Using Blockchain in Autonomous Vehicles

Nidhee Kamble
Department of Computer Engineering
VJTI Mumbai
India
ndkamble_b17@ce.vjti.ac.in

Revathi Vijayaraghavan
Department of Computer Engineering
VJTI Mumbai
India
rvijayaraghavan_b17@ce.vjti.ac.in

Ritu Gala
Department of Computer Engineering
VJTI Mumbai
India
rsgala_b17@ce.vjti.ac.in

Eshita Shukla
Department of Computer Engineering
VJTI Mumbai
India
epshukla_b17@ce.vjti.ac.in

Dhiren Patel
VJTI Mumbai
India
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 systematic literature review of how blockchain can help in improving not only security but also other aspects of the AV systems. We have found, through our survey, that blockchain technology can aid 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 room for improvement in the sectors of Autonomous Vehicles (AV), that can be achieved with the incorporation of blockchain into Intelligent Transport Systems (ITS) or even individual vehicular units.**

***Index Terms*—Blockchain, Distributed Ledger Technology (DLT), Autonomous Vehicle (AV), Connected Vehicles (CV), Intelligent Transportation System (ITS)**

I. 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 in today's time. 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. AVs will not only be eco-friendly and energy-conscious but also provide comfortable user experience, cause an increase in lane capacity, 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 a complete reality. 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 also 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, 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). 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 changing/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 suggest the use of blockchain technology to help tackle these issues and concerns. 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 II discusses basic terminologies and issues in autonomous vehicles. In Section III, proposed solutions for problems in AVs using blockchain are discussed. Section IV discusses the challenges of using blockchain in AVs, with suggested directions to address them. Conclusion and future scope are presented in Section V with references at the end.

II. BACKGROUND

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

A. Autonomous Vehicles

Siemens PLM Software[1] mentions AVs being better in terms of affordability, experience, and adaptability in comparison with traditional vehicles. In the context of these factors, the research on autonomous vehicles is focussed on the functionalities that are offered (or can be offered) by them, and the technologies used by them. Some proposals build on top of the currently existing ones - like guided parking - while some lay foundations for completely new ones - like accident reporting architectures.

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[2] 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*
  In 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*
  In 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, Alexander Zelinsky, Michel Parent, Charles E. Thorpe [3]*, 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).

B. Technologies Used in AV Ecosystem

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*[4].

Technologies used for AVs build upon the native functions of traditional, level 0 vehicles to optimise them specifically. *Correa, A., Boquet, G., Morell, A., & Lopez Vicario, J.*[5] 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. The paper gives a background[6] on 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 notable mentions in enlisting previous research is of Roadside Units (RSUs), used to utilise unused resources of AVs - like rechargeable battery and storage capacity - using IPARK[7], a system for guided parking over infrastructureless VANETs.

C. 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.

D. Blockchain

A blockchain[8] 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)[9]. 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.

The term *'blockchain'* has been used to refer to one of the following in the papers that we studied: a ledger whose usage is limited to being a shared database, or a chain which is verifiable and immutable (either by permission or by the proposed consensus mechanism).

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).

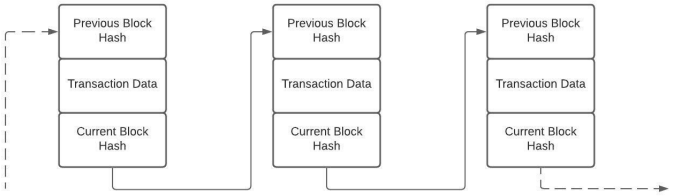

Fig. 1. Structure of Blockchain

E. Smart Contracts

Smart contracts are software programs that live on a blockchain and form the basis of many of the new blockchain applications and schemes.[10] Smart contracts are a technology that is inherently for trustless environments. The need for smart contracts arose from desired flexibility regarding transactions on blockchains. Robustness is traded for speed and programmability. Smart contracts can also be used for microtransactions. A remarkable feature of smart contracts on Ethereum is the use of token standards, which facilitate transactions of different kinds of assets associated with different units of value. Currently, such tokenisation finds applications in legal matters (property transfer or agreements), as well as merchant exchanges.

It is hence a challenge to effectively replace every facet of the system(s) where disputes over legal issues are as fair as the consensus mechanism their settlement uses, eliciting a need for scrutiny and analysis for the effectiveness of blockchain consensus mechanisms.

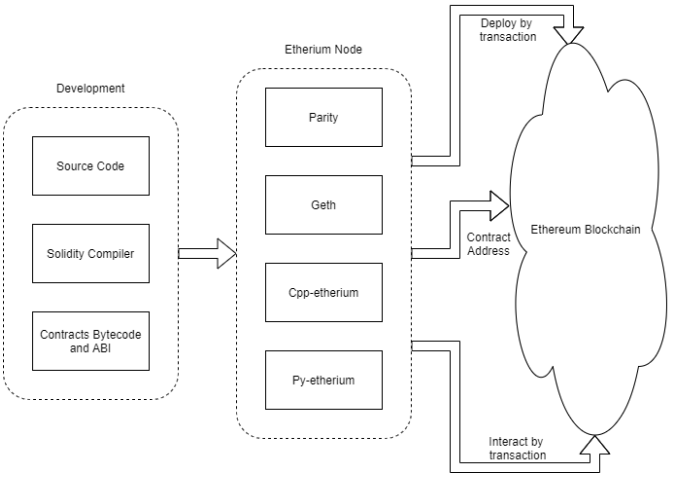

Fig. 2. The process of smart contract's development, deployment, and interaction on Ethereum[11]

F. 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), Proof of Stake (used by Ethereum 2.0), Proof of Vote and Proof of Burn.

G. 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 connectivities 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.[12] 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 unauthorised complete control of the vehicle or data tampering. Further, with autonomy, comes 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.[13]

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.

III. USE OF BLOCKCHAIN IN AVs

A. 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[14] 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* [15] 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 & Bakibayev, Timur & Abeshev, Kuanysh & Makarova, Irina & Shubenkova, Ksenia & Pashkevich, Anton. [16] 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.[17] *Vrizlynn L.L. Thing et. al.,*[18] 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.*[19]. 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*[20]. Key management could become an issue for each device and they cause a potential weakness in the system.

Rathee, Geetanjali, et al. 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.

B. Blockchain to Improve AV Functionalities

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

1) 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*[21] 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.

2) Insurance and Payments

M. Demir, O. Turetken and A. Ferworn[22] 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 [23] 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.

3) Charging Stations and Power Requirements

Alejandro Ranchal Pedrosa and Giovanni Pau [23] 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, Andreas Unterwege, et al. [2] 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 for transparency and verifiability. The

phases of requesting and serving of corresponding charging locations have been elaborated upon.

4) Parking for AVs

There are intelligent parking management architectures that are suited specifically for the system heterogeneity of AVs. *Jennath, H. S. et al.*[17] 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.

C. Optimising 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 & Gurmani, Muhammad & Sultana, Tanzeela & Azeem, Muhammad & Iftikhar, Muhammad & Javaid, Nadeem*[25] 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 & Javaid, Nadeem.[26] 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.

IV. ANALYSIS

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

A. Relevance of Blockchain

1) 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.

2) 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.

3) Lack of Appropriate Consensus Mechanisms:

The prevalent consensus mechanisms for blockchain - Proof of Work, Stake, and Authority - are criticised in a few research papers for their inability to maintain the decentralisation 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 incentivisation.

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.

B. 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 aren't feasible on AVs which might in turn result in low throughput of the system, by causing an increase in latency.

C. Future of Related Industries

Exploring the current proposals and analysed 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.

D. 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, 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.

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.

E. 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.

V. CONCLUSION

The adoption of AV and blockchain technologies has been compared to the adoption of the Internet in the 1990s - disruption of conventional systems, met with cynicism, slow rise to popularity, spread in reach, and an eventual boom in use cases - allowing for their mass usage with passage in time. In the near future, autonomous cars will coexist with traditional cars, giving birth to systems that may fulfil the needs of either both or just AVs, hence differing in their motivation. Every technology and application is created by the developers with a specific vision, but what niche their creations fit into is decided by how the users receive it. Like the Internet was not intended for sharing cat videos but became significantly widespread *because* of them, AVs and blockchain can have even more applications in domains that we may not be aware of or be able to envision at present. There is significant scope in areas of AVs that can be aided by blockchain technology, and our survey particularly suggests more research be done in the use of blockchain for facets of AVs as suggested in the previous section.

REFERENCES

[1]The future car: Driving a lifestyle revolution https://www.plm.automation.siemens.com/media/global/en/Siemens-PLM-SES-Future-Car-wp-69077-A11_tcm27-31327.pdf [accessed 29 Oct, 2020]

[2] "Dot/NHTSA policy Statement Concerning Automated Vehicles", 2016 http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Autonomous-Vehicles-Policy-Update-2016.pdf [accessed 23 Oct, 2020]

[3] Broggi, Alberto & Zelinsky, Alexander & Parent, Michel & Thorpe, Charles. (2008). Intelligent Vehicles. 10.1007/978-3-540-30301-5_52.

[4] 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

[5] Correa, A., Boquet, G., Morell, A., & Lopez Vicario, J. (2017). Autonomous Car Parking System through a Cooperative Vehicular Positioning Network. Sensors, 17(4), 848. doi:10.3390/s17040848

[6] Geng, Y.; Cassandras, C.G. A new Smart Parking System Infrastructure and Implementation. Procedia Soc. Behav. Sci. 2012, 54, 1278–1287.

[7] 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.

[8] Guerrero-Ibañez, Juan & Zeadally, Sherali & Contreras Castillo, Juan. (2018). Sensor Technologies for Intelligent Transportation Systems. Sensors. 18. 1212. 10.3390/s18041212.

[9] Jawhar, Imad & Mohamed, Nader & Usmani, Hafsa. (2013). An Overview of Inter-Vehicular Communication Systems, Protocols and Middleware. Journal of Networks. JOURNAL OF NETWORKS, VOL. 8, NO. 12, DECEMBER 2013. 10.4304/jnw.8.12.2749-2761.

[10] How Smart Contracts Work
Blockchain technology could run a flight-insurance business without any employees
https://spectrum.ieee.org/computing/networks/how-smart-contracts-work [accessed 23 Oct, 2020]

[11] A Survey on the Security of Blockchain Systems - Scientific Figure on ResearchGate.https://www.researchgate.net/figure/The-process-of-smart-contracts-development-deployment-and-interaction_fig3_319249505 [accessed 23 Oct, 2020]

[12]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.

[13] Correa, A., Boquet, G., Morell, A., & Lopez Vicario, J. (2017). Autonomous Car Parking System through a Cooperative Vehicular Positioning Network. Sensors, 17(4), 848. doi:10.3390/s17040848

[14] Guo, Hao & Meamari, Ehsan & Shen, Chien-Chung. (2018). Blockchain-inspired Event Recording System for Autonomous Vehicles. 218-222. 10.1109/HOTICN.2018.8606016.

[15]M. Singh, and S. Kim, “Intelligent Vehicle-Trust Point: Reward based Intelligent Vehicle Communication using Blockchain,” arXiv preprint arXiv:1707.07442, 2017
[16]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. 10.1016/j.trpro.2020.02.024.
[17] 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.
[18] 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.
[19] Rathee, Geetanjali, et al. "A blockchain framework for securing connected and autonomous vehicles." Sensors 19.14 (2019): 3165.
[20] 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.
[21] 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, doi: 10.1109/TII.2018.2887101.
[22] 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, doi: 10.1109/SDS.2019.8768669
[23] 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.
[24] Knirsch, Fabian & Unterweger, Andreas & Engel, Dominik. (2017). Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. Computer Science - Research and Development. 10.1007/s00450-017-0348-5.
[25] Abubaker, Zain & Gurmani, Muhammad & Sultana, Tanzeela & Azeem, Muhammad & Iftikhar, Muhammad & Javaid, Nadeem. (2019). Decentralized Mechanism for Hiring the Smart Autonomous Vehicles using Blockchain.
[26] Dogar, Ghulam & Javaid, Nadeem. (2019). Blockchain Based Fleet Management System for Autonomous Vehicles in an Intelligent Transport System.
[27] Merkle Tree - https://en.wikipedia.org/wiki/Merkle_tree [accessed 23 Oct, 2020]
[28] Mathur, S.; Jin, T.; Kasturirangan, N.; Chandrasekaran, J.; Xue, W.; Gruteser, M.; Trappe, W. ParkNet: Drive-by Sensing of Road-side Parking Statistics.Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys ’10), San Francisco, CA, USA, 15–18 June 2010; ACM: New York, NY, USA, 2010; pp. 123–136.
[29] Barone, R.E.; Giuffre, T.; Siniscalchi, S.M.; Morgano, M.A.; Tesoriere, G. Architecture for parking management in smart cities. IET Intell. Transp. Syst. 2014, 8, 445–452
[30] Cooper, Chris & Booth, Andrew & Varley-Campbell, Jo & Britten, Nicky & Garside, Ruth. (2018). Defining the process to literature searching in systematic reviews: A literature review of guidance and supporting studies. BMC Medical Research Methodology. 18. 10.1186/s12874-018-0545-3.
[31] Moras, Julien & Cherfaoui, Véronique & Bonnifait, Philippe. (2010). A lidar Perception Scheme for Intelligent Vehicle Navigation. 1809-1814. 10.1109/ICARCV.2010.5707962.
[32] Gavrila, Dariu & Franke, Uwe & Wohler, C. & Gorzig, S.. (2001). Real time vision for intelligent vehicles. Instrumentation & Measurement Magazine, IEEE. 4. 22 - 27. 10.1109/5289.930982.
[33]Blockchain - Wikipedia: https://en.wikipedia.org/wiki/Blockchain [accessed 23 Oct, 2020]
[34]Short, J., & Murray, D. (2016). Identifying autonomous vehicle technology impacts on the trucking industry.
[35] Jane Macfarlane and Matei Stroila. 2016. Addressing the uncertainties in autonomous driving. SIGSPATIAL Special 8, 2 (July 2016), 35–40. DOI:https://doi.org/10.1145/3024087.3024092
[36]Yu, X.; Marinov, M. A Study on Recent Developments and Issues with Obstacle Detection Systems for Automated Vehicles. Sustainability 2020,
[37] A survey of public opinion about autonomous and self-driving vehicles in the U.S., the U.K., and Australia - Schoettle, Brandon; Sivak, Michael (2014-07) https://deepblue.lib.umich.edu/handle/2027.42/108384
[38] Talks by Andreas A. Antonopoulos