Howcanblockchainbeintegratedintoautonomoussystems to ensure dataintegrity and trustworthiness, and what are the potentialpitfallsindecentralizedautonomoussystemoperations?

Abstract

Real-timeapplicationsalwayshavesecurityissuespresentintheirecosystemwhichneedstobeimproved. Blockchain technology can be considered as a solution that can ensure network security. Theintegration of blockchain technology into autonomous systems has now become an important candidateto resolve network security issues in devices that work on p2p communications. As humans becomemore reliant on autonomous vehicles, the importance of finding a solution to the problems linked withdata security needs to be addressed to comply with international security laws. The paper aims to findtheimportanceofblockchaintechnologyandhowitcanbeintegratedintodifferentclassesofautonomousvehicles.Intheresearch,an analysis of existing papers will be included along with aproposeddesignthatcanbedeployedtosolvetheproblemsassociatedwithdata security usingblockchain technology. Besides the improvements offered by blockchain technology, all the additionalchallenges associated with designing a new system and deploying this technology will be reviewed. Thelimitationsoftheworksalongwiththefutureresearchopportunitiesthat might open up will bepresentedinthispaper.

Keywords: Blockchain technology, network security, Autonomous vehicles work, environmentalboards

Introduction

Autonomous vehicles work on the basis of heaps of fresh training data, from various input sources suchasGPS,Sensors,communicationnetworks,Radars,andenvironmentalboardstomakereal-timedecisionsallowingthemtocruiseandnavigatetheenvironmentsafelyandefficiently.Itisimportantthatthe data that is received is from a trustworthy source and it is accurate i.e., no additional inputs arepresent in the data stream that might poison the integrity of the data under consideration. The accuracyof the data would allow these autonomous vehicles to build public confidence in these technologiesenablingthemtopassthesafetyrequirementsand regulations allowing them to work in delicatesituations where human lives are at stake. Blockchain networks offer the principles of decentralization,immutability, and transparency which is the key characteristics required for making it an objectivelybetter solution to enable data security and confidentiality while data is being fed to these autonomousvehicles.

Inthisresearchpaper,thepotentialbenefitsandthechallengesofintegratingblockchaintechnologyintoautonomous systems will be explored, the primary methods that can be used to enhance the datasecurity enabled by blockchain to ensure the trustworthiness of the system to allow safer operations willbeexamined.The potential drawbacks along with the flaws in the current designs that have beenproposedwouldbeexamined to understand the areas of improvement and opportunities that areofferedbyusingblockchaininasystemofautonomousvehicles.

ProblemStatement

Autonomous systems, such as self-driving cars and drones, are rapidly improving ensuring efficiency incommute and deliveries while maintaining a standard of safety. The reliable operations of these vehiclesrelyontheaccuratedatainputsreceivedfromthedifferentcomponents,sensors, and networks.Ensuring the integrity of data in autonomous environments remains a challenge. Traditional methods fordatavalidationandsecurityfallshortwhiledealingwithcontinuouslivedataasitcanbebreachedeasily,raising a need for a system that could address the challenges associated with investigating and designingasolutionusingblockchainforimprovedsecurityandtrustinautonomousdataprocessingandtransmission.

BackgroundofAutomationinVehicles

To understand the network of vehicles and levels of automation, the vehicles themselves can be furthercategorized into 5 stages. All of these levels are more assistive towards the driver from basic driving tofullyautomatedvehicles.Thecategoriesofvehiclesarefurtherdescribedinthesectionbelow.

Level0(NoAutomation): Inthislevel,thereisnoautomation,andthehumandriverisresponsibleforallaspects of driving. Basic driver assistance systems like ABS and traction control may be present, thedrivermayhaveelectricalassistancebutnoproperautomation.

Level 1 (Driver Assistance): Level 1 vehicles offer driver assistance features, such as adaptive cruisecontrolorlane-keepingassistance.Thesystemcanassistthedriverbutattentiontotheroadisrequired.

Level 2 (Partial Automation): Level 2 vehicles have more advanced driver assistance systems that cansimultaneously control both steering and acceleration/deceleration. Driver monitoring is still requiredbutthelevelofocusisabitrelaxed.

Level 3 (Conditional Automation): At this level, the vehicle can manage most aspects of driving undercertain conditions. The driver can disengage from active control but must remain ready to intervenewhen the system requests. Traffic assistance and parking assistance are some examples that can beconsideredaslevel3automation.

Level 4 (High Automation): Level 4 vehicles are highly autonomous and can operate without humaninterventioninspecificenvironmentsorconditions.Humanoversightsarenotrequiredinsuchvehicles.

Level 5 (Full Automation): Level 5 represents fully autonomous vehicles that can work without anyhuman involvement. These vehicles are not bound by any conditions and can function similarly to ahumandrivingorbetter(1).

TechnologiesPartoftheAutonomousVehicleSystems

1. Sensors:

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

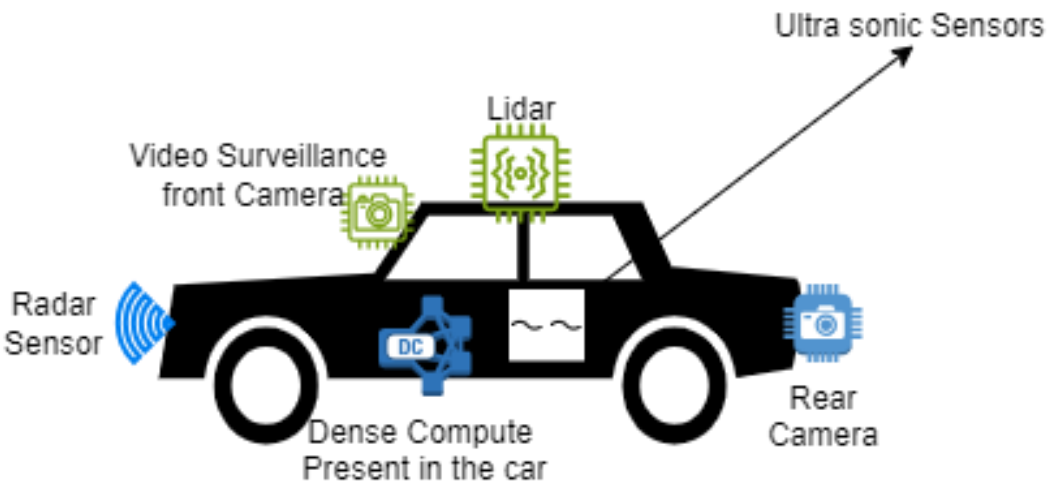

Figure1:SensorsinAutonomousVehicles(34)

2. GPSandIMU:

The location data is received using a transmitter that processes the GPS data to determine the vehiclepositionandtheIMUspartofthevehiclecandeterminethenavigationaccuracy,andthespeed(52).

3. ControlSystems:

The vehicle itself is dependent on the control system, the ECUs are deployed that are responsible for theengine braking and steering, whereas the overall car electronics and mechanical vehicle features arecontrolledbyadedicateddrive-bysystem.

4. Connectivity:

V2Xtechnology enables communication between vehicles and infrastructure or other vehicles. Thisenhances safety and can provide real-time traffic information, for instance, if multiple AVs are stuck in atrafficjamitcanalertotherAVspartofthesystemtouseadifferentroutenotcausingatrafficjam.

5. High-PerformanceComputing:

AVs use powerful CPUs to process data from sensors to make real-time driving decisions. To process thelarge number of queries for performing complex calculations and decision making a GPU is used in theAV.

6. MachineLearningandArtificialIntelligence:

AVs often use machine learning and AI algorithms to interpret sensor data and recognize objects basedontheirtrainingdatatomakedrivingdecisions.

DataProcessingandCaptureinanAutonomousVehicleNetwork:

The Autonomous works on the basis of data processing and manipulation, the whole process starts withdata collection when high-performance sensors explained in the above section are used to collect datafromthevehiclesurroundings,creatingastreamofrawdata.Oncethedatahasbeencollected,the

sensor data is fused to create a representation of the environment that can help in understanding thescenario. AI and machine learning algorithms are now used to identify the objects from the fused data,the perception stage extracts the valuable information i.e. road features, vehicles and pedestrians fromthefusedsensordata(51).

TheadditionalnetworksassistingthedrivingsuchasGPSandIMUsmapthedatatoaccuratelydetermine the vehicle's position within its environment for safety.Based on the localized data, a pathcan be planned that would be followed by the AV, and the acceleration, braking and driving decisionswould be processed in real time using sensor fusion and high-performance computing (50). The controlsystem present in the dense compute engine makes sure that the vehicle follows the traffic rules andsafety requirements. The controls trigger the actuators allowing the vehicle to gas and steer accordingly(49).

Data related to the vehicle's operation, sensor inputs, and decisions are typically logged and stored foranalysis, debugging, and post-incident investigation. The data that is processed can be used in machinelearningforimprovementinautonomousdrivingsystems.

The diagram below would help in understanding how the autonomous vehicles work, and how data isprocessedinthewholescenario.

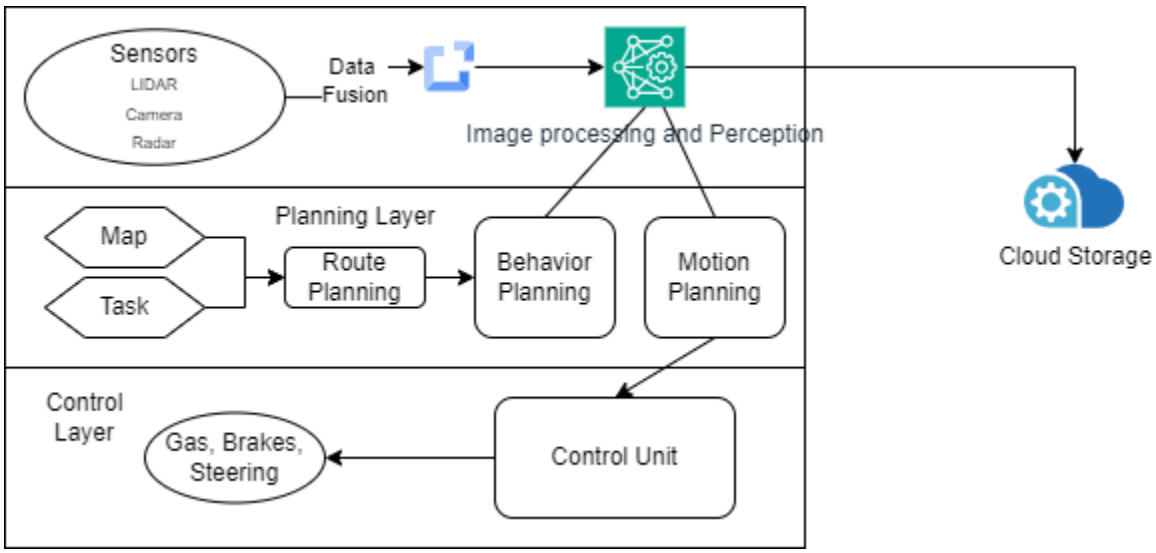

Figure2:DataProcessinginAutonomousVehicles(35)

IntroductiontoBlockchainNetworks

In recent years, the integration of blockchain to solve security issues in complex network structures hasnow emerged as a transformative solution to address challenges related to secure data processing andstorage. Traditional methods involving data handling and managing security often fall short in ensuringintegrity for complex networks requiring newer solutions to manage the needs. Blockchain, initiallydevisedasthefoundationaltechnologybehindcryptocurrenciescanbeusedtoaddressdatamanagement andsecurityissues(10).

The fundamental characteristic of a blockchain network that makes it a considerable option for securedatatransformationisthedecentralizednatureanddistributedledgersysteminwhichchangesarenot

possible unless the nodes are notified. These core features offered by blockchain make it an optimalchoice for Autonomous vehicle networks as it is capable of addressing the following challenges withease.

Ensuring data integrity is critical for AVs, as any tampering with sensor data or navigation instructionscould lead to safety risks. Blockchain's immutability guarantees that once data is recorded, it cannot bealtered or manipulated without consensus. Enhancing the overall reliability of data that is being used fordecision-making.Autonomousvehiclesoftenoperateusinganetworkofconnectedvehiclesandinfrastructure. Decentralization reduces the vulnerability to points of failure caused at a central point,makingitmoreresilienttoattacks(48).

Transparency ensures that AV data can be audited and traced back to its source. In the event of anaccident, an audit trail can help determine the cause and responsibility enabling the regulators andinsuranceproviderstotrusttheAutonomousVehicleSystems.

Moreover, blockchain also offers smart contracts that can automate different features of AV operations,such as toll payments, insurance claims, or charging fees for electric AVs. These contracts can executepredefined rules autonomously, reducing the overheads associated with the administration as all of theworkwouldthenbecomeautomatedensuringcompliancewithregulations.Lastly,Blockchainoffersdatasharingthat is secure and consensus among the entities involved. For example, traffic data sharedthroughblockchaincanhelpthesevehiclesoptimizeroutes,andreducetrafficjams.

UseOfBlockchaintoImproveAutonomousVehicleFunctionalities

The integration of blockchain technology into AV ecosystems has the potential to become a solution todatasecuritychallenges.Blockchain,renownedforitsdecentralizedledgerandimmutablerecord-keeping capabilities, offers a shift in the traditional method for storing and transporting data. Asthetechnologyhasprogressedthefocusofusingblockchainfor Autonomous vehicles has gainedattentionfrom researchers and industry stakeholders. Numerous pieces of research under differentareas linked with the functionalities of Autonomous vehicle networks have been published that offerenhanced protection and improvement in the features using blockchain (46). The following section willfocusonhighlightingsomepapersassociatedwithimprovingAVfunctionalitiesusingblockchaintechnology. The review would highlight the challenges addressed and the methodologies proposed byscholars in this field. Moreover, it would aim to shed light on the proposed designs and frameworks thatuse blockchain to enhance the capabilities of autonomous vehicles. From data integrity and securecommunicationtooptimizedroutingandsmartcontract-drivenautomationperformancecanbeoptimized as several studies and safety measures have been described in the literature part of thissection(47).

VehicleAd-hocNetworkUsingBlockchain

AVehicleAdhocNetwork(VANET)isacommunicationnetworkamongvehiclesandroadsideinfrastructure. It enables real-time data sharing for purposes like traffic management and road safety.Blockchain can enhance VANETs by providing secure data sharing. Smart contracts can automate tollpaymentsandtrafficcoordination,blockchaincanalsopreventdatamanipulationorhackingattemptsinthesenetworks(10).

A research survey conducted by Jyoti Grover in 2022 focused on highlighting several pieces of researchthat used blockchain to improve VAnet security. The paper highlighted the existing challenges present inthe ad-hoc network and how these challenges can be addressed using blockchain. The advantages ofblockchain such as its decentralized nature and immutability were highlighted in the paper, as it makes iteasier for the network to record transactions. The technical issues related to the widespread acceptanceof the idea were highlighted, as employing a new technique can be a difficult job in an existing market(2).AnotherresearchwasconductedbySanjeevet AI, which focused on blockchain-based ad-hocnetworks for AV applications. It highlighted research that included blockchain for facilitating secure datatransfer along with sharing critical information, a literature review was presented that focused on theapplicationofdifferentblockchainnetworksand how these private networks be embedded in thesystem of AV for data security and transportation. The application assists the use of blockchain forbuilding smart cities powered by Autonomous vehicles and how can cooperation between these vehiclesensure that additional overheads such as traffic congestion and authenticity of service providers beresolvedbyemployingadistributedledgerprotocol(3).

Another research was presented by Benjamin Leiding et al. in which an Ethereum-based network allowsthe application of rules for the users that were part of the system. The transactions that were made onthe platform had to pay a price that allowed running the service on the Ethereum node (45). Theautomation in the network was to improve the loyalty program of the customers by processing thetransaction and providing a secure method for charging their cars. The whole Vehicular ad-hoc wasdesigned to entertain self-driving and regular cars so that they could easily charge their electric vehicleswhilethepaymentwasprocessedusingtheEthereumblockchain,anautomatedsubscriptionmodelwa sintroducedtofacilitatetheloyalcustomersofthenetworkthatwasdeployedonEthereum.Thediagrambelows howstheworkingofthedesignwhichwasproposedinthepaper(4).

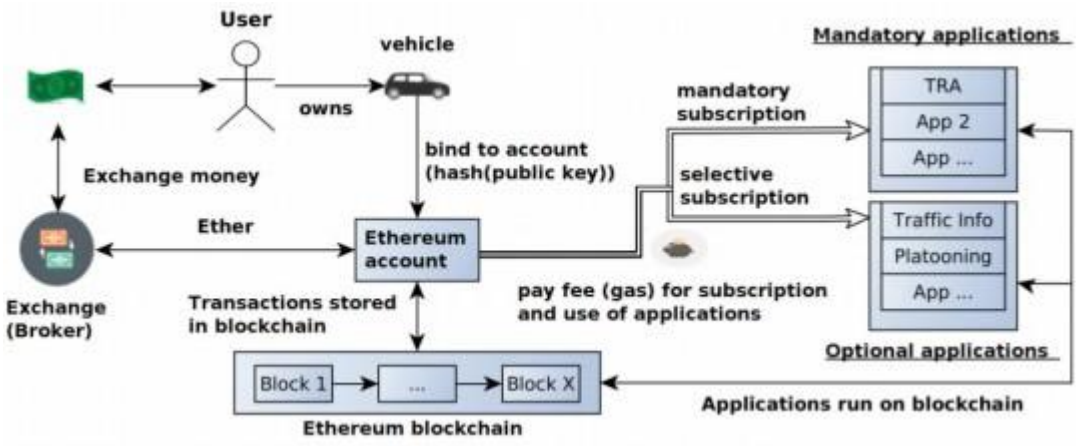

Figure3:UseofEthereuminAutonomousVehicles(36)

Blockchain-basedDesigntoReduceDataSpoofing

GPS spoofing is a cybersecurity flaw in which false coordinates are generated to deceive GPS receiversand mislead them about their actual location. This manipulation of location data can significantly impactAutonomous Vehicles by causing them to navigate incorrectly or follow different routes. AVs rely heavilyonaccurateGPSdataforprecisenavigation.GPSspoofingattackscanleadAVstolosecontroland

potentiallyresultinaccidentsorunauthorizedaccesstosensitiveareas.Thefollowingdiagramdemonstratesho waGPSspoofingattackworks(11).

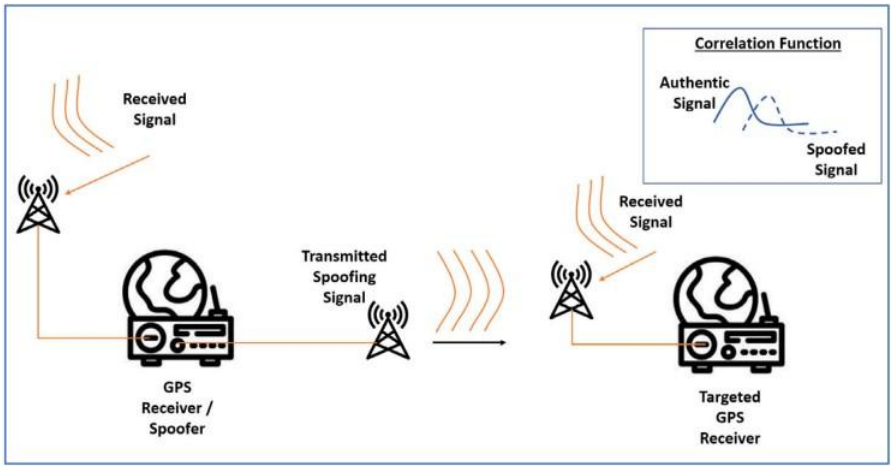

Figure4:GPSspoofingattack(33)

BlockchainhasthepotentialtoreduceGPSspoofingsignificantlyasblockchainrecordsdatainatamper-resistant ledger. GPS data stored on the blockchain cannot be altered without consensus fromthe network participants. This ensures that once GPS coordinates are recorded, they remain unchangedand reliable.Moreover,cryptographictechniquesfordataverificationinblockchain-basednetworks.GPSdata is cryptographically signed, making it extremely difficult for malicious actors to manipulate or spooflocation information without detection. Data on the blockchain is transparent and visible to all networkparticipants.AnydiscrepanciesinGPSdatawouldbequicklyidentifiedbynetwork users, makingspoofingattemptsmorelikelytobedetected.

ResearchconductedbySateeshKumaretal.highlightedthevulnerabilitiesofUAVs making themsusceptible to GPS spoofing attacks. The research proposes the development of an energy-intensiveblockchain-based platform designed to control drone operations. This platform is intended to ensuretrust and security for all parties involved in drone operations. Blockchain technology is leveraged toenhance security, data integrity, and trust within the UAV ecosystem. The primary objective of the paperwas to address the vulnerability of UAVs to GNSS spoofing attacks. The research acknowledges thatexisting algorithms for countering spoofing attacks have limitations within the long-term errors thatgather over time. To overcome this, the proposed approach introduces an innovative use of EthereumBlockchaintocreateablockchainnetworkaimedatmitigatingspoofingattackseffectively.Theblockchain network is used to register components and relevant data associated with UAV operations.The ledger within the blockchain ensures data integrity and cryptographic keys, making it resistant totampering. Geolocation data is periodically verified by the blockchain network to detect and eliminateanyoutliersorerroneousdata(8).

ResearchconductedbyRajeshetal.addressedcybersecurityandprivacyconcernsrelatedtoautonomous vehicles in an ecosystem where smart transportation is common. The paper conducts acomprehensive analysis of threat classifications specific to autonomous vehicles. It focuses on threatsthatAVs may encounter. Moreover, theresearchalsohighlightscountermeasuresandsecuritymeasures

to mitigate cyberattacks on AVs. It explores potential solutions to address the identified threats whileemphasizingtheimportanceofsafeguardingAVpassengers.Thepaperintroducesblockchaintechnology asameanstoaddressthesecurityandprivacyconcernsassociatedwithAVs.Itdiscusseshowblockchaincan offer a decentralized and secure framework that reduces the risk of single points of failure andenhancestheoverallsecurityofAVoperationsTheresearchfurtherproposesablockchain-basedintegrated architecture for AVs, that could mitigate security and privacy issues while ensuring serviceavailability(9).

UseofBlockchaininReal-worldAutonomousSystems

ResearchconductedbyChoietal.proposedasystemforAVcommunication that improved theirefficiency and security. The data packet while the transmission was encrypted, the design used FL toensurethe privacy of the data exchanged. A mathematical framework was used using a controlledblockchain network. The block size, arrival rate, and other attributes were analyzed which helped inidentifyingthedatapacket.Thestudyfurtheridentifiedchallengesinexistingautonomouscommunication,a ndwhatdifferentthreatswerepresenttowirelesscommunicationofAVs(15).Anotheruse case of a blockchain-based ride-hailing platform was presented in a research conducted by Srikanthet al. The network of vehicles used in their service included AVs. The design presented how efficientlyblockchainwasabletodistributetheworkload(16).

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

SecurePayments,VehicleSharing,andFreightIndustry

The convergence of autonomous vehicles and blockchain technology represents a shift in the mode oftransportation and logistics. As AVs continue to evolve, they are becoming safer and cheaper for theusers to employ instead of human labor, the following section will look into some research on howautonomous vehicles can improve payment gateways, vehicle sharing, and mass freight transport andwhatimpactofusingblockchain-basedalternativeswouldpresentonthismarket(20).

Research conducted by Abubakar et al. presented a paper in which a blockchain-based protocol waspresent for the management of vehicles that are being used by service providers as it helped in trackingthelocationandtheactivestatusofautonomousvehicles.Fortheconsensusmechanism,aProof-of-Work algorithm was selected as validation was required to overcome the demand responseevents. The paper provided a design in which adding new vehicles to the fleet was possible along withhiringdriversandprocessingtheirdetailssecurelyinthead-hocnetworkusingblockchain(5).

In 2019 DogarGhulam conducted research that focused on the system in which an autonomous fleet ofvehicles could become a part of a system that had an intelligent transport network. The fleet wasresponsibleforprovidingservicestotheautonomousvehiclesthatwerelinkedwithanyjobsorregistered to any organization. The vehicles part of a job or a company were registered on the networkwhich allowed the stakeholder to manage the attributes and fill in the job details securely once thevehicle was part of the Intelligent trust point mentioned in the research. The paper presented a designthat could help in job scheduling, and task completion as an incentive-based fleet management systemwasdevelopedthatwaspoweredbyblockchaininwhichtheworkernodeswereawarded(6).

AnalysisoftheUseCases

The integration of blockchain technology into autonomous vehicles presents an opportunity to addressthe critical challenges for management and enhancing operations helping it to innovate. As the paperhaspresentedanumberofusecasesofblockchainforenhancedsecurityandautomationinAVsystems,th esectionwillprovideanoverviewoftheanalysisofthepresentedsystems(21).

TamperResistance

Tamper resistance in blockchain significantly improves the security of a system, it allows defense againstdifferent types of alteration in the context of any network. The core feature offered by blockchain isimmutability, meaning that once data is recorded in a block and added to the chain, it cannot be alteredor deleted without consensus from the network participants. This property ensures data integrity on theblockchain network. In the case of Autonomous vehicles, accurate data is critical for decision-making asnavigation and safety are dependent heavily on the input (44). Malicious actors may attempt to tamperwithdata,suchasalteringsensorreadingsormanipulatingvehicleinstructions,theconsensusmechanis m offered by the distributed ledger ensures that any unauthorized attempts to modify data aredetected and prevented. Many Research papers have focused on delivering a tamper-free ledger systemthat could ensure the integrity of data while in communication. The papers provide an understanding ofwhatnotableadvantagesintermsofprotocolsareofferedbyblockchainthatmakethenetworkresilientenou ghtosustaintamperingattacks(7).

LackofAppropriateConsensusMechanism

Blockchain technology has revolutionized various industries by providing a secure means of recordingand verifying transactions. However, the current consensus mechanisms, Proof of Work, Proof of Stake,andProofofAuthorityhavefacedcriticisminresearchpapers for their limitations in maintainingdecentralization and ensuring the integrity of on-chain data. The backlash is particularly increased whenusingblockchainapplications to improve a potential supply chain. The first concern is flaws in thedecentralization methods as power tends to get concentrated in PoW, PoS, and PoA mechanics if anyregion is providing higher computational power (22). This centralization of control raises questions onthe characteristics of a blockchain network and theoretically, this could be a flaw that any malicious usercan misuse for personal gains (23). Secondly, the alternatives to these consensus mechanisms that areproposedintheresearch papers, have faced criticism for their failure to provide incentives to theparticipantnodes.Incentivesmotivateparticipantstovalidatetransactionsandmaintaintheblockchain'sse curityandintegrity(6).

FutureoftheAVIndustry

The future of autonomous vehicles promises convenience and improves security through the integrationof blockchain technology. Some of the potential ways blockchain could improve the widespread use ofAutonomousVehiclesarethefollowing:

SecureVehicle-to-EverythingCommunication:

Blockchaincansecurevehiclecommunicationbyenablingvehiclestoexchangedatainatamper-resistantandauthenticatedmanner.Thisensuresthatinformationsharedamong AVs,infrastructure,andother connectedentitiesremainsunaltered,reducingtheriskofdatamanipulationorcyberattacks(24).Thecriticalsafety-relatedcommunicationsarekeptunaltered,makingthedatasharedwithinthesystemsresilientagainstmaliciousinterferenceandunauthorizedaccess(12).

SecureOver-the-Air(OTA)SoftwareUpdates:

AVs regularly receive software updates for enhanced functionality and security. Blockchain can ensuretheintegrityandauthenticityofOTAupdates.AVscanverifythesourceandcontentofupdates,reducingtheriskofmaliciousoftwareinfiltrationandunauthorizedmodifications(25).Bypreventingunauthorizedsoftwarechanges,blockchaincanimprovetheoverallcybersecuritypostureofAVs(13).

AutonomousVehicleIdentityandAuthentication:

Blockchain can be used to establish and manage unique digital identities for AVs, allowing for secureauthenticationinvariousscenarios(26).AVscansecurelyidentifythemselvestoothervehicles,infrastructure, and service providers, reducing the risk of impersonation and unauthorized access. Thisuse case enhances the overall security of AV networks by ensuring that only authenticated vehicles canparticipate(14).

IssuesWiththeUseofBlockchaininAVSystems

If autonomous vehicles are set up correctly and used in an environment where relative technologies arealso present, they have the potential to transform the commute and delivery system in busy cities. Theintegration of blockchain is a promising solution to deal with the security concerns that might be raisedwhilesharingandprocessingdatain AV systems but the integration of blockchain technologies inexisting networks can be a difficult task to monitor and perform (27). Blockchain in itself is capable ofproviding security and addressing scalability issues as part of any supply chain due to its decentralizednature, it also presents specific issues that need to be addressed before it is considered to be deployedonalargerscale.SomeoftheissuesofusingblockchaininAVnetworksarediscussedinthissection(28).

ScalabilityIssues

Oneof the foremost challenges in deploying blockchain within AV systems is scalability. Blockchainnetworks, especially public ones like Ethereum, can struggle to handle a high volume of transactions in atimelymanner.ThiscanbeaconcernforAVnetworks,where real-timedatasharinganddecision-makingare important (29). As Ethereum in itself is a relatively bigger blockchain network it tends to lack whileprocessingalargenumberoftransactionsmakingitdifficultfortheAVnetworkstochooseitasthe

optimal choice. AV fleets have the potential to grow in the upcoming future and if a blockchain-basednetwork is used for storing and processing the data, it can be difficult to upscale and process a largernumber of requests and it may result in a bottleneck (43). There are solutions present to resolve thescalability issues such as using a layer-2 blockchain network. Researchers are working on designing anetwork that can process a large number of transactions that could potentially satisfy the scalability andbottleneckissuesofthewholesystem(30).

ComputationalIssues

Blockchaintransactionsinvolvecomplexcryptographicoperationsthatdemandcomputationalresources. ForAVs, whichoftenoperateonresource-constrainedhardware,thecomputationaloverheadof blockchain transactions can be a significant concern. AV networks rely on the data generated fromsensors and microprocessors are present in the vehicles that can only compute a limited complexityproblem (31). The low processing powers of Autonomous vehicles can affect the efficiency of real-timeprocessinganddecision-making,potentiallyimpactingsafety-criticalfunctions.Theonlysolutionpresentedtothisproblemistooptimize the cryptographic algorithms that are being used and tointegrate specialized hardware that could solve some of the computational issues that any vehicle wouldface(5).

LackofKnowledge

The successful integration of blockchain into AV systems requires an understanding of both domains,since both technologies are new, very few experts are present that could help in providing insights intothe system flaws. The knowledge gap of both fields being new is a hurdle for the researchers that theyneedtoovercome.Bridgingtheknowledgegapisessentialtodesigningrobustblockchain-basednetworks for vehicles. Collaboration between the domain experts of both fields is necessary to ensurethat the blockchain network is implemented perfectly to align with the safety standards and regulationsallowingdronesandautonomousvehiclestooperatefreely(14).

LimitedExistingSystems

Since blockchain itself is a relatively new technology it can be difficult to incorporate blockchain-basednetworks in the field of autonomous vehicles as no proper wide-scale implementation is present thatwould allow us to analyze the potential flaws of such a system and the costs along with the overheadsassociatedwithmanagingasystemofthistype.Whiletherearenotableresearchprojectsandproof-of-concept demonstrations, these have not yet reached widespread adoption in the AV industry.The limited existing systems represent both a challenge and an opportunity (32). The lack of wide-scaledeploymentofarchitectureshowsthatthescarcityofreal-worldapplicationsindicatesthatthetechnology is in its base state, if proper experimentation is conducted any potential regulatory flawspresent in the system can be identified and fixed prior to setting it up for global use. Moreover, it alsoprovides researchers an open ground for research as promoting research in this field would help indeveloping two relatively new fields of blockchain and Autonomous vehicles, as we could potentiallyhighlightthetechnologicalandsecurityflawsthatmayarisebyintegratingthetwonetworks(37).

While blockchain holds promise for enhancing the security of autonomous vehicle systems, it is essentialtoaddresschallengestofullyutilizethepotentialefficiencyofthe network (38). Overcoming theseissues will require collaboration between the stakeholders, testing new designs on the live data so thatthe regulatory flaws can be identified, and ongoing research efforts for the seamless integration ofblockchaintechnologyintothefutureofautonomoustransportation(11).

ResolutionofSecurityIssues

Autonomous vehicles rely on data from different sources, making them an easier target for attacks asbesides the data being transferred, a large number of communications between the vehicles are alsoincludedwhichcanpotentiallybehijackedbyanattackerformaliciouspurposes.ResearchconductedbyVrizzlynetal.classified the different types of attacks that are susceptible to these AVs, the broadclassification included physical attacks and remote attacks, in physical attacks, code modification, andcodeinjectionwerecommonwhereassignalspoofingandpacketjammingalongwithmodificationofthe data transfer packets were all associated with remote attacks. The paper highlighted the ways all ofthese attacks can impact an AV and how blockchain could be deployed to solve most of these problems(7).

The following section will provide an overview of the ways blockchain can be used to mitigate the issueshighlightedintheresearch.

CodeModification

Blockchainmaintainsanimmutableledgerofcodeanddata,makingitextremelydifficulttomodifycodewithout detection. Smart contracts execute the code on the blockchain, which can be used to enforcecodeintegrity,ensuringthatonlyauthorizedandvalidatedcodeisexecuted(41).

CodeInjection:

Blockchain'stransparency and tamper-resistant nature help prevent code injections. Only code thatpassesvalidationandconsensuscanbeexecuted,reducingtheriskofmaliciouscodeinjection(42).

SignalSpoofing:

Blockchain can enhance the security of communication and signal integrity in autonomous systems.Using cryptographic keys and digital signatures, blockchain can validate the authenticity of signals andensurethattheyarenotspoofed.Thisensuresthatsignalsreceivedfromothervehiclesorinfrastructurearetrustworthy(39).

PacketJamming:

Blockchain'sdecentralizednaturecanmitigatepacketjamming.Decentralizednetworksaremoreresilienttolocalizeddisruptions,asdatacanberelayedthroughalternativeroutes.Additionally,blockchaincanbeusedforcriticaltrafficcontroltoensureitreachesitsdestination,eveninthepresenceofjammedchannels(40).

ModificationofDataTransferPackets:

In a blockchain network, data transfer packets cannot be altered without leaving a trace. When data isrecordedontheblockchain,anyattempttomodifyitwouldrequireconsensusfromnetworkparticipants,making unauthorizeddatamodificationextremelychallenging(8).

Conclusion

Inconclusion,theintegrationofself-drivingcarsandblockchaintechnologycanrevolutionizethetransport and logistics industries. Innovation in the field can make transportation secure, efficient, andreliable.Theapplicationofblockchaininautonomousvehiclescanenhancedatasecurity,particularlyin

securepayments,andmanagementofa large number of AVs, moreover the functionalities of theexistingAVscanalsobeimprovedif blockchain-based transaction processing is applied. It enablestransparent transactions, improving the overall trustworthiness of the system. Moreover, it offers thepotential for services that can manage the fleet of AVs, optimize routes that have autonomous vehiclesto reduce traffic congestion, and better management of freight operations. All of these aspects can helpinmakingasmartertransportationecosystem(4).

Asthesetechnologiescontinuetoadvanceandgainwideradoptionafuturewheremoreblockchain-based applications are common can be observed. Moreover, the smart supply chain that ispowered by the network would also enable accessible, and environmentally friendly options for theusers. While there are challenges to address, ongoing research and development in this area can offerimprovements in transportation if widespread adoption is successful. In summary, the combination ofautonomous vehicles and blockchain technology represents the right step in the future direction wheretraditional methods are ignored to promote technologically advanced solutions for cutting overheadcostsandrevolutionizingnthetransportsystemgloballyintheupcomingyears.

References

1. Narbayeva S, Bakibayev T, Abeshev K, Makarova I, Shubenkova K, Pashkevich A. Blockchaintechnologyonthewayofautonomousvehiclesdevelopment.TransportationResearchProcedia[Internet].2020Jan1;44:168–75.Availablefrom:https://doi.org/10.1016/j.trpro.2020.02.024
2. GroverJ.SecurityofVehicularAdHocNetworksusingblockchain:Acomprehensivereview.Vehicular Communications [Internet]. 2022 Apr 1;34:100458. Available from:https://doi.org/10.1016/j.vehcom.2022.100458
3. DwivediSK,AminR,DasAK,LeungMT,ChooKKR,VollalaS.Blockchain-basedvehicularad-hocnetworks: A comprehensive survey. Ad Hoc Networks [Internet]. 2022 Dec 1;137:102980.Availablefrom:https://doi.org/10.1016/j.adhoc.2022.102980
4. LeidingB,MemarmoshrefiP,HogrefeD.Self-managedandblockchain-basedvehicularad-hocnetworks. ACM [Internet]. 2016 Sep 12; Available from:https://doi.org/10.1145/2968219.2971409
5. Abubaker Z, Gurmani MU, Sultana T, Rizwan S, Azeem M, Iftikhar MZ, et al. Decentralizedmechanismforhiringthesmartautonomousvehiclesusingblockchain.In:Lecture notesinnetworks and systems [Internet]. 2019. p. 733–46. Available from:https://doi.org/10.1007/978-3-030-33506-9_67
6. PournaderM,ShiY,SeuringS,KohSCL.Blockchainapplicationsinsupplychains,transportandlogistics: a systematic review of the literature. International Journal of Production Research[Internet]. 2019 Aug 11;58(7):2063–81. Available from:https://doi.org/10.1080/00207543.2019.1650976
7. Thing VLL, Wu J. Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. IEEEInternationalConferenceonInternetofThings(iThings)[Internet].2016Dec1;Availablefrom:https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2016.52
8. KumarMS,VimalS,JhanjhiNZ,DhanabalanSS,AlhumyaniH.Blockchainbasedpeertopeercommunication in autonomous drone operation. Energy Reports [Internet]. 2021 Nov1;7:7925–39.Availablefrom:https://doi.org/10.1016/j.egyr.2021.08.073

9. Gupta R, Tanwar S, Kumar N, Tyagi S. Blockchain-based security attack resilience schemes forautonomousvehiclesinindustry4.0:Asystematicreview.Computers&ElectricalEngineering[Internet]. 2020 Sep 1;86:106717. Available from:https://doi.org/10.1016/j.compeleceng.2020.106717
10. LiXJ,MaM,YongYX.ABlockchain-Basedsecurityschemeforvehicularadhocnetworksinsmartcities. TENCON 2021 - 2021 IEEE Region 10 Conference (TENCON) [Internet]. 2021 Dec 7;Availablefrom:https://doi.org/10.1109/tencon54134.2021.9707356
11. Sung YH, Park SJ, Kim DY, Kim S. GPS spoofing detection method for small UAVs using 1DconvolutionNeuralNetwork.Sensors[Internet].2022Dec2;22(23):9412.Availablefrom:https://doi.org/10.3390/s22239412
12. Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z. Blockchain-Based dynamic keymanagementforheterogeneousintelligenttransportationsystems.IEEEInternetofThingsJournal [Internet]. 2017 Dec 1;4(6):1832–43. Available from:https://doi.org/10.1109/jiot.2017.2740569
13. HeX,AlqahtaniS,GambleRF,PapaM.SecuringOver-The-AirIoTFirmwareUpdatesusingBlockchain. ACM [Internet]. 2019 May 5; Available from:https://doi.org/10.1145/3312614.3312649
14. Das D, Dasgupta K, Biswas U. A secure blockchain-enabled vehicle identity managementframeworkforintelligenttransportationsystems.Computers&ElectricalEngineering[Internet].2023Jan1;105:108535.Availablefrom:https://doi.org/10.1016/j.compeleceng.2022.108535
15. PokhrelSR,ChoiJ.FederatedLearningwithBlockchainforautonomousVehicles:analysisand design challenges. IEEE Transactions on Communications [Internet]. 2020 Aug1;68(8):4734–46.Availablefrom:https://doi.org/10.1109/tcomm.2020.2990686
16. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain andautonomous vehicles: recent advances and future directions. IEEE Access [Internet].2021Jan1;9:130264–328.Availablefrom:https://doi.org/10.1109/access.2021.3113649
17. Jiang X, Yu FR, Song T, Leung VCM. Intelligent resource allocation for video analytics inBlockchain-Enabledinternetofautonomousvehicleswithedgecomputing.IEEEInternetof Things Journal [Internet]. 2022 Aug 15;9(16):14260–72. Available from:https://doi.org/10.1109/jiot.2020.3026354
18. AyvazS,CetinSC.Witnessofthings.InternationalJournalofIntelligentUnmannedSystems [Internet]. 2019 Apr 15;7(2):72–87. Available from:https://doi.org/10.1108/ijius-05-2018-0011
19. Guo H, Meamari E, Shen CC. Blockchain-inspired Event Recording System forAutonomousVehicles.JournalofSensors[Internet].2018Aug1;Availablefrom:https://doi.org/10.1109/hoticn.2018.8606016
20. Guo H, Li W, Nejad M, Shen CC. Proof-of-Event Recording System for autonomousVehicles:aBlockchain-Basedsolution.IEEEAccess[Internet].2020Jan1;8:182776–86.Availablefrom:https://doi.org/10.1109/access.2020.3029512
21. SalahK,RehmanMHU,NizamuddinN,Al-FuqahaA.BlockchainforAI:ReviewandOpenResearch Challenges. IEEE Access [Internet]. 2019 Jan 1;7:10127–49. Available from:https://doi.org/10.1109/access.2018.2890507

22. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralizedblockchain-basedauthenticationsystemforIoT.Computers&Security[Internet].2018Sep1;78:126–42.Availablefrom:https://doi.org/10.1016/j.cose.2018.06.004
23. ChattopadhyayA,LamKY.Securityofautonomousvehicleasacyber-physicalsystem.IEEE Xplore [Internet]. 2017 Dec 1; Available from:https://doi.org/10.1109/ised.2017.8303906
24. JabbarR,FetaisN,KharbecheM,KrichenM,BarkaouiK,ShinoyM.BlockchainfortheInterne t of vehicles: How to use blockchain to secure Vehicle-to-Everything (V2X)communication and payment? IEEE Sensors Journal [Internet]. 2021 Jul15;21(14):15807–23.Availablefrom:https://doi.org/10.1109/jsen.2021.3062219
25. Yeasmin S, Haque A. A Multi-Factor authenticated Blockchain-Based OTA updateframeworkforconnectedautonomousvehicles.2021IEEE94thVehicularTechnol ogyConference (VTC2021-Fall) [Internet]. 2021 Sep 1; Available from:https://doi.org/10.1109/vtc2021-fall52928.2021.9625372
26. Dorri A, Steger M, Kanhere SS, Jurdak R. BlockChain: a distributed solution toautomotivesecurityandprivacy.IEEECommunicationsMagazine[Internet].2017Dec1; 55(12):119–25.Availablefrom:https://doi.org/10.1109/mcom.2017.1700879
27. Hasan GMM, Datta A, Rahman MA. Poster Abstract: Chained of Things: A Secure andDependableDesignofAutonomousVehicleServices.IEEEXplore[Internet].2018Apr1;A vailablefrom: https://doi.org/10.1109/iotdi.2018.00048
28. Wang JZ, Li M, He Y, Li H, Xiao K, Wang C. A blockchain based Privacy-Preservingincentivemechanismincrowdsensingapplications.IEEEAccess[Internet].20 18Jan1;6:17545–56.Availablefrom:https://doi.org/10.1109/access.2018.2805837
29. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain andautonomous vehicles: recent advances and future directions. IEEE Access [Internet].2021Jan1;9:130264–328.Availablefrom:https://doi.org/10.1109/access.2021.3113649
30. DuZ,WuC,YoshinagaT,YauKA,JiY,LiJ.FederatedLearningforVehicularInternetofThings:r ecentadvancesandopenissues.IEEEOpenJournaloftheComputerSociety[Internet]. 2020 Jan 1;1:45–61. Available from:https://doi.org/10.1109/ojcs.2020.2992630
31. BadrMM,AmiriWA,FoudaMM,MahmoudM,AljohaniAJ,AlasmaryW.Smartparkingsyste m with privacy preservation and reputation management using blockchain. IEEEAccess [Internet]. 2020 Jan 1;8:150823–43. Available from:https://doi.org/10.1109/access.2020.3016945
32. Lai C, Zhang M, Cao J, Zheng D. SPIR: a Secure and Privacy-Preserving Incentive SchemeforReliableReal-TimeMapupdates.IEEEInternetofThingsJournal[Internet].2020Jan1;7(1):416–28.Availablefrom: https://doi.org/10.1109/jiot.2019.2953188
33. Kamal M, Barua A, Vitale C, Laoudias C, Ellinas G. GPS location spoofing attack detectionforenhancingthesecurityofautonomousvehicles.2021IEEE94thVehicularTechno logyConference (VTC2021-Fall) [Internet]. 2021 Sep 1; Available from:https://doi.org/10.1109/vtc2021-fall52928.2021.9625567
34. Lattarulo R, Pérez J, Dendaluce M. A complete framework for developing and testingautomateddrivingcontrollers.IFAC-PapersOnLine[Internet].2017Jul1;50(1):258–63.Availablefrom:https://doi.org/10.1016/j.ifacol.2017.08.043

35. ZhuZ,ZhaoH.AsurveyofdeepRLandILforAutonomousDrivingPolicylearning.IEEETransactions on Intelligent Transportation Systems [Internet]. 2022 Sep1;23(9):14043–65.Availablefrom:https://doi.org/10.1109/tits.2021.3134702
36. JabbarR,KharbecheM,Al-KhalifaKN,KrichenM,BarkaouiK.BlockchainfortheInternetofVehicles: a decentralized IoT solution for vehicles communication using Ethereum.Sensors [Internet]. 2020 Jul 15;20(14):3928. Available from:https://doi.org/10.3390/s20143928
37. Banabilah S, Aloqaily M, Alsayed E, Malik N, Jararweh Y. Federated learning review:Fundamentals,enablingtechnologies,andfutureapplications.InformationProcessingand Management [Internet]. 2022 Nov 1;59(6):103061. Available from:https://doi.org/10.1016/j.ipm.2022.103061
38. FagnantDJ,KockelmanKM.PreparinganationforautonomousvehicIes:opportunities,barriers and policy recommendations. Transportation Research Part A-policy andPractice [Internet]. 2015 Jul 1;77:167–81. Available from:https://doi.org/10.1016/j.tra.2015.04.003
39. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain andautonomous vehicles: recent advances and future directions. IEEE Access [Internet].2021Jan1;9:130264–328.Availablefrom:https://doi.org/10.1109/access.2021.3113649
40. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges.FutureGenerationComputerSystems[Internet].2018May1;82:395–411.Availablefrom:https://doi.org/10.1016/j.future.2017.11.022
41. SherminV.DisruptinggovernancewithblockchainsandsmartcontIacts.StrategicChange [Internet]. 2017 Sep 1;26(5):499–509. Available from:https://doi.org/10.1002/jsc.2150
42. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security:application areas, security threats, and solution architectures. IEEE Access [Internet].2019Jan1;7:82721–43.Availablefrom:https://doi.org/10.1109/access.2019.2924045
43. Sanka AI, Cheung RCC. A systematic review of blockchain scalability: Issues, solutions,analysisandfutureresearch.JournalofNetworkandComputerApplications[Internet].2021Dec1;195:103232.Availablefrom:https://doi.org/10.1016/j.jnca.2021.103232
44. Angin P, Mert MB, Mete O, Ramazanli A, Sarica K, Gungoren B. A Blockchain-Baseddecentralized security architecture for IoT. In: Lecture Notes in Computer Science[Internet].2018.p.3–18.Availablefrom:https://doi.org/10.1007/978-3-319-94370-1_1
45. Jain S, Ahuja NJ, Srikanth P, Bhadane KV, Nagaiah B, Kumar A, et al. Blockchain andautonomous vehicles: recent advances and future directions. IEEE Access [Internet].2021Jan1;9:130264–328.Availablefrom:https://doi.org/10.1109/access.2021.3113649
46. HofmannE,RüschM.Industry4.0andthecurrentstatusaswellasfutureprospectsonlogistics. Computers in Industry [Internet]. 2017 Aug 1;89:23–34. Available from:https://doi.org/10.1016/j.compind.2017.04.002
47. Fraga-LamasP,Fernández-CaramésTM.AreviewonblockchaintechnologiesforanadvancedandCyber-Resilientautomotiveindustry.IEEEAccess[Internet].2019Jan1;7:17578–98.Availablefrom:https://doi.org/10.1109/access.2019.2895302
48. LuongNC,HoangDT,GongS,NiyatoD,WangP,LiangYC,etal.ApplicationsofDeepReinfor

cementLearninginCommunicationsandNetworking:asurvey.IEEE

CommunicationsSurveysandTutorials[Internet].2019Jan1;21(4):3133–74.Availablefrom:https://doi.org/10.1109/comst.2019.2916583

49. Al-FuqahaA,GuizaniM,MohammadiM,AledhariM,AyyashM.InternetofThings:Asurvey on enabling technologies, protocols, and applications. IEEE CommunicationsSurveys and Tutorials [Internet]. 2015 Jan 1;17(4):2347–76. Available from:https://doi.org/10.1109/comst.2015.2444095
50. PereiraJLF,RossettiRJF.Anintegratedarchitectureforautonomousvehiclessimulation.IEEE Xcess [Internet]. 2012 Mar 26; Available from:https://doi.org/10.1145/2245276.2245333
51. ErmanAT,VanHoeselL,HavingaPJM,WuJ.Enablingmobilityinheterogeneouswirelesssensor networks cooperating with UAVs for mission-critical management. IEEE WirelessCommunications [Internet]. 2008 Dec 1;15(6):38–46. Available from:https://doi.org/10.1109/mwc.2008.4749746
52. ZhengL,ZhuY,XueB,LiuM,FanR.Low-CostGPS-AidedLiDARStateEstimationandMapBuilding. Journal of Sensors [Internet]. 2019 Dec 1; Available from:https://doi.org/10.1109/ist48021.2019.9010530