs well against the given test cases but needs to be tested more extensively.
[24]	Verifying Vehicle Lifecycle	Blockchain to Improve AV Functionalities	The proposed blockchain base distributed framework for automotive industry allows for significant time and cost savings and enabling manufacturers and suppliers to protect their brands against counterfeit products.	For such a framework to exist in a smart city, there needs to be a standardized regulatory framework.
[19]	Insurance and Payments	Blockchain to Improve AV Functionalities	The use of blockchain for vehicle insurance ledger allows sharing the vehicle insurance records in a transparent manner and allows for the collective nature of contribution as participants' may not trust each other.	Similar to the previous paper, this proposed solution too would require some governance of the blockchain, perhaps in the form of a consortium.
[2]	Insurance and Payments	Blockchain to Improve AV Functionalities	The most promising advantage of this proposed architecture	Although the use of state channels in the proposed

			is the possibility of blockchain compliant, fast payments due to the use of state channels.	solutions is beneficial, there are associated risks with state channels related to set up and obliviousness of the parties involved, such as improper time-locks, coin theft, data loss or forgetting to broadcast transactions on time.
[17]	Charging Stations and Power Requirements	Blockchain to Improve AV Functionalities	The proposed solution is a blockchain based protocol for finding the nearest and cheapest charging station, ensuring the privacy and confidentiality of the consumer.	The solution requires a specific number of properties to be met by a blockchain, for it to be used, and scalability remains the most discerning issue.
[1]	Vehicle Sharing	Optimizing Related Industries	The proposed system allows whole information about the route to be revealed to the customer by real time traffic information. Further, there is a reduced transaction cost due to the mechanism of peer to peer car sharing which removes the need for any bank or any reliable authority.	The proposed system assumes a driverless environment. As such issues like accident verification and payment of tolls need to be tackled. This proposed architecture can be combined with other proposed architectures mentioned to create a robust.

[9]	Freight Industries	Optimizing Related Industries	The paper proposes how different fleets of special vehicles would carry out operations for different organizations for different purposes in a blockchain enabled Intelligent transport.	Testing has been done for a small fleet size (120). Thus, the scalability of the proposed system is a matter yet to be determined.
[10]	Charging Stations and Power Requirements	Blockchain to Improve AV Functionalities	Decreased latency (30% faster). Reduced cost of Operation	Approach violates the principle of the separation of concerns.

5 Conclusion

Blockchain, with its key characteristics of decentralization, immutability and transparency, has true potential of being adopted in AVs due to its ability to seamlessly tackle many issues that AVs are expected to have. In this paper, we have provided a comprehensive literature review on the current use cases of blockchain technology in autonomous vehicles. We first provided an overview of autonomous vehicles followed by an overview of blockchain architecture. We then investigated the current use cases by partitioning them into three broad groups on the basis of usage of blockchain in Autonomous Vehicles - as a decentralized storage and security mechanism, for Improving AV Functionalities, and for optimizing Related Industries. Finally, we provided a brief analysis of these use cases, discussing their relevance and issues. As a future scope, Bitcoin's Lightning Network (LN) can be implemented for payment channels or for primary payment rail coordination for freight chain activities. LN is a second-layer solution enabling Bitcoin to scale to over a million transactions per second (compared to 7 of Bitcoin) with payments routed peer-to-peer within milliseconds. As our analysis suggests, there is significant scope for the integration of blockchain technology in AVs, and our survey particularly suggests that more research needs to be conducted in the use of blockchain for the different facets of AVs mentioned in this paper.

References

1. Abubaker, Zain & Gurmani, Muhammad & Sultana, Tanzeela & Azeem, Muhammad & Iftikhar, Muhammad & Javaid, Nadeem. (2019). Decentralized Mechanism for Hiring the Smart Autonomous Vehicles using Blockchain.
2. Alejandro Ranchal Pedrosa and Giovanni Pau. 2018. ChargeltUp: On Blockchain-based technologies for Autonomous Vehicles. In Proceedings of the 1st Workshop on

Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18). Association for Computing Machinery, New York, NY, USA, 87–93.

3. Anil Saini, Shreyansh Sharma, Palash Jain, Vikash Sharma, and Arvind Kumar khandelwal. 2019. A secure priority vehicle movement based on blockchain technology in connected vehicles. In Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19). Association for Computing Machinery, New York, NY, USA, Article 17, 1–8.
4. Asmaa Berdigh and Khalid El Yassini. 2017. Connected car overview: solutions, challenges and opportunities. In Proceedings of the 1st International Conference on Internet of Things and Machine Learning (IML '17). Association for Computing Machinery, New York, NY, USA, Article 56, 1–7.
5. Benjamin Leiding, Parisa Memarmoshrefi, and Dieter Hogrefe. 2016. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16). Association for Computing Machinery, New York, NY, USA, 137–140.
6. Blockchain - Wikipedia: https://en.wikipedia.org/wiki/Blockchain, last accessed 2021/02/14.
7. Broggi, Alberto & Zelinsky, Alexander & Parent, Michel & Thorpe, Charles. (2008). Intelligent Vehicles.
8. Correa, A., Boquet, G., Morell, A., & Lopez Vicario, J. (2017). Autonomous Car Parking System through a Cooperative Vehicular Positioning Network. Sensors, 17(4), 848.
9. Dogar, Ghulam & Javaid, Nadeem. (2019). Blockchain Based Fleet Management System for Autonomous Vehicles in an Intelligent Transport System.
10. Felix Kohlbrenner, Pezhman Nasirifard, Christian Löbel, and Hans-Arno Jacobsen. 2019. A Blockchain-based Payment and Validity Check System for Vehicle Services. In Proceedings of the 20th International Middleware Conference Demos and Posters (Middleware '19). Association for Computing Machinery, New York, NY, USA, 17–18.
11. Geng, Y.; Cassandras, C.G. A new Smart Parking System Infrastructure and Implementation. Procedia Soc. Behav. Sci. 2012, 54, 1278–1287.
12. Guerrero-Ibañez, Juan & Zeadally, Sherali & Contreras Castillo, Juan. (2018). Sensor Technologies for Intelligent Transportation Systems. Sensors. 18. 1212.
13. Guo, Hao & Meamari, Ehsan & Shen, Chien-Chung. (2018). Blockchain-inspired Event Recording System for Autonomous Vehicles. 218-222.
14. Improving Performance and Scalability of Blockchain Networks https://www.wipro.com/blogs/hitarshi-buch/improving-performance-and-scalability-of-blockchain-networks/, last accessed 2021/02/14.
15. Jennath, H. S., S. Adarsh, Nikhil Chandran, R. Ananthan, A. Sabir and S. Asharaf. “Parkchain: A Blockchain Powered Parking Solution for Smart Cities.” Frontiers Blockchain 2 (2019): 6.
16. Jolfaei, A., & Kant, K. (2019, June). Privacy and security of connected vehicles in intelligent transportation system, 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks–Supplemental Volume (DSN-S), 2019, (pp. 9-10), IEEE.
17. Knirsch, Fabian & Unterweger, Andreas & Engel, Dominik. (2017). Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. Computer Science - Research and Development.
18. Lyubomir Stoykov, Kaiwen Zhang, and Hans-Arno Jacobsen. 2017. VIBES: fast blockchain simulations for large-scale peer-to-peer networks: demo. In Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos (Middleware '17). Association for Computing Machinery, New York, NY, USA, 19–20.

19. M. Demir, O. Turetken and A. Ferworn, "Blockchain Based Transparent Vehicle Insurance Management," 2019 Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 2019, pp. 213-220.
20. M. Singh, and S. Kim, “Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain,” arXiv preprint arXiv:1707.07442, 2017
21. Merkle Tree - https://en.wikipedia.org/wiki/Merkle_tree, last accessed 2021/02/14.
22. Narbayeva, Saltanat & Bakibayev, Timur & Abeshev, Kuanysh & Makarova, Irina & Shubenkova, Ksenia & Pashkevich, Anton. (2020). Blockchain Technology on the Way of Autonomous Vehicles Development. Transportation Research Procedia. 44. 168-175.
23. Ole Meyer, Marc Hesenius, Stefan Gries, Florian Wessling, and Volker Gruhn. 2018. A decentralized architecture and simple consensus algorithm for autonomous agents. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (ECSA '18). Association for Computing Machinery, New York, NY, USA, Article 7, 1–4.
24. P. K. Sharma, N. Kumar and J. H. Park, "Blockchain-Based Distributed Framework for Automotive Industry in a Smart City," in IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4197-4205, July 2019.
25. Rathee, Geetanjali, et al. "A blockchain framework for securing connected and autonomous vehicles." Sensors 19.14 (2019): 3165.
26. Thing, V. L., & Wu, J. (2016, December). Autonomous vehicle security: A taxonomy of attacks and defences. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 164-170). IEEE.
27. Yebes, J.J.; Bergasa, L.M.; García-Garrido, M. Visual Object Recognition with 3D-Aware Features in KITTI Urban Scenes. Sensors 2015, 15, 9228-9250.
28. Zhao, H.; Lu, L.; Song, C.; Wu, Y. IPARK: Location-aware-based intelligent parking guidance over infrastructureless VANETs. Int. J. Distrib. Sens. Netw. 2012, 8, 1–12
29. “Dot/NHTSA policy Statement Concerning Automated Vehicles”, 2016 http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Autonomous-Vehicles-Policy-Update-2016.pdf, last accessed 2021/02/14.